NAMIBIA UNIVERSITY
OF SCIENCE AND TECHNOLOGY

Faculty of Computing and Informatics

Department of Computer Science

A Lightweight Authentication Architecture for Unsupervised Internet of Things (IoT) in Smart Home Applications

Thesis

Submitted in fulfilment of the requirements for the degree of

Doctor of Philosophy in Computer Science

at

Namibia University of Science and Technology

Submitted by:	Attlee M. Gamundani
Student Number:	216104092
Supervisor:	Prof. H.N. MUYINGI
Co-Supervisor:	Dr A. Phillips
Date of Submission:	November 2018

METADATA

TITLE:	Mr
STUDENT NAME:	Attlee Munyaradzi Gamundani
SUPERVISOR:	Prof. Hippolyte Nsung-Nza MUYINGI
CO- SUPERVISOR:	Dr Amelia Phillips
DEPARTMENT:	Computer Science
QUALIFICATION:	PhD in Computer Science
SPECIALISATION:	Computer Security
STUDY TITLE:	Doctor of Philosophy in Computer Science
MAIN KNOWLEDGE AREA:	Information Assurance and Security
KEYWORDS:	Authentication; Architecture; Lightweight; Smart Home; Internet of Things; Unsupervised
TYPE OF RESEARCH:	Applied Research
METHODOLOGY:	Design Science Methodology
STATUS:	Thesis
SITE:	Main Campus, Windhoek
DOCUMENT DATE:	April 2019
RESEARCH LAB:	Digital Forensics and Information Security

DECLARATION

I, **ATTLEE MUNYARADZI GAMUNDANI**, hereby declare that the work contained in this thesis for the degree of PhD in COMPUTER SCIENCE project, entitled: **"A LIGHTWEIGHT AUTHENTICATION ARCHITECTURE FOR UNSUPERVISED INTERNET OF THINGS (IoT) IN SMART HOME APPLICATIONS,"** is my own original work and that I have not previously in its entirety or in part submitted it at any university or other higher education institution for the award of a degree.

I further declare that I fully acknowledged any sources of information used for this research in accordance with the Institution's rules.

Signature: ________________________ Date: 22 March 2019

ABSTRACT

The Smart Home environment is made up of different objects that have sensing capabilities and have the potential to interact with each other seamlessly. This brings a lot of convenience to the control and monitoring of the surroundings around the home environment. This reality is brought about as a result of the Internet of Things (IoT) phenomenon. The potential benefits presented by IoT technologies around the Smart Home environment can and are hampered by security issues that are yet to be resolved both at the perception layer and the transmission layer.

The need to secure data collected around the home environment and the exchange of such data among the smart objects is of paramount importance. The general limitation that things in the Internet of Things suffer from is that of computational power and storage space. Resource constrained devices hinder the application of robust security solutions that conventional networking environment devices enjoy hence the need to look at the suitable solutions that meet the resource basis of things in an optimal way. To realise this objective, this research employed a constructivist paradigm, which guided the design of an artefact that was tested under the guided framework of the design science research approach.

The focus on authentication as a security dimension has been motivated by its interweaved nature into other security pillars. Authentication proves to be a primary security key window in that if it fails to detect unauthorised access, all other security loopholes are opened in the entire networked environment.

A simulated Smart Home environment that modelled critical application requirements for Assisted Ambient Living (AAL) spaces and Energy Saving Solutions (ESS) was used to evaluate the proposed lightweight authentication architecture's efficiency, which was tested against existing similar solutions around the same functionality. The lightweight authentication architecture presented in this submission was tested using the SCYTHER tool, which allowed verification, falsification and security testing by checking on various classes of attacks and possible architecture behaviour. The architecture turned out secure for tested insider, impersonation, replay and man-in-middle attacks, which were considered ideal as guided by the Dolev-Yao model.

The contribution of this research is its pragmatic approach to the security design for constrained things in IoT that can operate with little to no human intervention – hence unsupervised. Key findings from this work highlight two important aspects for proper security advancement, which are identity management of things in the IoT space and the scalability of using agent based models to reduce resource demands at the device level.

As an envisaged current and future relevance of this work, it may inform the security design of authentication solutions in IoT application environments in ad hoc personal area network setups and feed into the bigger vision of smart cities.

Keywords: Authentication; Architecture; Lightweight; Smart Home; Internet of Things; Unsupervised.

ACKNOWLEDGEMENTS

To the God Almighty, be all Glory and Honour!!

It is a great honour and privilege to seize this opportunity to acknowledge the sacrifice, love, dedication, commitment, and perpetual support of the following key people for walking me through this pilgrimage towards this esteemed accomplishment in no particular order.

- Dear wife Nyarai and lovely daughter Tatianna, sparing your valuable time to allow me to focus on this research – I can't put a price to that.
- Focused and dedicated mentors, Prof. Hippolyte N. MUYINGI and Dr Amelia Phillips.
- The Faculty of Computing and Informatics at NUST and the entire NUST Community, for making the research environment conducive.
- The visionary Digital Forensics and Information Security Research Cluster for the continual support and inspiration.
- The Gamundani Family members and the Banana Family members for giving me time and space to focus on these studies when you needed me most.
- All those that contributed directly or indirectly towards the accomplishment of this worthwhile milestone, you are always remembered - friends, relatives, and colleagues.

DEDICATION

A special dedication to my beautiful wife Nyarai and my lovely daughter Tatianna, you are my pillars of strength girls

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

PUBLICATIONS RELATED TO THIS WORK

Gamundani, A. M. (2015). An impact review on Internet of Things attacks. In *Proceedings of 2015 International Conference on Emerging Trends in Networks and Computer Communications, ETNCC 2015*.17-20 May 2015, Windhoek, Namibia. https://doi.org/10.1109/ETNCC.2015.7184819

Gamundani, A. M., Phillips, A., & Muyingi,H.N., (2018). An Overview of potential authentication threats and attacks on Internet of Things (IoT): A focus on Smart Home Applications. In *Proceedings of the 11th IEEE International Conference on Internet of Things(iThings-2018)Halifax,Canada*.http://cse.stfx.ca/~iThings2018/acceptedlist.htm

Gamundani, A. M., Phillips, A., & Muyingi,H.N., (2018). A Review and Costing of Lightweight Authentication Schemes for Internet of Things(IoT): Towards design of an authentication architecture for Smart Home applications. In *Proceedings of the 6th International Workshop on Applications and Techniques in Cyber Security 2018 (ATCS 2018), in Conjunction with SecureComm 2018, Singapore.*

Gamundani, A. M., Phillips, A., & MUYINGI,H.N., (2018). Privacy Preservation and Security Dilemma: Relationship proposition for IoT authentication. In *Proceedings of the International Conference on Recent Innovations in Electrical, Electronics & Communication Engineering –(ICRIEECE), India.*

LIST OF ACRONYMS AND ABBREVIATIONS

2FLIP	Two Factor Authentication
3G	3rd Generation
6lowPANS	IPv6 over Low Power Wireless Personal Area Networks
AA	Authentication Architecture
AAA	Authentication, Access Control, Assurance
AAL	Ambient Assisted Living
ABE	Attribute Based Encryption
ABE	Attribute Based Encryption
ABM	Agent Based Modelling
AI	Artificial Intelligence
AODV	Ad hoc On-Demand Distance Vector
AVISPA	Automated Validation of Internet Security Protocols and Applications
BISC	Biometric – IMEI & SIM - Colour
BLE	Bluetooth Low Energy
CCN	Context Centric Networks
CDM	Challenge Driven Model
CIA	Confidentiality, Integrity, Availability
CoAP	Constrained Application Protocol
COMPASS	Computerised Model for Predicting and Analysing Support Structures
CPS	Cyber Physical Systems
DaoT	Dynamic and Energy-aware Authentication Scheme for the Internet of Things
DIY	Do It Yourself
DoS	Denial of Service
DoS	Denial of Service
DSM	Demand-Side Management
DTLS	Datagram Transport Layer Security
DTMF	Dual Tone Multi Frequency
ECC	Elliptical Curve Cryptography
EDGE	Enhanced Data for GSM Evolution
ESS	Energy Saving Solution
ESDA	Enhanced Secure Device Authentication
ESH	Eclipse Smart Home
GDPR	General Data Protection Rule
H2M	Human to Machine
HA	Home Agent
HEM	Home Energy Management
HEMS	Home Energy Management System
HIVE	Home Automation System for Intrusion Detection

HOL	High Order Logic
HSS	Home Security System
HTTP	Hyper Text Transfer Protocol
HVAC	Heating, Ventilation, and Air Conditioning
IACAC	Identity Authentication and Capacity Based Access Control
IBC	Identity Based Cryptography
ID	Identity
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IoT	Internet of Things
IoTtalk-RC	Internet of Things talk Remote Control
IP	Internet Protocol
IPv6	Internet Protocol Version 6
ISC	Inner Social Connectedness
LAN	Local Area Network
LTE	Long Term Evolution
M2M	Machine to Machine
MANETS	Mobile Ad hoc Network
MATLAB	MATrix LABoratory
MQTT	Message Queuing Telemetry Transport
MQTT-SN	Message Queuing Telemetry Transport for Sensor Networks
NDN	Data Networking
NFC	Near Field Communication
OSC	Outer Social Connectedness
PAN	Personal Area Networks
PIR	Passive Infrared
PSK	Pre Shared Key
PUF	Physically Unclonable Function
QoL	Quality of Life
QoS	Quality of Service
RADIUS	Remote Authentication Dial in User Service
REPAST	Recursive Porous Agent Simulation Toolkit
REST	Representational State Transfer
RFID	Radio Frequency Identification
ROI	Region of Interest
RSA	Rivest-Shamir-Adleman algorithm
SAREF	Safety Research Experiment Facility
SDGs	Sustainable Development Goals
SDN	Software Based Network
SH	Smart Home
SHS	Smart Home Systems

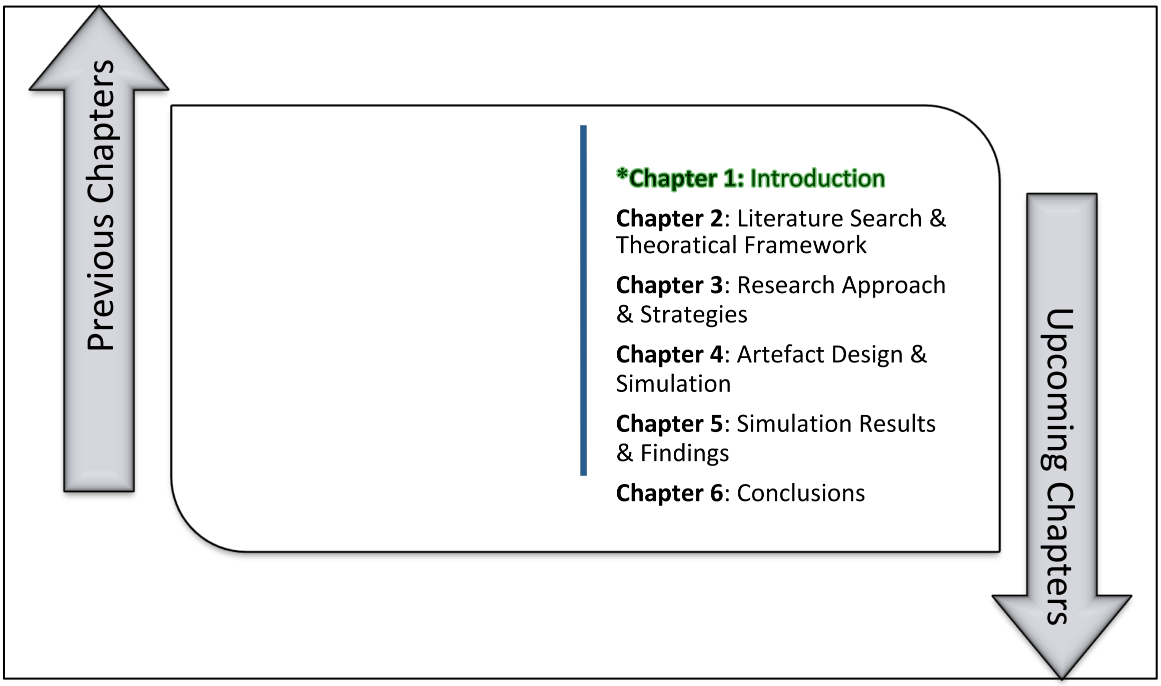
SILDA	Secure Intuitive and Low cost Device Authentication
SMACK	Short Message Authentication ChecK
SPDL	Security Protocol Description Language
SQL	Structured Query Language
SSL	Secure Sockets Layer
TCM	Trusted Cryptography Modules
TCP	Transport Control Protocol
TCP/IP	Transport Control Protocol over Internet Protocol
TESLA	Timed Efficient Stream Loss-Tolerant Authentication
TLS	Transport Layer Security
TV	TeleVision
UDP	User Datagram Protocol
URC	Universal Console
UWB	Ultra Wide Band
UX	User eXperience
V2G	Vehicle to Grid
VANETS	Vehicular Ad hoc Network
VOS	Voltage Over Scaling
VS	Virtual Storage
Waas	Wisdom as a Service
WI-FI	Wireless Fidelity
WIM	World In Miniature
WSN	Wireless Sensor Networks
XaaS	Everything as a Service
XOR	Exclusive OR

WORKING DEFINITIONS

The following are the simplified and contextualised definitions that apply to the key terms used in this research: -

- **Lightweight** – *a solution that computationally has limited processing and storage capabilities requirements*
- **Authentication** – *the process of identity verification to grant access to a set of resources*
- **Architecture** - *a set of rules and methods that describe the functionality, organisation, and implementation of* **authentication** *in a Smart Home*
- ***Unsupervised*** *- operating with little to no human intervention/interaction*
- **Smart Home** - *a typical environment made up of different devices that have sensing capabilities and which can interact with each other seamlessly*
- **Internet of Things –** *a network of interconnected devices that enable the building of a Smart Home*

CHAPTER 1: INTRODUCTION



Previous Chapters

***Chapter 1:** Introduction

Chapter 2: Literature Search & Theoratical Framework

Chapter 3: Research Approach & Strategies

Chapter 4: Artefact Design & Simulation

Chapter 5: Simulation Results & Findings

Chapter 6: Conclusions

Upcoming Chapters

This chapter sets the tone for the research by introducing the research concepts through highlighting the background to the research. To enable the reader to follow through the entire work presented herein, this chapter also defines the main key terms likely to be encountered throughout this document. A breakdown of the entire thesis layout is given at the end of this chapter to enable an easy following of the concepts covered.

1.1 Chapter Overview

This chapter gives a background to the research by highlighting the main driver for the research focus through spelling out the problem statement. Presented in this chapter is an outline of the conceptual framework for this work. In addition to outlining the key research objectives guiding the work, an articulation of the rationale for conducting the research is presented.

Chapter Organisation: Section 1.2 provides an overview of the phenomenon of IoT as the main pillar and broad research area. Building on that, Section 1.3 zooms into the potential research gaps from which the main focus of the research was derived. Section 1.4 outlines the research problem formulated. The research questions and objectives are summarised in sections 1.5 and 1.6 respectively. The last sections of the chapter are dedicated to details about the conceptual framework, the rationale for the study, delimitations, and scope of the study, research contributions and finally an outline of the thesis chapters.

1.2 Background

Internet of Things (IoT) is an evolving networking phenomena (Rizzardi, Sicari, Miorandi, & Coen-Porisini, 2016; Weber, 2010; Yao, Chen, & Tian, 2014). Moreover, "Despite the various definitions available, the common understanding on IoT revolves around the interconnection capabilities among things" (Gamundani, 2015, p. 114). The interconnection extends to objects and people. According to Mahalle (2013), in such a case, transformation takes place from an Internet of computers to IoT with device to device communication, which brings in the aspect of unsupervised interactions. Such heterogeneous network environments have come to being due to the diverse communication platforms, protocols and services which are now flooding the market (Rizzardi et al., 2016; Sicari, Rizzardi, Grieco, & Coen-Porisini, 2015). Some of the communication technologies are Radio Frequency Identification (RFID), Wireless Fidelity (Wi-Fi) and Wireless Sensor Networks (WSN) (Yang, Sun, & Guo, 2016).

To bring out a clear definition of IoT, the clarity offered by Haller (2010) as illustrated in Figure 1.1 paints a picture of the key players in IoT functionality as well as their relationships such as 'services accesses resources' that contain a device, device to device communication, and or the device sensing entity of interest.

A major discovery from this attempt to define things in IoT by Haller (2010) is that an absolute and clear-cut categorisation is not always possible, but rather it is subject to the perspective from where one is looking at a particular thing from. A more positioned definition is presented by Kang, Pang and Wang (2013), where IoT is presented as:

> a complex cyber-physical system that integrates all kinds of sensing, identification, communication, networking, and informatics devices and systems, and seamlessly connect all the people and things upon interests, so that anybody at any time and any place, through any device and media, can more efficiently access the information of any object and any service. (Kang et al., 2013, p. 64)

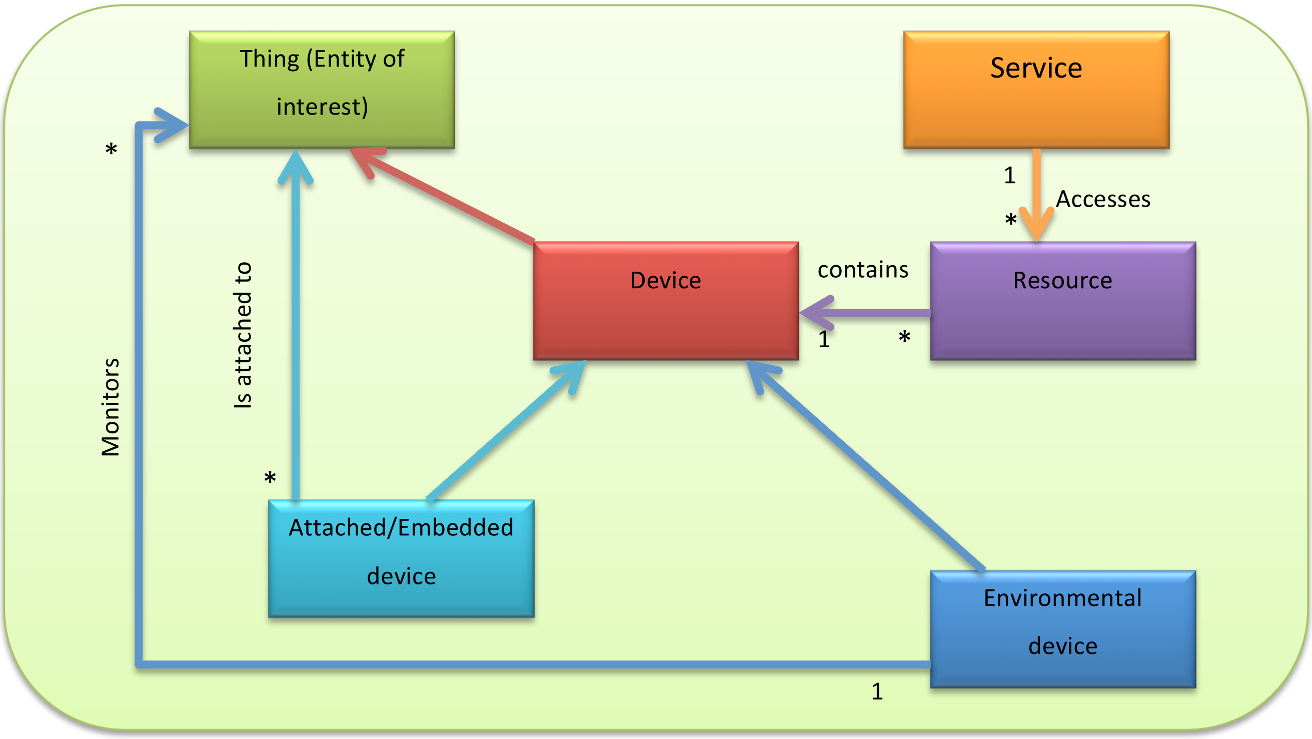


Figure 1.1: Relationship between things, devices, resources and services (Haller, 2013)

This view therefore concurs with the illustration in Figure 1.1. This corroborates the fact that defining a thing in the IoT has to be contextualised in order to allow for a precise understanding of the things in IoT.

Zooming into the IoT domain reveals the envisaged benefits and the mushrooming challenges that are being discovered for such an agile technology. To reach their maximum potential, IoT security threats need to be handled at every level of their lifecycle so that the technology reaches its maximum potential (Gusmeroli, Sundmaeker, & Bassi, n.d.; Weber, 2010). This will entail that the possible application domains for IoT will be minimised. Moreover, the pervasive, complex and heterogeneous nature of IoT on its own present a complicated security fibre (Yao et al., 2014).

The projected figures on digital gadgets possession per every user by 2024 are an average of six and even more, which indeed points to a complex network being created across the user horizon (Mahalle, & Anggorojati, 2013). Fifty billion devices are projected to be connected to the Internet by 2020 (Brandt, 2015). This signals the position this research is built upon, that individuals will likely lose control of their various interactions with the devices around them which can extend in connectivity with or without their physical involvement, hence resulting in unsupervised broadcasting of data.

The growth and continual use of enabling technologies such as Cloud computing platforms is facilitating the increase in the use of IoT as supported by massive storage, inelastic communication possibilities which are backed by sensors, wireless mobile communication and embedded systems acting as key enablers (Zhu, Uddin, Qin, & Venkatasubramanian, 2017). However, the scepticism around the growth and usage of IoT enabled technologies mainly points towards security loopholes (Gubbi, Buyya, Marusic, & Palaniswami, 2013).

IoT is playing an important role in many different scenarios in our daily lives, from smart cities to Smart Homes (Zhao & Ge, 2013). The Smart Home application environment therefore, may not be prepared to fully harness the capabilities and functionalities of IoT in a secure manner as supported by the device-level IoT security vulnerabilities summarised in **Chapter 2, Figure 3.3**. Therefore this research intended to explore the best secure authentication mechanism to solve some of the identified challenges in **Chapter 2**.

The seamless nature of connectivity between objects and humans or objects and objects has necessitated authentication as a critical aspect to consider. The need to address the validation of sources of communication among the participating entities in the web of objects and people in the IoT environment is of paramount importance. There are three security layers for IoT, which can be summarised by the mapping in Figure 1.2. From this mapping, it can be noted that at every layer, authentication has a role to play.

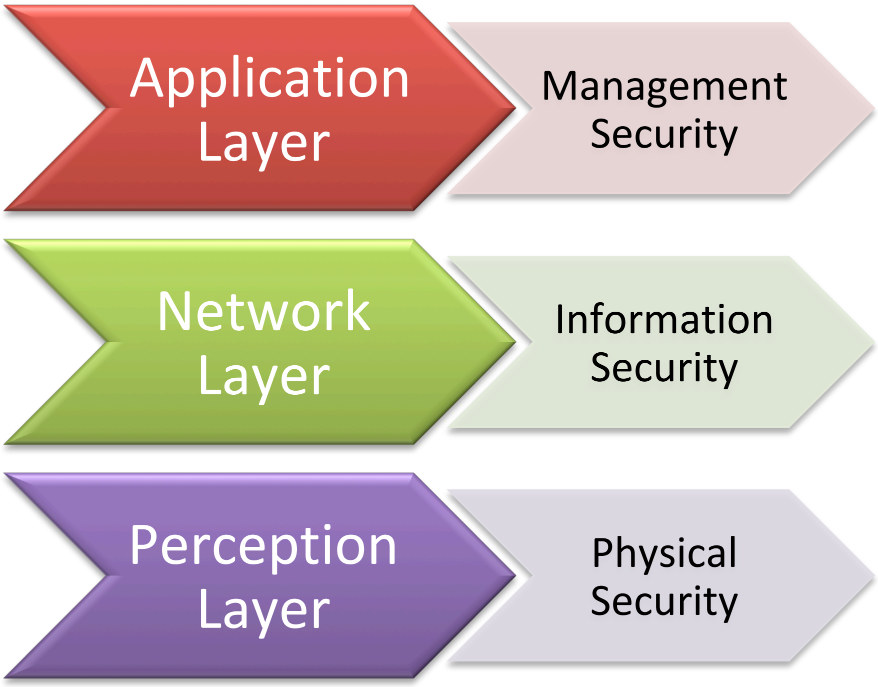


Figure 1.2: The mapping of security layers to security dimensions
(Zhao & Ge, 2013)

Authentication should be the initial handshake security level that has to grant access rights to pieces of data around the Smart Home environment. This is corroborated by Zhao and Ge (2013), who argue that "IoT should have these characteristics: comprehensive perception, reliable transmission, and intelligent processing" (p. 664).

1.3 Research Gap

The main security challenges attributable to IoT design, functionality and growth as presented by Mahalle (2013) are mainly evident in the application's weak security considerations. The weak application security challenges point towards authentication as the main loophole as it opens doors to other security threats. Addressing the authentication security challenge implies a well-formulated strategy for addressing major security weaknesses. Thus authentication in a Smart Home application is key as it addresses the data confidentiality level of the security triad, which mainly focuses on the privacy of user information (Sharma, Khanna, & Bhatnagar, 2017).

A security solution design by Wu and Li (2013) which focused on Trusted Cryptography Modules (TCM), proposes solutions that are cryptographic by nature. Therefore, in the context of objects that are applicable to a Smart Home environment, these solutions may turn out to be heavy in terms of computational requirements, given the limited storage space and processing capacity. This solution by Wu and Li (2013) mainly focused on the trustworthiness of IoT design and implementation, which renders the approach limited in scope. Given the diverse areas of IoT applications, a more broad approach to security is needed as supported by Saied, Olivereau, Zeghlache and Laurent (2014). The need to evaluate the efficiency of available security protocols as a measure of security for security needs assessment for the heterogeneous IoT application domains can be adopted as espoused by Saied et al. (2014), as that is a critical phenomenon which still needs attention. **Chapter 2** details such typical solutions in an in-depth approach.

Authentication is among the top vital aspects for consideration towards the design of secure IoT communication. However, the provision of a distributed, lightweight and bulletproof solution for a total security solution towards IoT applications remains one of the biggest challenges (Mahalle, 2013). Researchers therefore, still need to find suitable authentication scheme improvements towards the design of secure and viable solutions at an application layer.

The work done by Mahalle (2013) under the identity management solution left some of the following issues open for future research as summarised in Figure 1.3: -

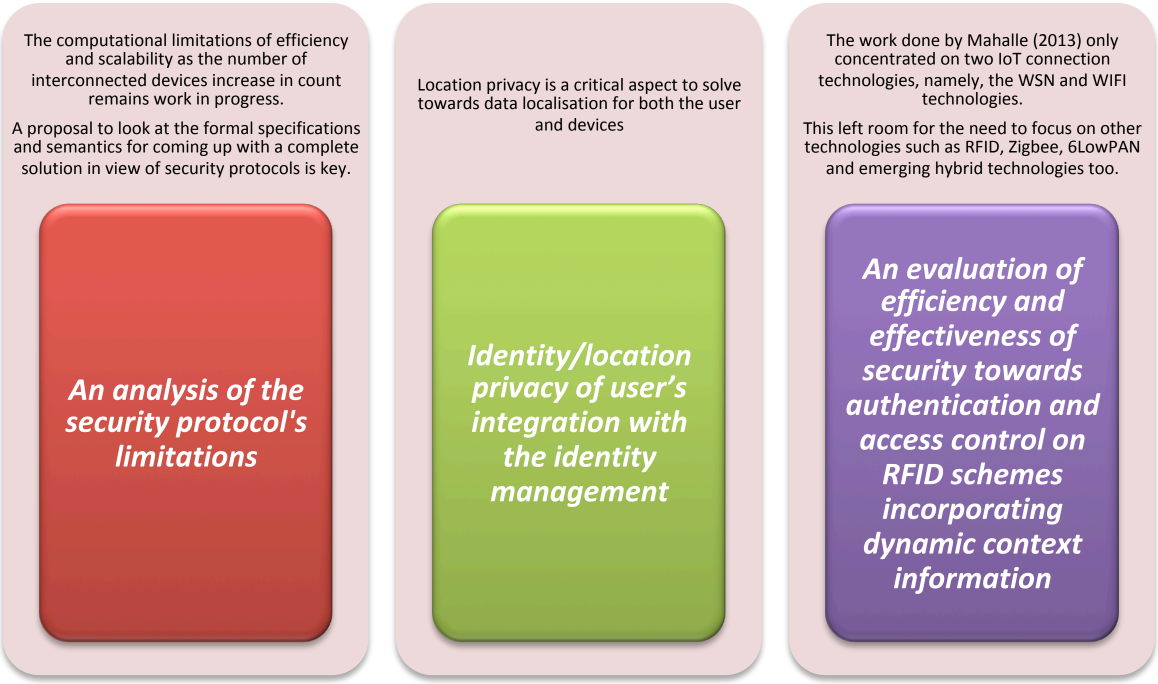

The computational limitations of efficiency and scalability as the number of interconnected devices increase in count remains work in progress.
A proposal to look at the formal specifications and semantics for coming up with a complete solution in view of security protocols is key.
An analysis of the security protocol's limitations
Location privacy is a critical aspect to solve towards data localisation for both the user and devices
Identity/location privacy of user's integration with the identity management
The work done by Mahalle (2013) only concentrated on two IoT connection technologies, namely, the WSN and WIFI technologies.
This left room for the need to focus on other technologies such as RFID, Zigbee, 6LowPAN and emerging hybrid technologies too.
An evaluation of efficiency and effectiveness of security towards authentication and access control on RFID schemes incorporating dynamic context information

Figure 1.3: Open issues for further research

1.4 Problem Statement

Authentication as a key primary security window in IoT application design and implementation is still an open issue as existing solutions are constrained to meet the trade-offs of computational efficiency and lightweight solutions (Mahalle, 2013; Sicari et al., 2015; Yao et al., 2014). The lack thereof of a universal solution for the heterogeneous forms of IoT communication networks is a concern.

As supported by Yao et al. (2015), the majority of resource-constrained nodes motivate for a rigid lightweight IoT security as a key consideration. Thus, the main challenge being addressed by this research is explictly stated as: -

The design of secure authentication architecture, incorporating lightweight properties of IoT is still an open issue.

Thus, the goal of this research is presented as: -

To design secure lightweight authentication architecture for unsupervised IoT in a Smart Home application environment.

1.5 Research Objectives

To realise the above-stated goal, the following objectives had to be met, namely to: -

1. Identify the potential authentication threats to IoT Smart Home applications;
2. Analyse current IoT authentication architectures that suit Smart Home applications;
3. Design a lightweight IoT secure authentication architecture for Smart Home applications; and
4. Evaluate the proposed secure solution for correctness and computation efficiency.

1.6 Research Questions

To realise the main goal of this research, key questions needed to be formulated and answered which guided the set objectives that speak to the overall research focus. The main question that this study sought to answer is: -

How can IoT devices that have limited computational power, storage space, and operate with little human intervention be able to authenticate when their stored data are accessed securely, and by whom and when in a Smart Home application domain?

The sub questions below try and simplify the task of answering this broad question and they are namely:

1. What are the potential authentication threats to IoT in Smart Home applications?
2. What are the available authentication mechanisms for IoT and their relative performance?
3. How can Smart Home IoT objects be authenticated in a computationally efficient, secure and correct manner?
4. What performance evaluation approach and strategy can best validate the architecture?

1.7 Conceptual Framework

IoT is a concept to get things connected to the Internet, and Thing-to-Thing or Machine to Machine (M2M) interaction is the core IoT technology (Hui, Sherratt, & Sánchez, 2017). The term M2M implies that the communication between two electronic systems occur autonomously without any human interventions (Morsalin et al., 2017).

Various low-cost embedded devices are considered, that sense, process, store and communicate data autonomously (Ahmed & Kim, 2016). IP based communication forces data to be tightly coupled with communication channel and device-to device addresses, and named data networking (NDN) has been proposed as an extension to context-centric networks (CCNs) as a future Internet architecture. NDN gives identity to content as a "first-class citizen" within the network in contrast to the naïve Internet, where some numeric IP addresses of the source/destination modes and channel security are the focal points during communication (Ahmed & Kim, 2016)

NDN secures each packet at the time of its production, enabling data caching (replication) at each node while preserving the security aspects of data throughout the packet's lifetime (Ahmed & Kim, 2016). Given this scenario, an end-to-end security is emphasised by this setup. It is crucial to ensure that data is securely transmitted, hence enabling the realisation of the Confidentiality, Integrity and Availability (CIA) components to a reasonable state.

Heterogeneous IoT communication technologies such as Zigbee, Bluetooth, Wi-Fi, Wi-Fi Direct and LAN can exist in a given Smart Home (Ahmed & Kim, 2016). This heterogeneity is one that adds to the complexity of IoT applications. Different technologies imply sometimes-different manufacturers. There is often the challenge of handling the different heterogeneous features to avail a holistic security setup.

The main security issues in IoT as highlighted by Sicari et al. (2015) are summarised in Figure 1.4 below. Each of the identified challenges is interdependent on authentication in one-way or the other. Access control requires authentication to grant permission to the required resources or services. To ensure a secure middleware, we need to authenticate how access to the middleware is rendered and what rights can be granted, as part of middleware security. Before trust can be extended between communicating parties, these parties need to be authenticated against the set privileges and access rights. Access policy enforcement can be assured if we authenticate the source of the instructions for the given policy. To ensure privacy, access to personal information has to be granted to authorised users through authentication, which equally speaks to confidentiality on the other hand.

Mobile security can thus be realised if the access control layer is properly secured through authentication. Also highlighted by Yao et al. (2014), is the fact that the increase in the number of sensors available and their ability to interconnect and be linked to user personal information, and the need to control personal data calls for the prioritisation of data security. This then justifies why in a Smart Home environment such IoT sensors need to authenticate themselves in their interaction within their locally created ad hoc networks. This has to be ensured before allowing outsiders to have access to the collected and stored inside information, which may be sensitive to the Smart Home inhabitants. This therefore, points to the reason why the focus of this study was on authentication.

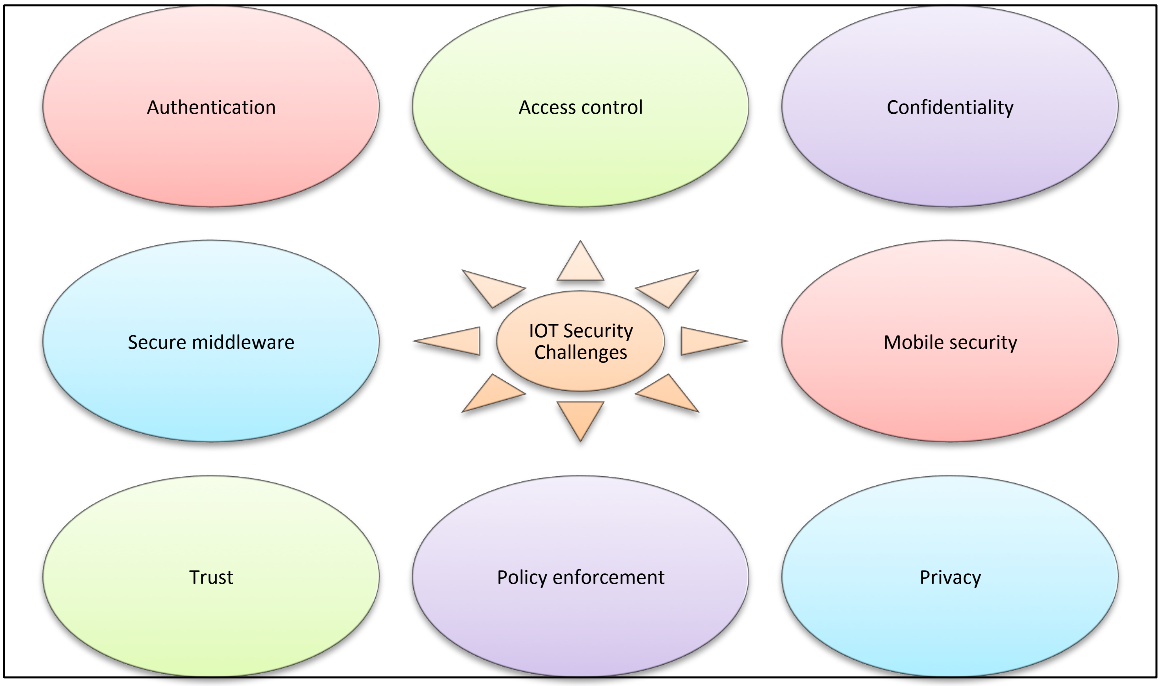


Figure 1.4: Main security issues in IoT
(Sicari et al., 2015)

The overarching conceptual framework guiding this work on the security domain is the security triad as displayed in Figure 1.5 below. The lightweight authentication solution proposed for this work was evaluated based on the security triad for its effectiveness and functionality.

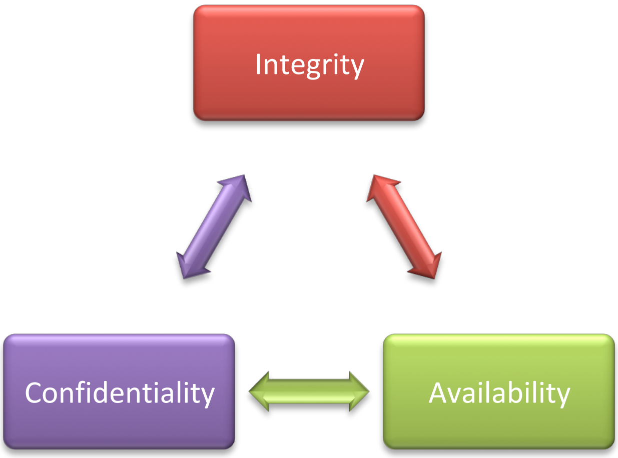


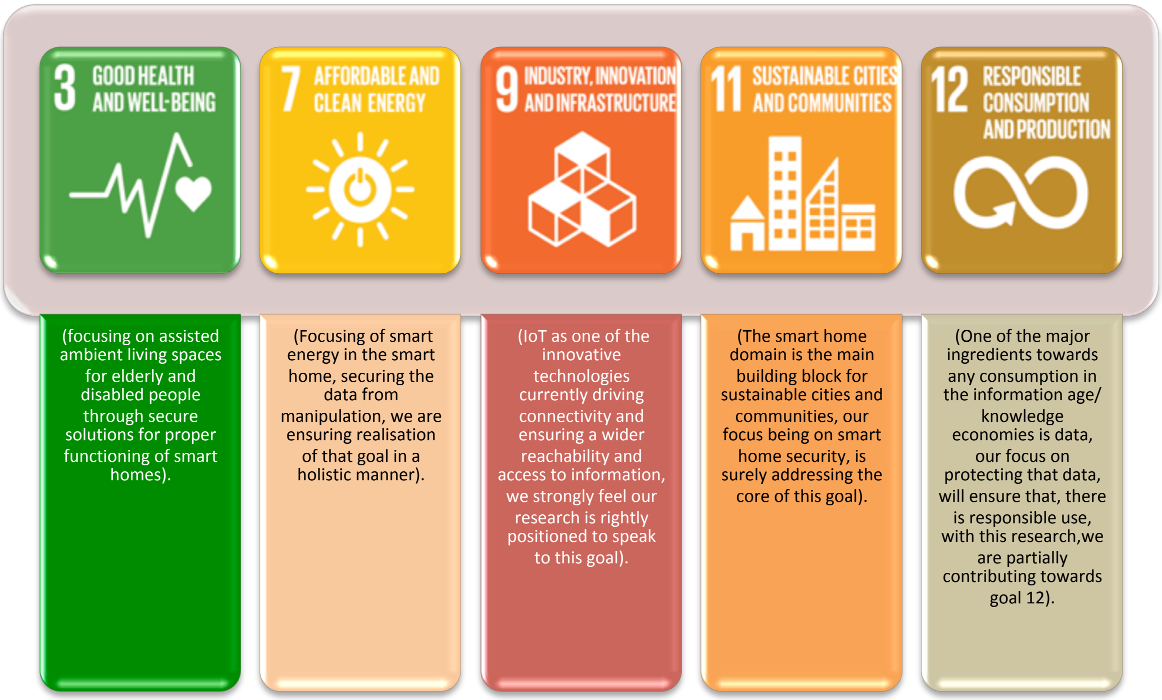
Figure 1.5:The security triad
(Henderson, 2015)

1.8 Rationale

Following the Challenge Driven Model (CDM) (which is further explained in **Chapter 3**), part of the 17 United Nations (UN) Sustainable Development Goals (SDGs)(SDGs, 2017) for practical relevance guided this research, and we position it in light of addressing and contributing partially or in full to some of the highlighted goals. The five SDGs (3, 7, 9, 11 & 12) that our work speaks to and how it does so are summarised in Figure 1.6 below.

Among other envisaged benefits of this research, accountability and transparency in the interconnection of IoT objects can be realised. Cyber perpetrated crimes may be addressed to a relative level. Moreover, the deployment of future technologies around IoT may receive a boost based on the findings that were tabled after the completion of this research.

The focus on a solution that can be applied to constrained resources that have the capabilities to interconnect among themselves, with little to no human intervention, gave a solid starting point for building a comprehensive security architecture for the ever growing IoT solutions that can be advanced at an individual level all the way through to industrial and nationwide solutions.


3 GOOD HEALTH AND WELL-BEING
7 AFFORDABLE AND CLEAN ENERGY
9 INDUSTRY, INNOVATION AND INFRASTRUCTURE
11 SUSTAINABLE CITIES AND COMMUNITIES
12 RESPONSIBLE CONSUMPTION AND PRODUCTION

(focusing on assisted ambient living spaces for elderly and disabled people through secure solutions for proper functioning of smart homes).

(Focusing of smart energy in the smart home, securing the data from manipulation, we are ensuring realisation of that goal in a holistic manner).

(IoT as one of the innovative technologies currently driving connectivity and ensuring a wider reachability and access to information, we strongly feel our research is rightly positioned to speak to this goal).

(The smart home domain is the main building block for sustainable cities and communities, our focus being on smart home security, is surely addressing the core of this goal).

(One of the major ingredients towards any consumption in the information age/ knowledge economies is data, our focus on protecting that data, will ensure that, there is responsible use, with this research,we are partially contributing towards goal 12).

Figure 1.6: How our research speaks to 5 of the SDGs
(SDGs, 2017)

Much work has been advanced towards security of IoT from different perspectives, yet there still remains a challenge to handle the inbuilt security solutions for IoT, as well as the perspective of looking at the whole security solution from the autonomous nature of IoT devices – which is the unsupervised context to be adopted in this research.

As IoT is one of the evolving technologies, it presents a strong learning ground, thus embarking on this research may help the researchers to realise the current security concerns in the cyber space. Therefore there was real value in investing time and resources on this research as it promises future professional growth for the researchers.

1.9 Delimitation and Scope

The scope of this research is limited to IoT Personal Area Networks (PAN) created and simulated in a Smart Home domain. The security dimensions were limited to authentication. Moreover, the application focus in the Smart Home was limited to Energy Saving Solutions (ESS) and Ambient Assisted

Living (AAL) applications (highlighted in **Chapter 2, Section 2.5**), so as to streamline our research focus towards contribution to the highlighted SDGs in Figure 1.6.

1.10 Research Contributions

- The major outcome of this work is secure authentication architecture for unsupervised IoT networks, which can be applied in the domain of Smart Home designs and has the potential to be escalated to other domains.
- The major contribution is to the general body of knowledge of Information Assurance and Security, and particularly advancement in the security protocol architecture and implementation in the Internet and Interconnected network technology.
- In considering security of typical unsupervised objects, their interaction should not be limited to homogeneous ones, but to explore the other various possible horizontal or vertical connections in a broad sense. It is envisaged that a more detailed approach to network challenges and threats can be extended from the findings of the implementation of the proposed solution.
- As part of the deliverables, at least four scientific publications were reviewed in peer-reviewed conferences and one of the publications was adopted as a book chapter in the Springer Journal, all these marked completed progress contribution indicators of the findings and novelty of this research.

1.11 Thesis Chapter Overview

Chapter 1: Introduction

Covers the background to the research, gives an outline of key terms and provides a conceptual framework for this research.

Chapter 2: Literature Search & Theoretical Framework

This chapter offers the decisive focus of the research by tiding all the literature review findings and spelling the focus of this particular research. It helps in defining the scope of the research. Positioned to populate the relevant literature in a bid to paint a picture of the Smart Home domain, and this chapter defines the basis of the research platform to be adopted for the entire research. The main deliverable is a detailed Smart Home environment walkthrough in the first section.

The chapter further explores the envisaged security threats specifically for the defined Smart Home domain. This section helps the reader to understand why focus was given to the chosen security threats compared to others, hence slowly shaping the main direction of this research.

In an attempt to give a detailed review of existing solutions and their respective application features and their performance gauge, this chapter is strategically positioned to set the tone for the main research focus towards the design of secure authentication architecture. A performance analysis of existing solutions was done on a costing basis.

The chapter finally gives the context of the Smart Home adopted, the threats to be addressed and the authentication techniques and features to be adopted.

Chapter 3: Research approach and strategies

This chapter details the literature on the research methodology and the chosen research paradigm. This chapter also details and unpacks the methodology to the full in the context of the approach proposed for this work. It also explains how data was collected, which variables were considered and how the data was analysed to draw the necessary conclusions.

Chapter 4: Artefact design and simulation

This section populates the design of the proposed architecture, how it was simulated and the scenarios that were created to simulate the Smart Home application environment as well as the security design implemented.

Chapter 5: Simulation results and findings

This chapter details an account of the simulation results and the analysis of the results presented for evaluation purposes.

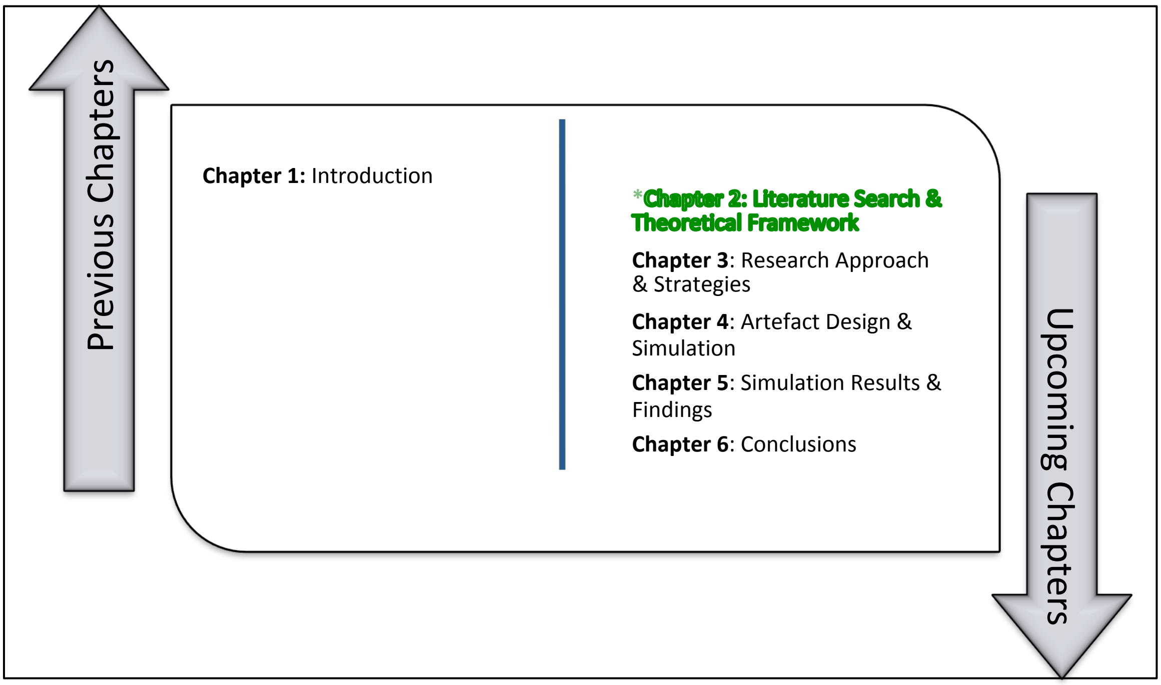
Chapter 6: Conclusions

This chapter summarises the findings from the simulated implementation and draws final conclusions of this work. As a pointer and a reflection slot, this chapter also guides towards future research directions in light of the field of focus enshrined in this work.

1.12 Chapter Summary

The following key aspects have been discussed in this chapter: - an overview of the phenomenon of IoT as the main pillar and broad research area for this research, potential research gaps where the main focus of this research was derived from, an outline of the research problem formulated for this research work, research questions and objectives, the conceptual framework of the research, defining the rationale of the research, marking the delimitation of the research as well as the scope, and spelling out the contributions of the research to the existing body of knowledge.

CHAPTER 2: LITERATURE SEARCH & THEORETICAL FRAMEWORK



Previous Chapters

Chapter 1: Introduction

***Chapter 2: Literature Search & Theoretical Framework**

Chapter 3: Research Approach & Strategies

Chapter 4: Artefact Design & Simulation

Chapter 5: Simulation Results & Findings

Chapter 6: Conclusions

Upcoming Chapters

With the mandate of making it clear to the reader what Smart Home context we are focusing on, this chapter is set to detail the contextual Smart Home setup of this research. Furthermore, the chapter unearths some of the potential applications and challenges typical to a Smart Home setup in the context of IoT. This chapter ensures fulfilment of research objective 1: "Identify the potential authentication threats to IoT in Smart Home applications", and Objective 2: "Analyse current IoT authentication architectures that suit smart home applications".

2.1 Chapter Overview

This chapter gives a summary based on widely consulted scientific literature reviews of the main focus of this research work in particular as summarised in Figure 2.1. Having gone through various literature sources and gaining several perspectives on similar subjects, it was important to streamline the content and focus our direction towards our main objective and overall goal of the research as enshrined in **Chapter 1**.

Chapter Organisation: Section 2.2 looks at the brief history of the Smart Home concept in preparation for defining what a Smart Home is in section 2.3. As a way of defining Smart Homes, section 2.3 gives two different approaches; 2.3.1 looks into Smart Home theories, and then 2.3.2 covers Smart Home models. Requirements for setting up or running a Smart Home are detailed in section 2.4, where networking requirements are highlighted in 2.4.1. The various things that make up a Smart Home are expanded in 2.4.2. Section 2.5 builds on top of previous sections to give a summary of the various applications common to Smart Homes. In the quest to give a holistic picture, section 2.6 covers the Smart Home challenges, which are relooked at in section 2.7 with a different angle, where the future of Smart Homes is highlighted.

Section 2.8 covers security threats towards authentication in general, in an attempt to give an overall outlook on security threats irrespective of the domain of focus. In Section 2.9, specific threats peculiar to IoT are then looked into in a broader approach. As a way of focusing the chapter's attention, section 2.10 brings in the threat landscape for Smart Home applications, which is mainly informed by the Dolev-Yao attack model. It is in Section 2.11 that security threats towards Smart Home applications are outlined and further broken down into classifications in 2.11.1. A layer-by-layer assessment of the threats is done in 2.11.2, 2.11.3 and 2.11.4, with a focus on device level, network level and application level respectively.

Section 2.12 takes a detailed look at IoT authentication by first highlighting some of the existing lightweight IoT authentication schemes, then zooming into lightweight authentication schemes that have been applied to Smart Home applications. Guided by the observations from section 2.12, section 2.13 gives comparisons of lightweight solutions based on the costing of the algorithms. Section 2.16

finally presents some recommendations for Smart Home security solution designs. Section 2.15 covers the focus area picked for Smart Homes, and then Section 2.16 looks at the IoT focus area. Section 2.17 looks at the authentication focus area, while Section 2.18 gives the overall research focus mapping. The overall conclusion of this chapter is presented in Section 2.19.

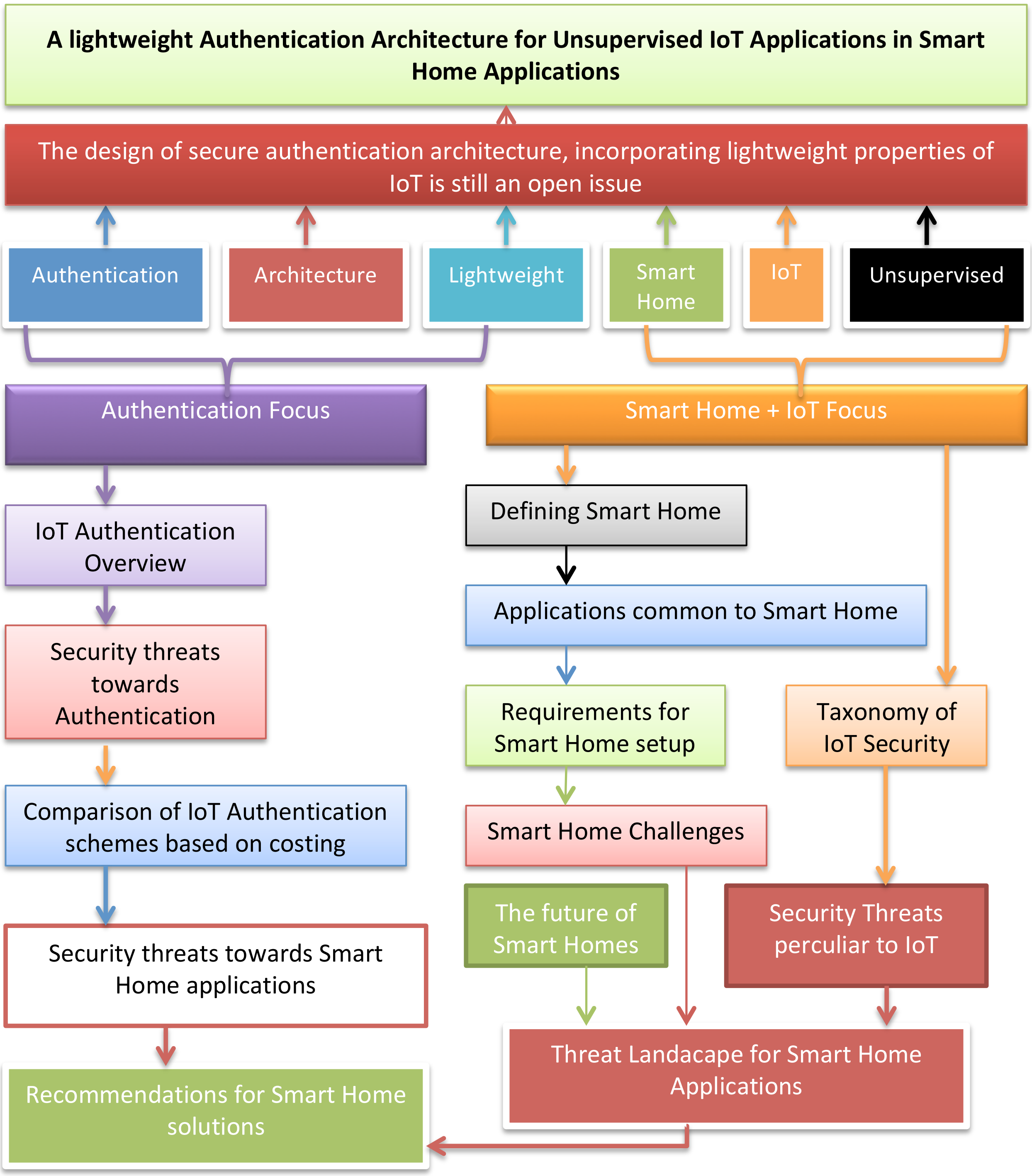

A lightweight Authentication Architecture for Unsupervised IoT Applications in Smart Home Applications
The design of secure authentication architecture, incorporating lightweight properties of IoT is still an open issue
Authentication
Architecture
Lightweight
Smart Home
IoT
Unsupervised
Authentication Focus
Smart Home + IoT Focus
IoT Authentication Overview
Security threats towards Authentication
Comparison of IoT Authentication schemes based on costing
Security threats towards Smart Home applications
Recommendations for Smart Home solutions
Defining Smart Home
Applications common to Smart Home
Requirements for Smart Home setup
Smart Home Challenges
The future of Smart Homes
Taxonomy of IoT Security
Security Threats perculiar to IoT
Threat Landacape for Smart Home Applications

Figure 2.1: Theoretical Framework

2.2 Defining the Smart Home

The definition given by Alaa, Zaidan, Zaidan, Talal, and Kiah (2017) on a Smart Home as a domain of IoT, a network of physical devices which provides electronic, sensor, software, and network connectivity inside a home is quite comprehensive. From this definition, the various components that make up a Smart Home are highlighted. We however, recommend that connectivity outside a home should be considered as part of the definition, as a Smart Home does not exist in isolation.

Smart Home (SH) or Home Agent (HA) is defined as an application of IoT technologies in the home environment and a major building block for smart cities when privacy protection issues are properly addressed (Hui et al., 2017). Another variation of the Smart Home definition is highlighted by Seo, Kim, Kim, and Lee (2016), where they define a Smart Home as a new environment that can apply the use of IoT. For that to happen, a seamless integration among humans, physical objects, and user interactions has to exist. From the definition given by Smirek, Zimmermann, and Beigl (2016), Smart Homes are presented as spaces meant to help people with special needs such as the elderly and those with disabilities, to stay with their familiar environments without necessarily having to be moved to other places they might not be comfortable with like hospitals or special care homes.

A crucial point of a Smart Home is to provide services that respond to the needs of the users (Fabi, Spigliantini, & Corgnati, 2017). The network is the most important feature that builds up a Smart Home as supported by Fabi et al. (2017), that it is the existence of connected home devices that distinguishes the Smart Home system from a home merely equipped with standalone and highly advanced technological features.

As outlined by Mokhtari, Zhang, Nourbakhsh, Ball, and Karunanithi (2017), the emergency of new technologies ranging from mobile computing to smart sensors and Internet of Things, Smart Homes have become a hot research topic. This assertion is further supported by Chen et al. (2017), where Smart Homes are presented as a key to the transformation of people’s lifestyles. Typical cyber physical systems (CPS) applications are SH and Ambient Intelligence (AmI) where monitoring, controlling and automating functions are accomplished through connected sensors and actuators (Hui et al., 2017).

The depiction of a Smart Home provided by Zhang, Xiang, Huang, Chen, and Alelaiwi (2018), gives an overview of the visual representation of the interconnectedness of devices in a Smart Home and how they interact with the outside world. Our depiction of the same scenario is what is visually represented in Figure 2.2 below.

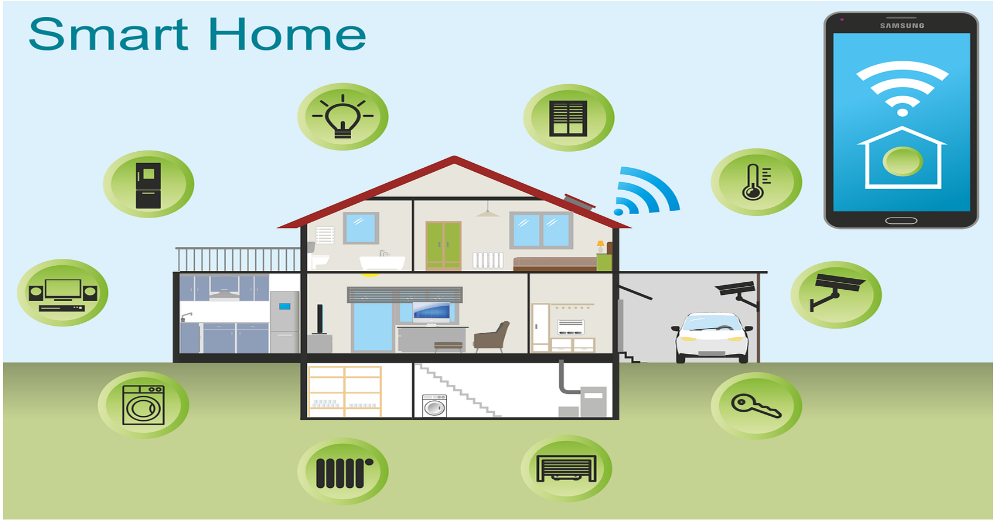


Figure 2.2: Smart Home setup

2.2.1 Smart Home theories

The use of sound to recognise user activity in Smart Homes is proposed by Lee, Choi, and Kwon (2017), where the use of acoustic sensor data acquired in an unobtrusive manner for maintaining maximum privacy possible is suggested. This is an interesting dimension as it gives a broad range of possible solutions to advance activity recognition beyond the visual effects.

A people-centric design approach, which is informed by collected and learnt personal behaviours, is considered central in building smart cities. In order to share resources effectively and intelligently, understanding such behaviours from a Smart Home context enables the provision of tailor-made services to individual inhabitants (Hui et al., 2017).

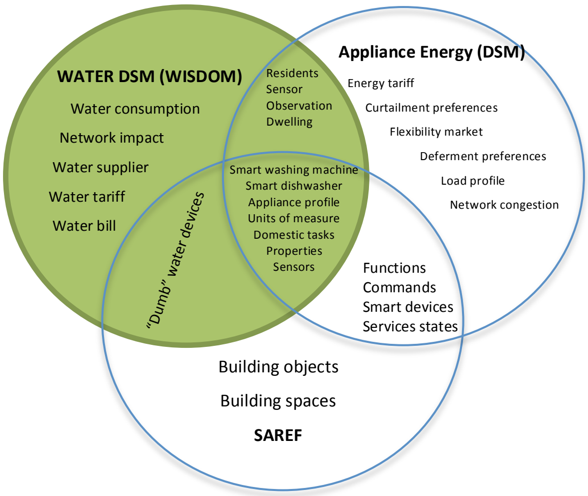
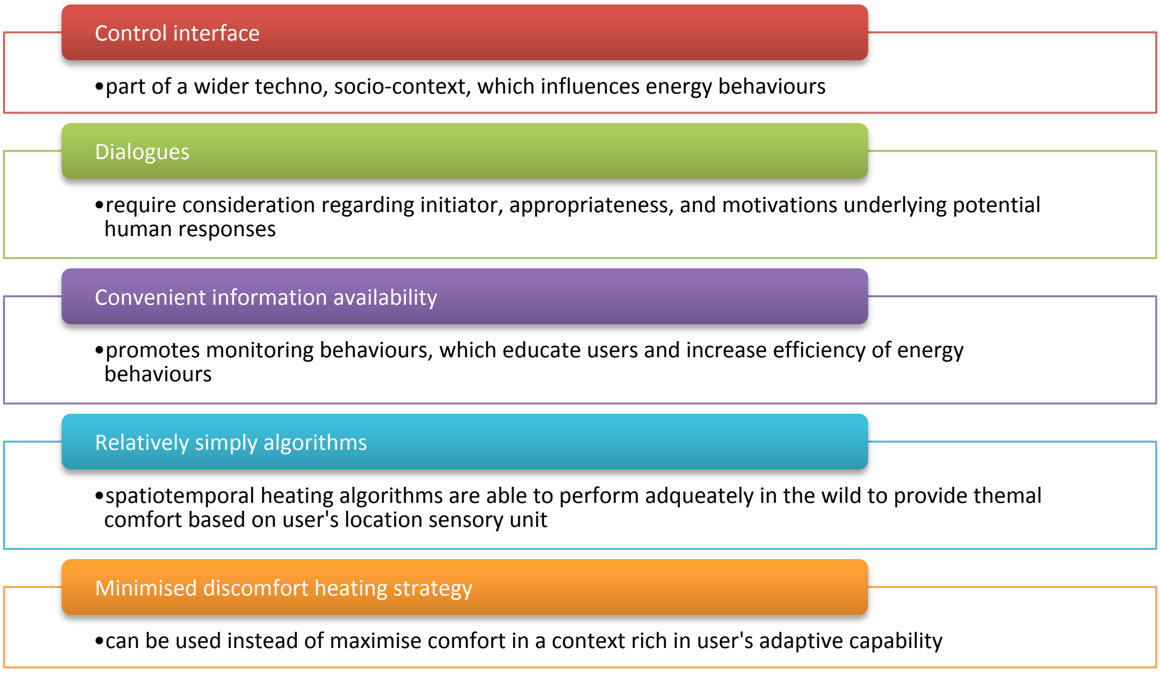


Figure 2.3: Object reuse across Smart Home applications
(Howell, Rezgui, & Beach, 2017)

A semantic knowledge management service and domain ontology which supports a novel cloud edge solution is highlighted by Howell et al. (2017). Through unifying domestic socio-technical water systems with clean and waste networks at the urban scale, such a model is able to deliver value-added services for consumers and network operators (Howell et al., 2017). A use case, which highlights the interoperability benefits of the semantic alignment at the building scale, is shown in Figure 2.3 above, which illustrates the hypothetical case of a consumer with both a water feedback app and appliance-scheduling app interacting with their devices through alignment with Safety Research Experiment Facility (SAREF) ontology.

Social connectedness is an interesting concept presented by Lee, Kwon, Lee, and Kim (2017), which gives interactions between users and the Smart Home devices. Lee et al. (2017) present two dimensions of social connectedness, which are Inner Social Connectedness (ISC) and Outer Social Connectedness (OSC). ISC relates to the connections between the devices and the user in a Smart Home, whereas OSC speaks to connections made from smart devices in other people's houses and the users in a Smart Home on focus. Over and above the connectedness, Lee et al. (2017) introduced two types of interactions, the unmediated and the mediated. With the unmediated interaction, the individual device reveals itself to the user hence it is easy to interact with, whereas with the mediated interaction, users interact with a single agent, which will be representing various Smart Home devices.

As summarised in their research, Lee et al. (2017) highlight that ISC was more effective with unmediated interaction while OSC thrived under mediated interaction.



Control interface

- part of a wider techno, socio-context, which influences energy behaviours

Dialogues

- require consideration regarding initiator, appropriateness, and motivations underlying potential human responses

Convenient information availability

- promotes monitoring behaviours, which educate users and increase efficiency of energy behaviours

Relatively simply algorithms

- spatiotemporal heating algorithms are able to perform adqueately in the wild to provide themal comfort based on user's location sensory unit

Minimised discomfort heating strategy

- can be used instead of maximise comfort in a context rich in user's adaptive capability

Figure 2.4: Spatiotemporal heating control variables
(Kruusimagi, Sharples, & Robinson, 2017)

As demonstrated by Kruusimagi et al. (2017), the ability to achieve a fine degree of spatiotemporal heating control in the domestic setting and the socio-themo-technical complexity of the setting by deploying a quasi-autonomous heating system are summarised in Figure 2.4 above. The notion of user experience (UX) is summed up in Figure 2.4 as the “Conceptual contributions and implications of UX in energy preservation behaviours by users in Smart Homes” (Kruusimagi et al., 2017).

2.2.2 Smart Home models

The centralised Smart Home architecture presented by Zhang et al. (2018) depicts an entity that constitutes a gateway and a heterogeneous set of products from different manufactures. The gateway becomes the central control and link between the various appliances and the inhabitants of the Smart Home. A role played by the gateway is also to facilitate interoperability and control of home appliances Zhang et al. (2018).

Among the key models and paradigms for Smart Home designs, Ambient Assisted Living (AAL) is common as postulated by Rawashdeh, Al Zamil, Samarah, Hossain, and Muhammad (2017), which enables activity monitoring for the elderly, children, disabled and people with special needs (Kara, Lamouchi, & Ramdane-Cherif, 2017). The AAL paradigm is one that promotes the seamless merging among between, Smart Homes, smart health and smart cities. The effective implementation of AAL thrives on activity recognition (Rawashdeh et al., 2017), which is possible through profiling the activities of the inhabitants of a Smart Home. The framework depicted in Figure 2.5 below shows how AAL is applied to render quality life services to homebound patients and any category of those in need of special attention and care.

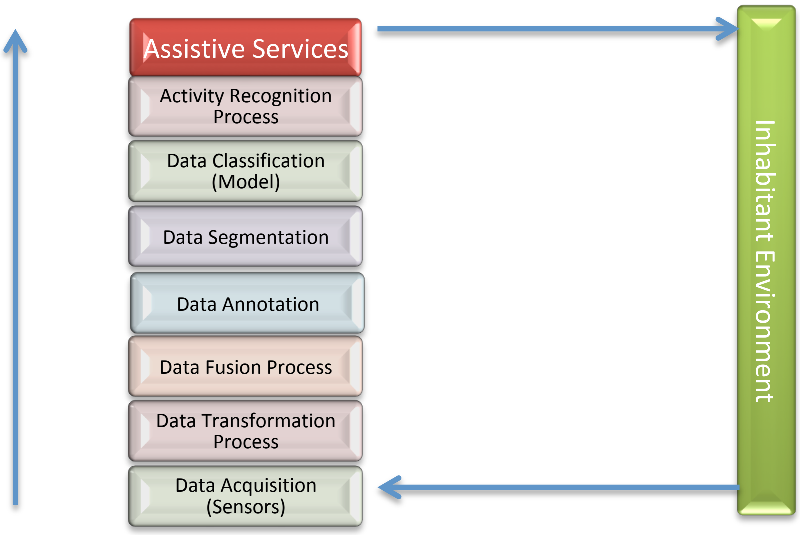

Assistive Services
Activity Recognition Process
Data Classification (Model)
Data Segmentation
Data Annotation
Data Fusion Process
Data Transformation Process
Data Acquisition (Sensors)
Inhabitant Environment

Figure 2.5: The framework of activity recognition in Smart Homes
(Rawashdeh et al., 2017)

The Eclipse Smart Home (ESH) project and the Universal Remote Console (URC) were designed with the sole purpose of addressing the integration and customisation of user interfaces (Smirek et al., 2016). ESH focuses on the integration of different devices and backend technologies, whilst URC provides a personalised and pluggable user interface (Smirek et al., 2016). Another similar model is presented for a novel non-wearable identification system to recognise multiple residents in a home environment through ambient non-intrusive ultra-wide band (UWB) sensors (Mokhtari, Zhang, Hargrave, & Ralston, 2017).

Home Energy Management System (HEMS) is becoming important for users to regularly monitor their energy consumption, at the same time maintaining the efficiency of their home appliances (Joo & Choi, 2017). Given the need to always be functional for devices in smart living spaces, loss of power may disrupt normal operations hence the essence of monitoring becomes key.

The Bi-level market model analyses the impact of Smart Home scheduling to the electricity market (Liu et al., 2017). The customers schedule home appliances for bill reduction at the community level, whereas aggregators minimise the energy purchasing expense from utilities at the market level, both of which consider the Smart Home scheduling impacts (Liu et al., 2017).

A six layer Smart Home security system (HSS) is presented by Morsalin et al. (2017) whose layers are implemented by near field communication (NFC) tag, secured password protection, fingerprint, M2M system, an android application and a passive infrared (PIR) sensor (i.e. motion sensor, this has been proposed as a reaction to the growth of burglary and theft which was threating traditional home security systems).

A hybrid-reality based user experience and evaluation of a context-aware Smart Home is advanced by Seo et al. (2016) using virtual reality. Integrating egocentric and exocentric virtual reality, user experience is modelled. A world-in-miniature (WIM) was constructed to make a Smart Home environment more realistic and natural by making use of various kinds of tangible and physical Smart Home activities, which were allowed for prototyping a number of appliances, sensors, and human physical object interactions (Seo et al., 2016).

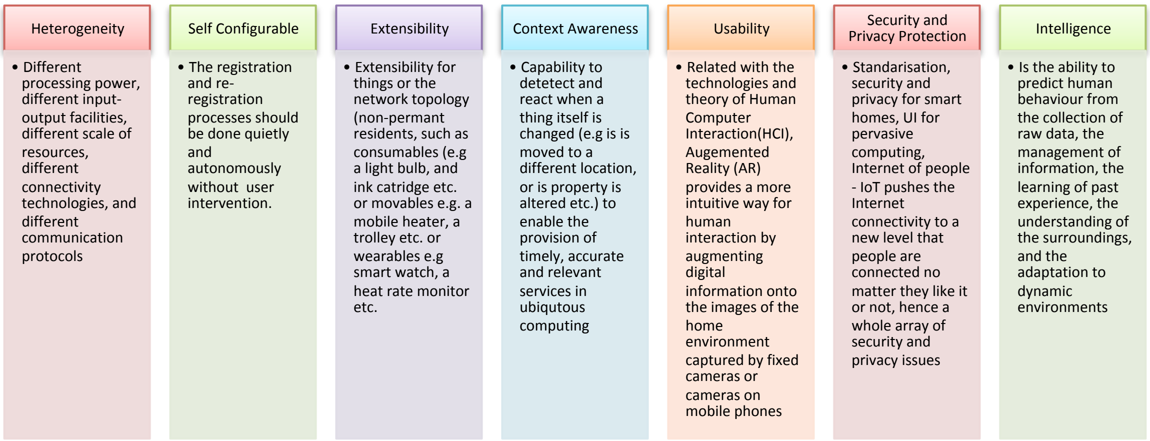
Through the proposed Region of Internet (ROI) extraction approach, the system generates a unique UWB signature for each individual which will be used for their identification (Mokhtari et al., 2017). This approach highly favours an AAL setup and energy saving models.

A novel multi-layer, cloud architectural model is presented by (Tao, Zuo, Liu, Castiglione, and Palmieri (2018), which was developed to enable effective and seamless interactions/interoperations on heterogeneous devices/services provided by different vendors in the IoT based Smart Home. With the focus on solving the heterogeneity issues in the presented layered cloud platform, the model could address data representation, knowledge, and application heterogeneity. An ontology-based security service framework was designed as part of the model for supporting security and privacy preservation in the process of interactions/ interpretations.

2.3 Requirements for Smart Home Setup

A more detailed requirement analysis and presentation for Smart Home setups was done by Hui et al. (2017), who recommended that IoT should provide holistic security for it to become an alternative in the context of critical equipment management inside a home environment. Hui et al. (2017), pointed to the need for high degree of heterogeneity, how repetitiveness, polarisation of user experience, demands of security and privacy protection, as typical and critical characteristics of Smart Homes. As summed up in Figure 2.6 below, the requirements pointed out by Hui et al. (2017) are quite central for consideration as they point towards some of the key attributes that need attention when designing security solutions.

The need to understand what features make up a Smart Home go a long way in facilitating a holistic approach towards advancing solutions that can practically be applied at specific layers. It is easier to address specific challenges and placing them in the context outlined in Figure 2.6 below.



Heterogeneity

- Different processing power, different input-output facilities, different scale of resources, different connectivity technologies, and different communication protocols

Self Configurable

- The registration and re-registration processes should be done quietly and autonomously without user intervention.

Extensibility

- Extensibility for things or the network topology (non-permant residents, such as consumables (e.g a light bulb, and ink catridge etc. or movables e.g. a mobile heater, a trolley etc. or wearables e.g smart watch, a heat rate monitor etc.

Context Awareness

- Capability to detetect and react when a thing itself is changed (e.g is is moved to a different location, or is property is altered etc.) to enable the provision of timely, accurate and relevant services in ubiqutous computing

Usability

- Related with the technologies and theory of Human Computer Interaction(HCI), Augemented Reality (AR) provides a more intuitive way for human interaction by augmenting digital information onto the images of the home environment captured by fixed cameras or cameras on mobile phones

Security and Privacy Protection

- Standarisation, security and privacy for smart homes, UI for pervasive computing, Internet of people - IoT pushes the Internet connectivity to a new level that people are connected no matter they like it or not, hence a whole array of security and privacy issues

Intelligence

- Is the ability to predict human behaviour from the collection of raw data, the management of information, the learning of past experience, the understanding of the surroundings, and the adaptation to dynamic environments

Figure 2.6: Major requirements for Smart Homes
(Hui et al., 2017)

The role of cloud computing in the overall build and functionality of the Smart Home is highly appreciated by Hui et al. (2017), as confirmed by the assertion that the offloading of the home server is happening with the proliferation of cloud computing services and the popularity of high speed home broadband. Services from many cloud computing supplies provide connection with Everything as a Service (XaaS) for remote monitoring, controlling and automating things in the Smart Home sector (Hui et al., 2017).

Smart Homes ultimately have these key requirements once established: mobility management, channel security, consistent data rates and handover support, as presented by Shin, Sharma, Kim, Kwon, and You (2017), which hint towards the need to look at security designs and requirements for Smart Home domains with more rigor.

2.3.1 Networking

The proliferation of ubiquitous wireless sensor networks (WSN) protocols has enabled WSNs to dominate the M2M connectivity technology in SH (Hui et al., 2017). Zigbee and Z-wave are the most common home control WSN protocols that provide low cost and low power mesh network connectivity, and also recently added to the list is the newly introduced Bluetooth low Energy (BLE 4.1) (Hui et al., 2017).

Cellular networks, for example Enhanced Data for GSM Evolution (EDGE), 3rd Generation (3G), Long Term Evolution (LTE), and many others, provide Internet connectivity for Internet Protocol (IP)-enabled devices, but the connection cost is relatively high (Hui et al., 2017). 6LowPAN also based on IEEE 802.15.4 like Zigbee and wireless Hart, enables direct IPv6 connectivity.

2.3.2 The Things in the Smart Home Environment

There are different appliances that have varying capabilities from computational capacity, storage to networking, that are found in Smart Home setups. As outlined by Zhang et al. (2018), a variety of use cases are possible in a Smart Home from light control, appliance control to security and safety systems. The home appliance can include but is not limited to “low cost sensors, smart lights, smart thermostats and cameras and other appliances integrated with intelligence” (Zhang et al., 2018).

The top-level structure of the Smart Home domain ontology as presented by Tao et al., 2018), herewith depicted in Figure 2.7 below, gives an overview of some of the key applications and setup of IoT devices in a Smart Home setup.

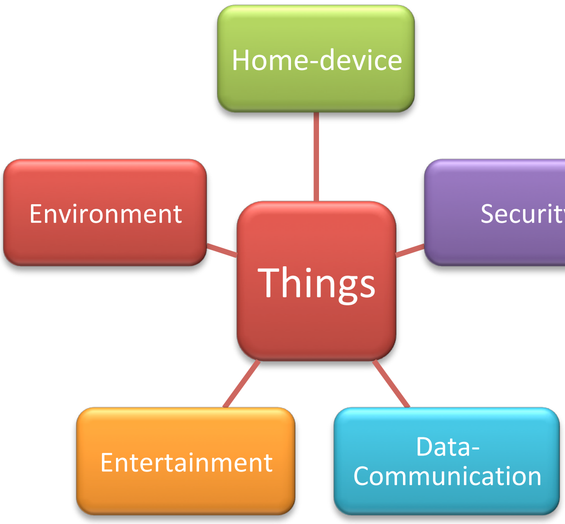


Figure 2.7:Top-level structure of Smart Home domain ontology
(Tao et al., 2018)

The home services corresponding to home-device include automatic cooking and cleaning, household environment monitoring, surveillance, etc., to make daily home life convenient, as well as improving efficiency and implementing energy saving policies (Tao et al., 2018).

Environment services are mainly related to managing temperature, humidity and lighting by providing automatic adjustment and adoption or remote control of air conditioning, lights, gas, and other unnecessary appliances running in standby mode or being turned off in the case of leaving the house.

The entertainment services include providing various audio-visual feasts for the householder at any time, automatically recording family television (TV) programmer preferences, and quickly accessing into the network for interactive services etc. (Tao et al., 2018).

Security services are mainly related to raising alerts and delivering them to the householder via the phone or Internet and triggering relevant solutions to protect home safety when there are abnormal home situations besides supporting a high abstraction level for dealing with security objectives in the process of interactions/ interoperations (Tao et al., 2018).

The data-communication services mainly encompass data sharing between the home and external services via Internet, and data exchanging between the home devices via short-distance exchanging between the home devices via short-distance wireless communications technology etc.

2.4 Applications Common to Smart Homes

A comprehensive literature review on IoT applications in Smart Homes was conducted by Alaa et al. (2017), and the taxonomy adopted is presented in Figure 2.7 below on IoT-based Smart Home applications. Based on the review done by Alaa et al. (2017) from 229 articles published between 2010 and 2016 from three databases namely, Web of science, Science direct and IEEE explore, the taxonomy of literature presented Figure 2.7 below gives a diverse focus in terms of what constitutes Smart Home applications.

The main services provided by Smart Homes are listed by Fabi et al. (2017) as :-

- Detect health conditions – eldercare, healthcare and childcare
- Store and retrieve multimedia from Smart Home - entertainment
- Surveillance – security.
- Devices monitor and control – energy efficiency

2.4.1 Home automation

A key application area for Smart Home solutions is home automation, and that ranges from different aspects in the Smart Home environment. As highlighted by Pienaar, Fisher, and Hancke (2015) and (Ashibani, Kauling, and Mahmoud (2017), home based automation powered by smart phones allows control over home electrical devices (e.g. Geysers, TV, Radio, Lights, etc.) in an embedded environment portrayal. As summed up by Ashibani et al. (2017), IoT devices are providing a wide range of services for Smart Homes such as surveillance cameras, smart lighting, and door locks.

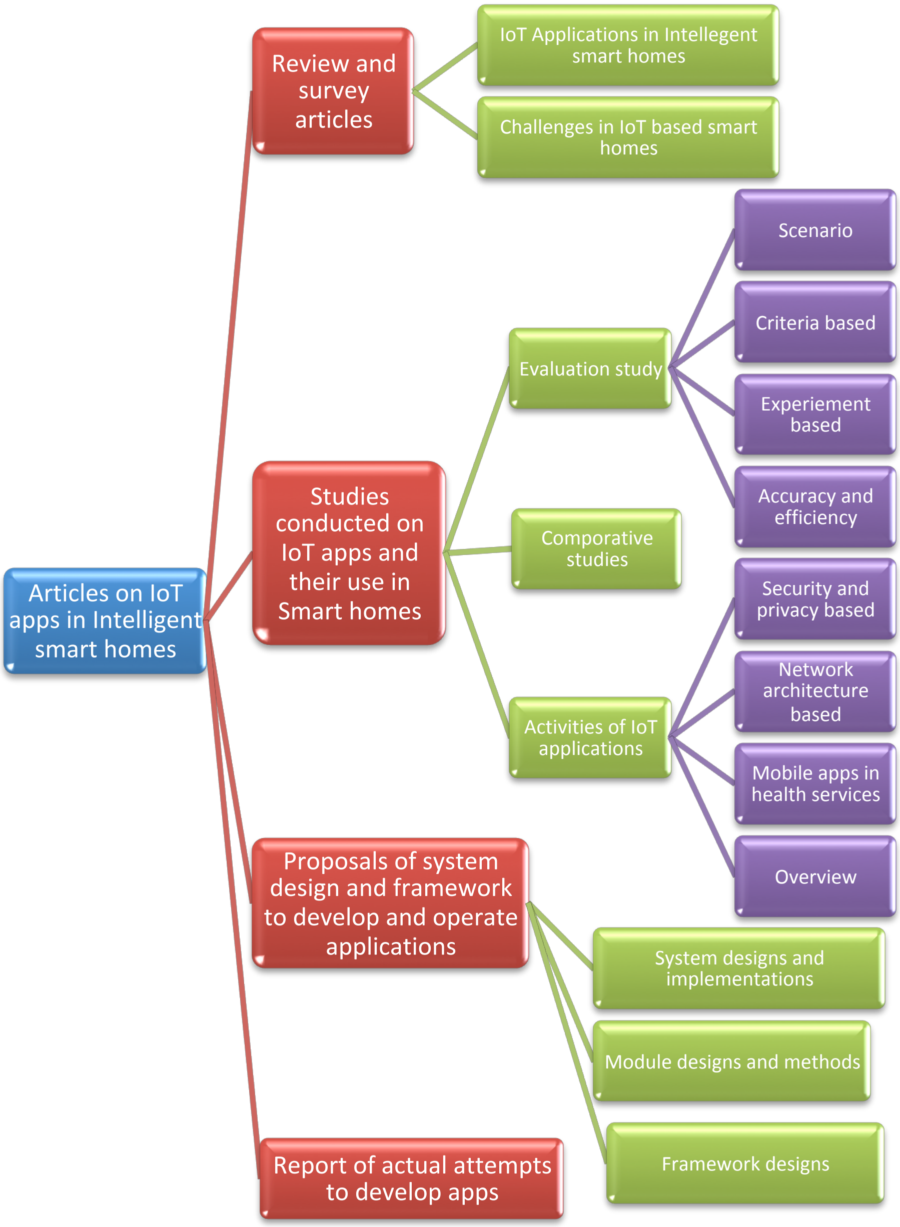

Articles on IoT apps in Intelligent smart homes
Review and survey articles
IoT Applications in Intellegent smart homes
Challenges in IoT based smart homes
Studies conducted on IoT apps and their use in Smart homes
Evaluation study
Scenario
Criteria based
Experiement based
Accuracy and efficiency
Comporative studies
Activities of IoT applications
Security and privacy based
Network architecture based
Mobile apps in health services
Overview
Proposals of system design and framework to develop and operate applications
System designs and implementations
Module designs and methods
Framework designs
Report of actual attempts to develop apps

Figure 2.8: Taxonomy of literature on IoT-based Smart Home applications
(Alaa et al., 2017)

The design thereof is at the backdrop of improving physical security via remote control in a setup that mimics a normal activity based home environment even when the inhabitants are physically absent (Pienaar et al., 2015).

A more precise application is highlighted by Brenkus, Stopjakova, Zalusky, Mihalov, and Majer (2015) through the smart wall power outlet which enables intelligent home power metering system capable of measuring power consumption and transferring the data wirelessly through the low energy integrated Bluetooth transmission. Smart plugs are one of the fast emerging IoT devices finding their way in home automation and making remote monitoring and control of Smart Homes easier (Ling et al., 2017). As an example demonstrated by Ling et al. (2017), one can turn on the heater with their smart phone even before getting home, because of the smart plug capability; however, this doesn't come cheap as there are security challenges to some of the available brands on the market, which was the main focus of Ling et al. (2017).

2.4.2 Energy management applications

The advent of IoT technology gave birth to more Smart Home appliances such as air conditioners, washers, and refrigerators, which are being deployed to provide more advanced services to residential consumers, which is expected to result in significant increases in residential energy consumption (Joo & Choi, 2017).

Energy management systems are also prevalent among applications in Smart Homes as supported by Al-Ali, Zualkernan, Rashid, Gupta, and Alikarar (2017). By monitoring and controlling energy consumption, IoT is enabling ubiquitous capabilities for appliances. This gives inhabitants of the Smart Home the cost saving edge. Combining activity detection mechanisms gives birth to applications that can control Heating, Ventilation and Air Conditioning (HVAC), lightning systems and AAL (Skocir, Krivic, Tomeljak, Kusek, & Jezic, 2016), which is one of the possible applications that a smart living space will need to be equipped with.

Many approaches on temperature control have been advanced as outlined in scenarios where the use of IoT and fuzzy logic for indoor and outdoor temperature and humidity towards energy saving and setting a more comfortable environment for users is displayed (Meana-Llorián, García, G-Bustelo, Lovelle, & Garcia-Fernandez, 2017).

Monitoring services, where user behaviours are profiled and relevant actions are advanced in light of activity detection are further explained by Park, Hwang, Won, and Park (2016). Some practical examples of activities for monitoring and control as given by Park et al. (2016) are sleeping conditions and preparing a meal; these will be monitored and based on previous learnt patterns and appropriate support actions will be executed.

Helping users to visualise household electricity consumption in real time has an important role on improving the household electricity efficiency and changing users' habits of using electricity (Fan, Qiu, Liu, Zhu, & Han, 2017). As further supported by Fabi et al. (2017), besides informing users about their environment, Smart Home Systems (SHS) should also provide some control where applicable. As an example, Fabi et al, (2017) postulate that energy either cooling, heating, conditioned air and lighting, should be available when only needed by the users, otherwise they should be off to cut costs.

2.4.3 Health care based applications

As postulated by Fanti, Faraut, Lesage, and Roccotelli (2016), home health care through AAL solutions can be considered as core. The need to have accurate sensor data for the purposes of establishing AAL solutions is therefore mandatory. Mano et al. (2016) proposed the use of patient images and emotional detection to assist patients and elderly people within an in-home health-care context.

Telemedicine is another key application attributable to Smart Homes (Roy et al., 2017), where monitoring of chronic illnesses for homebound patients can be advanced. This offers in-home patients monitoring and ubiquitous monitoring as demonstrated by Hofer, Schumacher, and Bromuri (2015) through their personal health system dubbed Computerised Model for Predicting and Analysing Support Structures (COMPASS), which, empowered by interoperability protocols, make use of mobile devices for the collection, analysis and subsequent transfer of sensed data to the set observation repository. The architecture of COMPASS is a client-server setting with a publish/subscribe mechanism, dynamic updates of machine learning models and Representational State Transfer (RESTful) services to perform the create, read, update and delete operations (Hofer et al., 2015).

2.4.4 Home safety and security applications

Smart Home environments as defined by Iinatti, Member, and Ha (2017) can visually be portrayed as an organized and networked collection of heterogeneous components (i.e. be it electronics or appliances) whose defined purpose is to provide smart services seamlessly to the Smart Home owners. The essence of availing convenience is being underscored, yet attached to that functional specification of Smart Home setups is an array of security loopholes that render them a ripe haven for different possible attacks of varying magnitudes as they interface directly with personal and sensitive data (Shin et al., 2017; Batool, Saqib, & Khan, 2017; Hossain, Noor, & Hasan, 2017).

Some of the key applications highlighted from literature for Smart Homes are intrusion and detection systems as presented in Daramas, Pattarakitsophon, Eiumtrakul, Tantidham, and Tamkittikhun (2016), where an Android application for monitoring, configuring and notification remotely is demonstrated. Home owners are promptly notified of any unusual events on their mobile devices, equipping them with the ability to advance instant action despite being physically absent from their own premises, thereby increasing the security of their homes by the click of a button (Daramas et al., 2016).

To improve security and safety for home assets, the Home Automation system for Intrusion Detection (HIVE) has been developed by integrating a set of intrusion sensors and actuators and IoT technology (Daramas et al., 2016).

2.5 Smart Home Challenges

The enabling environment for a Smart Home as a key towards the fundamental industrial and commercial envisaged test bed for IoT, Smart Grids as well as 5G connectivity (Silverajan, Luoma, Vajaranta, & Itapuro, 2015) is being fuelled by IoT (Ren, Song, Yang, & Situ, 2016). Commercial vendors are introducing health care, home automation and remote monitoring (Silverajan et al., 2015). These key facts about a Smart Home point to the fact of a delicate and an underdeveloped domain. Due to the infancy nature of the Smart Home domain, many of the solutions are on trial and not yet fully developed. On the other hand, the future projections into the growth of Smart cities (Saxena, Choi, & Lu, 2016; Paek, 2015) can be honoured if the critical arms to the Smart cities hub are given proper attention; hence Smart Homes are a critical component towards the wider Smart cities project.

The slow adoption of Smart Home solutions as supported by Hui et al. (2017) can be attributed to the high cost, difficult installation and unfriendly operations. The study done by Ford, Pritoni, Sanguinetti, and Karlin (2017) analysed 308 Home Energy Management (HEM) products and identified opportunities for energy savings; however, such potential benefits that are related to convenience, comfort or security may limit the realisation of savings. A balance between energy efficiency and the occupant's needs is required (Fabi et al., 2017). As also highlighted by Fabi et al. (2017), the Smart Home drivers and social barriers for the establishment of Smart Homes can be the willingness to pay, which is affected by:-

- Expected savings
- Perceived usefulness of consumption feedbacks
- Environmental awareness
- Intention to change user behaviour
- Trusting data protection – privacy issues

The gap in today's technology design in Smart Homes is the understanding of consumers' behaviour and the integration of this understanding into smart technology (Bhati, Hansen, & Chan, 2017). Worth noting are the highlighted major barriers to home automation by Fabi et al. (2017), which are listed as:-

- Losing control
- Reliability
- Viewing Smart Home technology as exclusive or irrelevant
- High installation costs

The Smart Home usually requires the integrations of many heterogeneous sensors and service applications in deployment and realisation (Seo et al., 2016). As further supported by Hui et al. (2017), device interworking is still one of the major challenges in IoT due to lack of standards. IoT is paving the way to many possibilities for the connected world, but there is a great challenge of vulnerabilities that already exists in the digital space and constant cyber-attack threats (Moskvitch, 2017). As outlined earlier, traditional usage and connectivity of Internet setups continue to play a significant role (Silverajan et al., 2015), thus the continual security challenge for Smart Home environments will prevail.

Different proprietary standards for WSNs are being proposed at the same time from the industry, such as WEAVE protocol from Google and Home Kit from Apple, but this may take a long time to converge to a globally acceptable protocol for SH and IoT (Hui et al., 2017).

The main concern on Smart Homes by users is related to the invasion of the domestic privacy, and too intrusive technologies (Fabi et al., 2017). One of the challenges noted by Smirek et al. (2016) is the lack of appropriate user interfaces to cater for heterogeneous user groups, which might also explain why privacy issues continue to be a hot button, hence the widespread adoption of Smart Home solutions has not taken place. Moreover, there is always a conflict between privacy awareness and context awareness. User intervention to balance the two could be the way out but the result will be a downgrade of autonomy (Hui et al., 2017). The other challenge also highlighted by Smirek et al. (2016) is the low interoperability between different Smart Home systems, which creates a disjoint setup for properly addressing security issues.

A major problem with some implemented Smart Home solutions is that they cannot flexibly accommodate the existing remotely controlled aftermarket appliances (Lin, Lin, Hsiao, & Wang, 2017). IoTtalk remote control (IoTtalk-RC) is a mechanism advanced by Lin et al. (2017) that utilises sensors as universal software-defined remote control for aftermarket home appliances. The complexity escalates when there are multiple owners in a single home space where multiple but different rules must be applied at the same time, in the same place, for the same things (Hui et al., 2017).

The Smart Home concept associated with the pervasiveness of network coverage and embedded computing technologies is assuming an ever-growing significance for people living in the highly developed areas. However, the heterogeneity of devices, services, communication protocols, standards and data formats involved in most of the available solutions developed by different vendors is adversely affecting its widespread applications (Tao et al., 2018).

2.6 The Future of Smart Homes

Artificial Intelligence (AI) gaining momentum and one of the key requirements for future Smart Home designs is outlined in the work of Chiang, Lu, and Hsu (2017). The possibility of sharing knowledge created from one Smart Home environment to the other is therefore a feature to consider. This is why any Smart Home solution should take into account how to effectively incorporate AI as proposed by Hui et al. (2017), that Human-to machine (H2M) interaction has become another part of Internet communication where machines get smarter with AI as things are becoming smarter, computerised and connected to the Internet. Therefore, easy setup process or auto-setup will be the ultimate goal for non-technical users when SH technology becomes more mature (Hui et al., 2017). Other than location recognition, emotion recognition based on effective computing is also an interesting field catching researchers' attention under the umbrella of Activity recognition (Hui et al., 2017).

Future Smart Home services with IoT technologies can have economic advantages and expandability by presenting easy accessibility to wireless networks, as well as the compatibility of various operating systems, languages and frameworks (Joo & Choi, 2017). This will positively contribute to the new phenomenon of Industry 4.0 (Hui et al., 2017) which is now a popular term in Germany as "Industri 4.0 ", already being advanced in smart grids for energy saving for homes and businesses based on the power grid to collect usage data from appliances.

Consumer-centric applications suggest the need for smart grid technologies to implement intelligent systems such as HEMS to offer efficiency and economic control of home applications (Joo & Choi, 2017). The Internet will disappear since nobody will notice the existence of the connection in the IoT world (Hui et al., 2017).

Cherry, Hopfe, MacGillivray, and Pidgeon (2017) explored the socio-technical imaginaries of a low carbon housing future, which is meant to reduce carbon emissions to zero. They paid particular attention to the links between the visions of the future and the publics that inhabit them. In their paper Cherry et al. (2017) explored expert derived visions of a low carbon housing future with members of the public themselves, investigating their acceptability alongside the values and concerns which shape their perceptions of these possible futures.

IoT frameworks for SH should support alternatives to current closed manufacturers' cloud like actor or data flow models in which applications can be distributed to and instantiated in a simple way using asynchronous messaging (Hui et al., 2017).

Future Smart Homes will reflect the full range of a new group of users who would precisely demand personalised user interfaces that take the individual user requirements and preferences into account (Smirek et al., 2016).

2.7 Taxonomy of IoT Security

The taxonomy of IoT security as presented by Yaqoob et al. (2017) gives a clear cut overview of the entire landscape from threats, to key security requirements and some important standards to be considered. This gives a starting point for looking at the security solution requirements for IoT as presented in Figure 2.9.

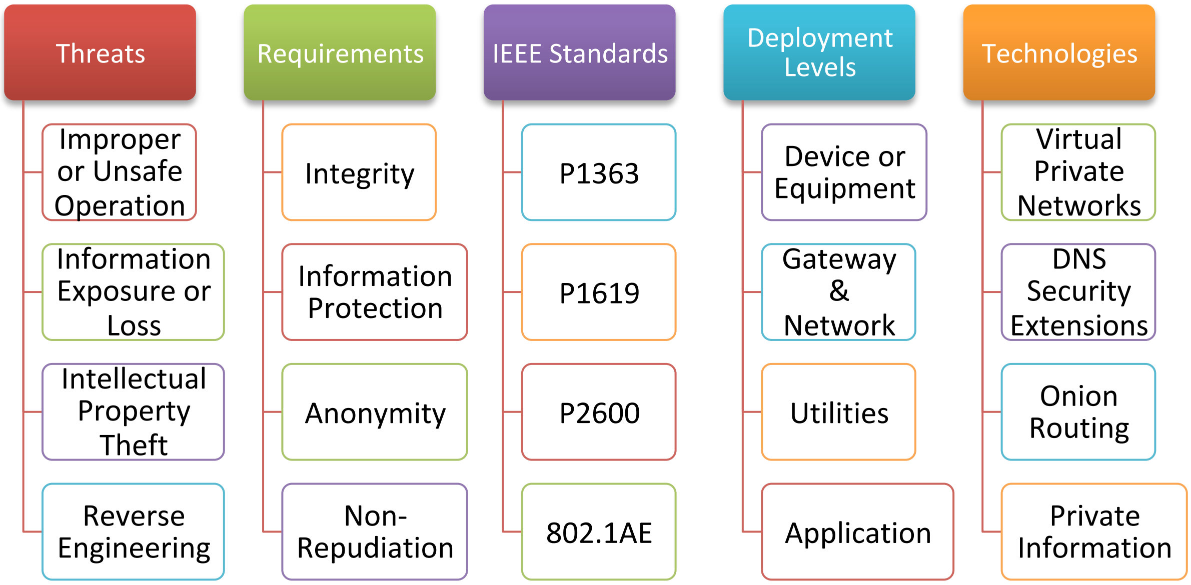


Figure 2.9: Taxonomy of IoT Security
(Yaqoob et al., 2017)

2.8 Security Threats Towards Authentication

IoT security has become a cause for concern as a result of the increased number of resource constrained smart devices which are not architecturally designed to employ robust security techniques on them (Majeed, 2017). As further expressed by Gu and Liu (2017), the challenges emanate from existing authentication schemes for IoT devices which include: pre-distributed authentication keys which are not feasible, and manual pairing, which requires more user effort especially when dealing with many IoT devices and context-based solutions, which are mostly peer-to-peer instead of being scalable. As summarized by Khemissa and Tandjaoui (2016a), IoT's obstacle towards their deployment rests on the authentication of different interconnected entities, and exchanged data confidentiality are the top concerns that need to be addressed.

Authentication can be viewed as the first line of security by ensuring the enforcement of security measures at level 0 (Crossman & Liu, 2016). The process of authenticating the various processes, applications and objects require a handshake that can be done before authorization is granted. The computational limitation and overall capacity nature of IoT devices makes it a challenge to apply conventional security techniques (Sharaf-Dabbagh & Saad, 2016). Another key challenge as highlighted by Shen, Li, Sahin, and Choi (2016) is that authentication that makes use of the public key system is not pliable under IoT application environments due to some of the reasons cited by Sharaf-Dabbagh and Saad (2016), which are computational limitations and the portable nature of IoT devices.

2.9 Security Threats Peculiar to IoT

The main security issues in IoT as highlighted by Sicari et al. (2015a) are interdependent on authentication in one way or the other. Access control requires authentication to grant permission to the required resources or services. Before trust can be extended among communicating parties, these parties need to be authenticated against the set privileges and access rights. As supported by Li, Yan, and Chang (2018), the IoT paradigm has many security and privacy challenges involving authentication and authorisation, data and personal information confidentiality, and secure communication and computation.

2.9.1 Authentication specific related threats

As highlighted by Cheng, Shenwen, Yingbo, Na, and Xuren (2015), loss of basic privacy, tracking, cloning, eavesdropping, physical attacks and denial of service attacks, are some of the surfacing threats for IoT authentication.

The work of Arafin, Gao, and Qu (2017) proves that some of the authentication schemes can be their own threats in their bid to provide authentication solutions. We witness a demonstration of the Voltage Over Scaling (VOS), a technique that operates on the basis of a computation process to produce a two-factor authentication scheme after profiling the error signature and gaining information of the underlying procedures whose variation was then combined with security key based authentication protocols. This approach effectively capitalized on the error by methodically profiling it to gain knowledge of the underlying process variation for computation purposes, hence providing a unique key authentication approach that employs hardware process variations.

A cloud based RFID authentication scheme presented by Karthi and Harris (2016) was targeting reader impersonation attacks and tag location tracking attacks hence it was aimed at providing tag location privacy. In a similar research done by Kaur, Kumar, Singh, and Obaidat (2016), it was concluded that identity revelation, information leakage, tracking and spoofing are typical to RFID systems which are defenceless against any varied nature of attacks, either active or passive. They suggest that Elliptical Curve Cryptography (ECC) has the ability to establish mutual authentication among the tags and servers, at the same time protecting them against eavesdropping, cloning risks and replay tracking attacks (Kaur et al., 2016).

Since most IoT devices are likely to be directly connected to the Internet while being battery powered for some, they are particularly vulnerable to DoS attacks specifically aimed at quickly draining battery and severely reducing device lifetime (Gehrmann, Tiloca, & Hoglund, 2015). The proposed Short Message Authentication Check (SMACK) offered an early detection mechanism by swiftly picking invalid messages upon reception and validated them against the lightweight message authentication code (Gehrmann et al., 2015), which was an initiative to address the DoS threats of this nature.

Some of the key highlighted potential attacks on user authentication protocols as tested against the RRAM based lightweight user authentication work of Arafin and Qu (2016) are as summarised in Figure 3.2.

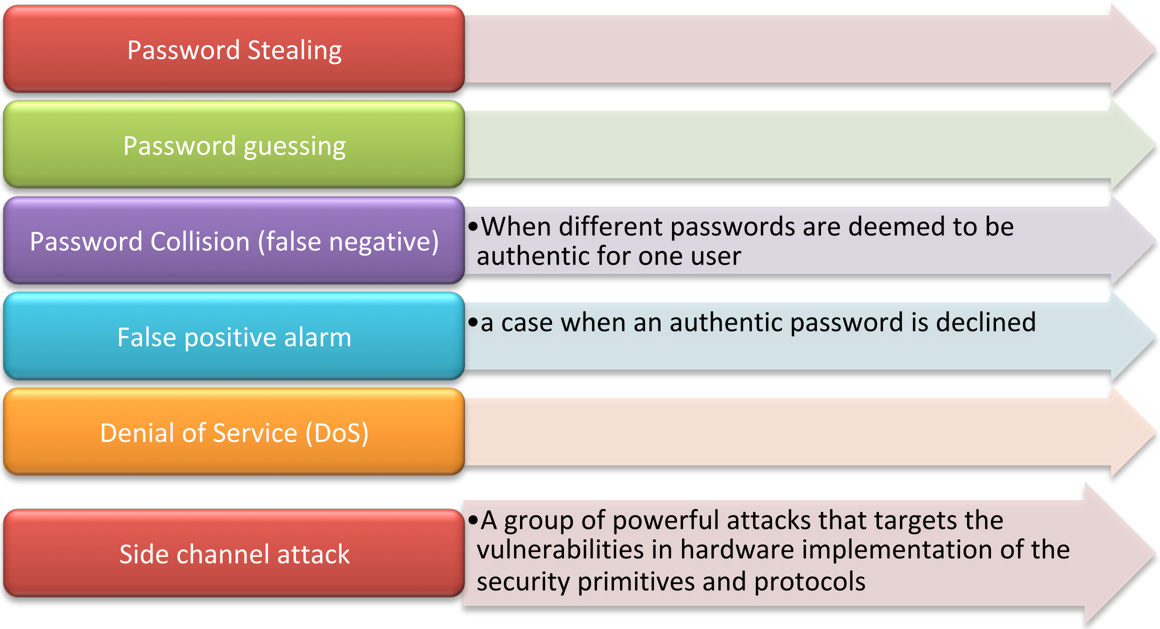

Password Stealing
Password guessing
Password Collision (false negative)
•When different passwords are deemed to be authentic for one user
False positive alarm
•a case when an authentic password is declined
Denial of Service (DoS)
Side channel attack
•A group of powerful attacks that targets the vulnerabilities in hardware implementation of the security primitives and protocols

Figure 2.10: Potential attacks on user authentication
(Arafin & Qu, 2016)

Light weight mutual authentication alternatives which are capable of providing data confidentiality are proposed by (Griffin, 2015), which make use of authentication key exchange to defend against phishing and similar attacks. As highlighted by Mbarek, Meddeb, Ben Jaballah, and Mosbah (2017), security vulnerabilities of lightweight authentication mechanisms and their inability to tackle memory DoS attacks motivated the work on an improved scheme derived from the streamlined Timed Efficient Stream Loss-Tolerant Authentication (µTESLA), referred to as X –µTESLA.

2.10 Threat Landscape for Smart Home Applications

In general, the threats inherent to IoT devices anywhere else are typically the same threats one would find in a Smart Home setup. The Smart Home domain may have setbacks of not having formal security design setups and that mainly depends on the expertise level of the inhabitants. If at manufacturer level certain devices don’t have robust security solutions embedded in them that will contribute to the vulnerabilities that a Smart Home domain is likely to suffer.

For consideration of a threat landscape for the purposes of this study, the Dolev-Yao attack model (Dolev & Yao, 1983) is considered. The possible attacks such as eavesdropping, message injects, replay, spoofing, insider and outside attacks are all deemed possible actions by the attacker. These attacks may be perpetrated with the motive to gain access to sensitive data, gain unauthorised control of Smart Home devices and propagate denial of service and service degradation.

The availability of IoT devices in a Smart Home enables human identification, tracking and profiling via the physical environment without their consent (Yaqoob et al., 2017, P. 454).

2.11 Security Threats Towards Smart Home Applications

The reason why we need to zoom further into authentication threats, which are specific to Smart Homes, is the unique nature of the domain of application. Generalizing authentication threats to IoT will not give a clear picture as to which ones are more prevalent under certain domains and not other domains. The picture painted in Section 2.2, of a Smart Home, is one that entails the need to contextualize the threats so that they can be effectively handled. As indicated in Section 2.8, some similarities are picked too under this section, validating our claim that security threats that are peculiar to IoT in any domain are still the same threats to be handled under a different domain as long as we have IoT in use, but maybe at a different level.

The control of Smart Homes is being made possible through mobile devices which can access the Internet (Ren et al., 2016), but they can easily be compromised if the very devices are not secured properly, causing an extension of the attack vector, hence possible threats to authentication thereof.

By reverse engineering a smart plug and advancing a unique set of attacks Ling et al. (2017) proved that they can effectively and efficiently obtain a victim’s authentication credentials. By exploiting the communication protocols, device scan attacks, brute force attacks, and spoofing attacks, and firmware attacks were performed. As presented by Ling et al. (2017), where they performed a case study on a smart plug system with a typical gadget in a Smart Home environment, the following vulnerabilities were picked:- insecure communication protocols, and lack of device authentication.

The Smart Home scenario is replete with smart devices that have the capability of interconnecting among themselves, making the whole security design in such an environment equally a challenging task. General security solutions cannot directly be advanced towards IoT application domains as a result of the existing unique standards and communication stacks as well as limited computing power (Sicari et al., 2015). A compromised sensor can push notification to the users' phone or peers' sensors and collect sensitive data from them (Yaqoob et al., 2017).

Malware is a typical threat that can be directed towards personal data in a Smart Home environment if the sensors present a weak authentication structure. Therefore, authentication mechanisms need to be looked at in order to address unauthorized users and devices from accessing data they are not privileged to access (Sicari et al., 2015).

To add on to the list of attacks Shen 2016) highlight the following:- insider attacks, impersonation attacks, man-in-the-middle attacks, reply attacks and unknown key sharing attacks which are presented as some of the prevalent authentication threats that need serious considerations when designing security solutions. IoT devices are vulnerable to sophisticated security attacks such as man-in-the middle attacks, as proffered by Kim, Yoo, and Yoo (2015).

In a Smart Home setup, the user's privacy information is at risk as a result of low security strength. The magnitude of the risk extends to accessing such private information by strangers as well as other malicious entities, for example eavesdroppers who can gather and aggregate the traffic information to profile a household (Song et al., 2017).

Attacks for rolling-code garage door openers simply synchronize the malicious remote with the existing remote control signals, and this requires only a few minutes or simply brute forcing the code or physical attack (Margulies, 2015). The approach by most manufacturers of having a centralized authentication, authorization and commands is to reduce the demands of the inevitable tech calls (Margulies, 2015), which eventually becomes a key threat to authentication. The main reason being that, the cloud platform opens new doors to a range of attack vectors; instead of attackers having one target, they end up having mass attacks of the same model and brand at a go (Margulies, 2015), especially during software updates where attackers can gain control of the whole system.

The diversity of the Smart Home devices causes many security and privacy challenges during their usage (Ren et al., 2016). Authentication based on fingerprint identification is still dangerous when it is defrauded with the fingerprint film (Ren et al., 2016).

2.11.1 Classification of IoT Authentication threats and attacks in Smart Homes

Now that Section 2.11 has unveiled the threats that are specific to IoT in Smart Homes, it is logical to classify them accordingly into the following key classes: -

- Device layer,
- Network layer, and
- Application layer.

These classifications are based on the key features of IoT devices as they are functionally positioned under various application scenarios as presented in Table 2.1, as Device level; Network level, and Application level. These three classifications are based on the 3-layer model for IoT which correlates to the perception, network and application layers (Ge, Hong, Yusuf, & Kim, 2018). The threats are presented as sources of potential weakness areas that attackers can capitalize on to gain unauthorized access to data or information that is key to the overall security of IoT devices in a Smart Home environment. The classification of attacks is done in two parts, considering data in transit and data at rest, as there is generally an oversight on the different states of data, which can be compromised at varying magnitudes. The examples given for each category of attacks is not an exhaustive list of the various attacks.

Table 2.1: Classification of authentication threats and attacks

	Threats	**Attacks**	
		In transit	*At rest*
Device Level	Limited resources Architecture Interfaces Software	*Firmware* *Brute force* *Defraud* *DoS*	*Firmware* *Physical* *Credentials*
Network Level	Architecture Openness Protocols	*Eavesdropping* *Device scan* *Spoofing* *Man-in-the middle* *Reply* *Unknown Key sharing*	*Device Scan* *Brute force*
Application Level	Interactions Constraints Environment Human	*Impersonation* *Malware* *Insider*	

2.11.2 Device level security threats

The device-level IoT security vulnerabilities summarized in Figure 2.11, are an indication of the varied nature of worries around IoT devices, hence the authentication of such devices is already at risk from various angles. There is no doubt that IoT security incidents based on a varied nature of configurations are susceptible to different risk magnitudes (Mohsin, Sardar, Hasan, & Anwar, 2017). Henceforth the risk level at device level still has a substantial stake towards the overall security worries for IoT applications.

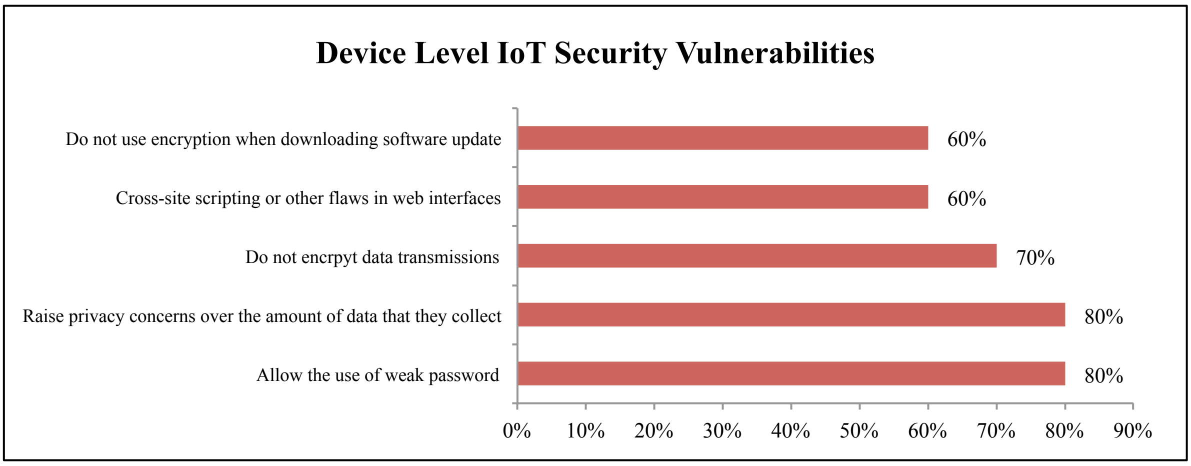


Figure 2.11:*Device-level IoT security vulnerabilities adopted from* (Tankard, 2015)

In addition to what is presented in Figure 2.11, devices such as sensors or embedded RFID tags are prime targets for the attackers. Attackers either replace or modify the device software to achieve their own illegal purposes by exploiting devices (Li, Xu, & Zhao, 2015a). The main security threats highlighted at data perception level as highlighted by Yaqoob et al. (2017) are summarized in Figure 2.12.

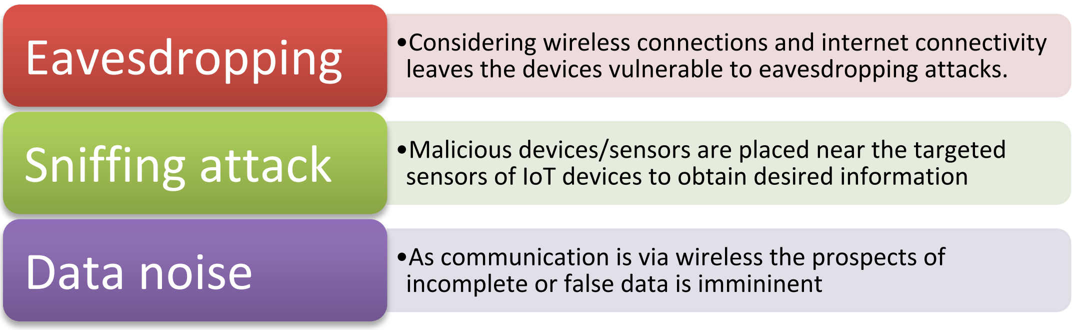
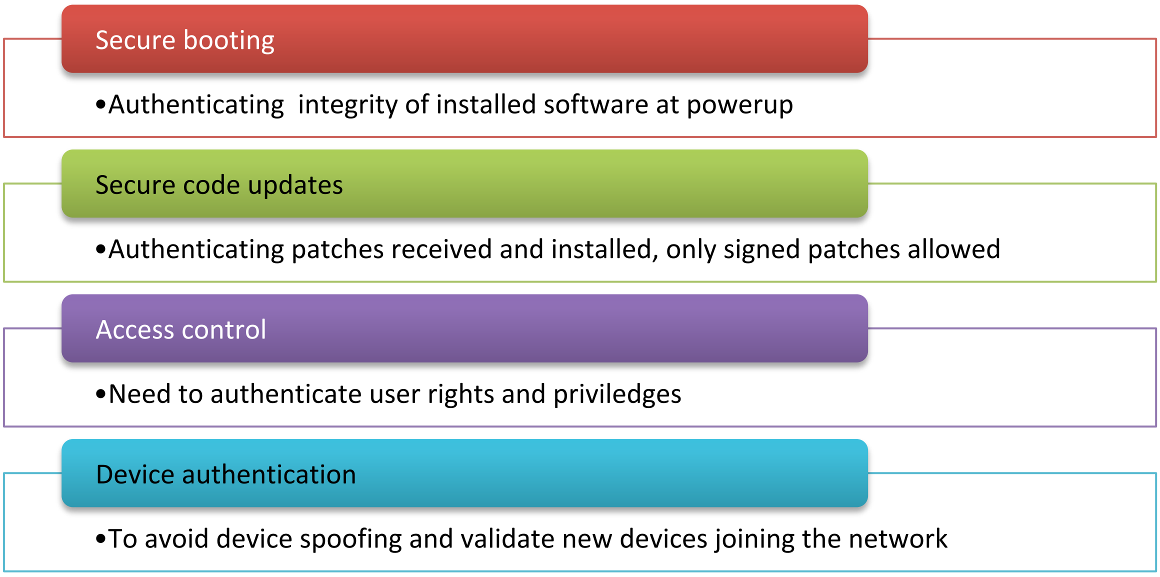

Eavesdropping
•Considering wireless connections and internet connectivity leaves the devices vulnerable to eavesdropping attacks.
Sniffing attack
•Malicious devices/sensors are placed near the targeted sensors of IoT devices to obtain desired information
Data noise
•As communication is via wireless the prospects of incomplete or false data is immininent

Figure 2.12: Security threats at data perception level

Device Level Security requirements: as this level comprises the involvement of people, things and places, the process through which devices perform their operations and interact with people needs to be secured. As summarized in Figure 2.13 below, some of the key requirements at device level are highlighted.



Secure booting

- Authenticating integrity of installed software at powerup

Secure code updates

- Authenticating patches received and installed, only signed patches allowed

Access control

- Need to authenticate user rights and priviledges

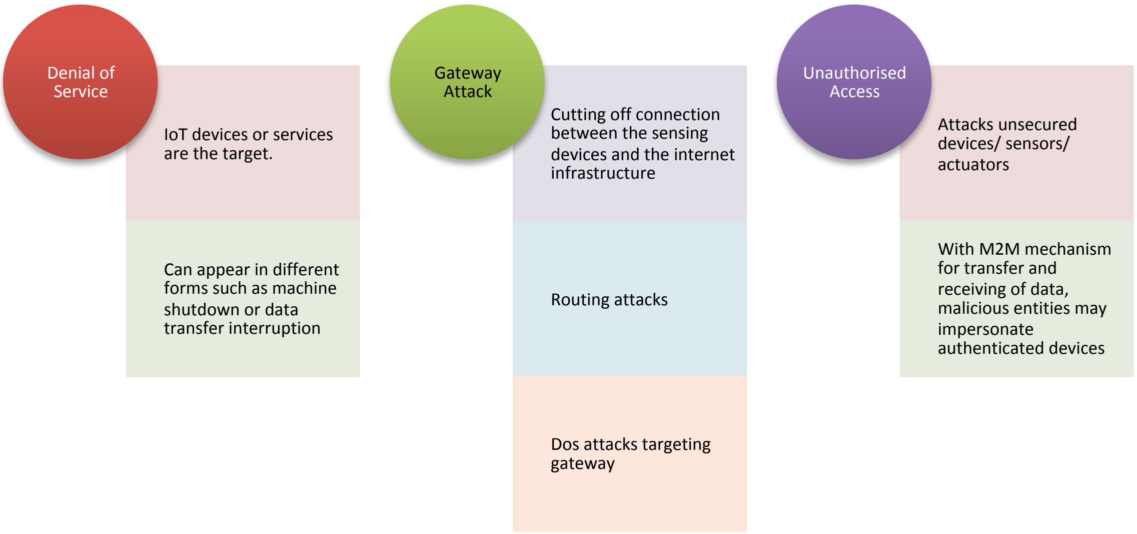
Device authentication

- To avoid device spoofing and validate new devices joining the network

Figure 2.13: Device level security requirements

2.11.3 Network level security threats

Also considered at the data transmission layer, the typical threats highlighted by Savola, Abie, and Sihvonen (2012), Yaqoob et al. (2017) and Kanuparthi, Karri, and Addepalli (2013) are summarized in Figure 2.14 below.



Denial of Service

IoT devices or services are the target.

Can appear in different forms such as machine shutdown or data transfer interruption

Gateway Attack

Cutting off connection between the sensing devices and the internet infrastructure

Routing attacks

Dos attacks targeting gateway

Unauthorised Access

Attacks unsecured devices/ sensors/ actuators

With M2M mechanism for transfer and receiving of data, malicious entities may impersonate authenticated devices

Figure 2.14: Device transmission security attacks

At the network layer, the interaction worth considering is between the devices or sensors and the Internet. There is physical intrusion and limited functional redundancy (Yaqoob et al., 2017) at this level, henceforth the key security concerns for focus are:-

- Malware and intrusion protection - the need to apply access control lists and filtering is therefore, needed; and
- Ensure message integrity through hash functions and verification protocols.

2.11.4 Application level security threats

Application program attacks which can cause an inability to receive security patches, malicious code attacks and tampering with node-based applications (Yaqoob et al., 2017) are prevalent at this level. A more detailed review of security threats is presented by Li et al. (2015a) where four layers are presented and the top 10 security concerns are highlighted. Table 2.3 below is an adaption of the representation. From the representation in Table 2.3, it can be noted that the security threats, vulnerabilities and requirements for IoT devices have varying magnitudes of impact; however, authentication/authorization has a universal effect on all the presented layers.

Table 2.2: Security concerns in IoT
(Li et al., 2015a)

Security Concerns	Interface Layer	Service layer	Network Layer	Sensing layer
Insecure web interface	✔	✔	✔	
Insufficient authentication/ Authorization	✔	✔	✔	✔
Insecure network services		✔	✔	
Lack of transport encryption		✔	✔	
Privacy concerns		✔	✔	✔
Insecure cloud interface	✔			
Insecure mobile interface	✔		✔	✔
Insecure security configuration	✔	✔	✔	
Insecure software/firmware	✔		✔	
Poor physical security			✔	✔

Dealing with device interactions involved in acquiring data from IoT devices and sending control commands (Yaqoob et al., 2017), the security requirements to be addressed at this level therefore are:-

- Non- repudiation – there is need for an audit trail of the changes
- Dynamic auditing mechanisms should be implemented.

2.12 IoT Authentication Overview

Authentication is among the top vital aspects for consideration towards the design of secure IoT communication. Authentication can be rendered as the first phase towards access control, and it can be device authentication or user authentication (Shaju & Panchami, 2016), or even more. However, the provision of a lightweight, bulletproof and distributed authentication scheme for total security solutions towards IoT applications remains one of the biggest challenges (Mahalle, 2013). Device authentication is critical and a very challenging task for the emerging IoT (Chen et al., 2017).

There are three security layers for IoT, which can be summarized as perception layer, network layer and application layer (Zhao & Ge, 2013). These security layers correspondingly correlate with the three security dimensions of the IoT security architecture, which entail information security, physical security and management security (Zhao & Ge, 2013). Authentication should be the initial handshake security level that has to grant access rights to pieces of data around the Smart Home environment. This is corroborated by Zhao and Ge (2013), who argue that "IoT should have these characteristics: comprehensive perception, reliable transmission, and intelligent processing" (p., 664).

Detailed review work and the classification of different authentication techniques for IoT was carried out by Saadeh, Sleit, Qatawneh, and Almobaideen (2016); building on that work, this section highlights and populates on some of them, highlighting some of the recent schemes as well. As Saadeh et al. (2016) quote Granjal, Monteiro, and Sa Silva (2015), as well as Li, Xu, and Zhao (2015b), that there is a general agreement that traditional TCP/IP protocols such as HTTP, TCP and IP are not efficient in supporting machine to machine (M2M) communication. This shows that for IoT authentication solutions to work, there has to be specific functional and technical refinement of existing solutions in a contextual approach as guided by their implementation.

The constrained nature of devices and critical security concerns of IoT applications, sensor-based and wireless systems will demand novel solutions towards system design, network design and data processing procedures (Lin & Wen, 2016). This is further supported by Nguyen and Iacono (2016) in their REST-ful Constrained Application Protocol (CoAP) message authentication scheme whose overarching goal through the establishment of a message-oriented security layer for CoAP was to address the specific challenges stemming from the architectural style of REST and the resource constrained nature of IoT networks and devices. For proving trustable services, Lin and Wen (2016) explored the possibility of developing a node-based identification protocol by striking a balance between energy consumption versus malicious node detection in a heterogeneous IoT setup.

As summarized by Kim et al. (2015), the key operations for authentication as observed from Denning, Kohno, and Levy (2013), Kothmayr, Schmitt, Hu, Brünig, and Carle (2013), and Saied et al. (2014), are:-

- Key establishment,
- Message authentication code, and
- Handshake.

It can therefore be highlighted that these are the three vital ingredients for effective authentication.

A close look at various solutions presented and applied for IoT authentication platforms signals the varied nature of such solutions. Common among the various solutions as covered in this section, despite the domain of application, is their lightweight nature, which of course has varying degrees depending on areas of implementation.

The first selection on lightweight IoT authentication schemes in general has been randomly done on the following key categories: -

- Two-factor authentication based,
- Use of pseudonyms,
- Hardware and bio based,
- Network based,
- Physically Unclonable Function (PUF) based,

- Three-factor authentication based, and
- Cloud computing application focused.

These were general trends observed from recent work on lightweight authentication schemes. The second selection on lightweight IoT authentication for Smart Home applications were mainly populated based on a random selection which satisfied the condition, A = {IoT, Lightweight, Authentication, Smart Home}.

2.13 Comparison of IoT Authentication Schemes Based on Costing

In this section, the various selected lightweight solutions are compared on the basic architectural attributes of hash functions (x), XOR (y) and concatenation (z). Based on the comparison given in Table 2.4, our recommendation is that the possible authentication techniques to adopt for Smart Home applications are those that do not have high cost but at the same time, they need to satisfy the fundamental security solution requirements as depicted in Section 2.15. The basis for choosing a typical scheme to apply in a Smart Home environment will be the consideration of the device features and the computational capabilities. Most of the IoT devices and sensors finding themselves in Smart Home environments are typically constrained in terms of storage space, computational capacity and memory size.

The costing comparison presented in Table 2.4 is a summary of fifteen (15) different protocols picked from the analysis, which was covered as part of the publication produced from this work, presented in Appendix 3. The selection of the costing values was based on the device level authentication. The reason for considering the device level was mainly on the basis that it is the constrained element in the whole IoT setup for Smart Home applications. Focus was then on the protocols offering the lowest value after summation of the three parameters considered for costing. Further analysis of Table 2.4 is extended to Section 2.17, where a decision is then made based on three lowly costed protocols by Khemissa et al. (2016), Huang et al. (2016) and Shen et al. (2016)'s protocols.

Table 2.3: Device level costing comparison of various protocols

Hash (x)	*3*	*2*	*4*	*2*	*3*	*12*	*7*	*5*	*5*	*5*	*8*	*9*	*2*	*1*	*4*
XoR(y)	*3*	*6*	*5*	*3*	*1*	*6*	*2*	*2*	*3*	*3*	*7*	*8*	*4*	*1*	*6*
||(z)	*2*	*16*	*8*	*1*	*3*	*13*	*5*	*4*	*14*	*16*	*12*	*15*	*6*	*1*	*4*
Protocols	*Zhang(N. Zhang, Wu, Yang,*	*Karthi et al(Karthi &*	*Janbabaei et al(Janbabaei,*	*Khemissa et al(Khemissa &*	*Huang et al(Huang, Juang,*	*Gope et al(Gope & Hwang,*	*Hossain et al(Hossain et al.,*	*Arasteh et al*	*Amin et al(Arasteh, Aghili,*	*Jiang et al(Jiang, Zeadally,*	*Linatti et al(Iinatti et al.,*	*Gope et al(Gope & Hwang,*	*Yang et al(J. H. Yang & Lin,*	*Shen et al*	*Yang et al(Jen-Ho, Ya-Fen,*

2.14 Recommendations for Smart Home Solutions

To guide the choice of solutions for Smart Homes from the comparisons done in Table 2.4, it is ideal to consider all the dimensions of the authentication protocol to be advanced from functional specifications to their resilience towards some known attacks as well as their resource requirements.

It is important to consider the identity of the objects for a holistic authentication solution. Uniquely identifying the objects or things in IoT will help. We strongly believe digital signatures will play an important role in this regard and introducing agent based trusted solutions would enhance the authentication solutions to be advanced to IoT platforms, especially in Smart Homes.

2.15 Synthesis of Literature

As clearly outlined from Section 2.1 to Section 2.13, the various literature reviewed, go deeper in confirming the research gap presented in Section 1.3. Of note is the existence of the challenge to design and secure authentication architectures, incorporating lightweight properties of IoT objects in various applications. As our focus was on smart home applications of IoT, a number of challenges have been highlighted and key to such challenges is the unsupervised nature of interactions among IoT objects.

To outline the focus of this research and mapping the focus area, we paint a picture of a Smart Home that this research worked upon, and then spell out the model(s) adopted for the Smart Home space in this research.

2.15.1 The Smart Home definition

Our adopted definition of a Smart Home will combines Alaa et al. (2017), Seo et al. (2016) and Smirek et al. (2016)'s definitions to give a working definition for this research of a Smart Home as:- **An organised space that implements IoT to provide easy management of the environment to provide services needed either within or outside the space.**

As visually displayed in Section 2.2, Figure 2.2, the Smart Home space considered for this research is as such. The main services considered are Assisted Ambient Living (AAL) environments, which are essentially designed Smart Home applications for a purpose; motivated by the need to avail the best secure data exchange among the various connected devices that eventually render the services needed in such an environment critical.

Closely tied to monitoring ambient living spaces is Energy Saving Solutions (ESS), which ensure the sustainability of the smart spaces. The main concern therefore was on how various interactions among the things in the Smart Home are protected such that there is no unauthorised use of their data.

For AAL spaces, much of the data is very sensitive to the inhabitants like medical and financial records and the need to update their current needs which the sensors and actuators with or without their interaction mainly administer, mostly unsupervised.

The rationale for choosing these focus areas for our study was outlined in Chapter 1, Section 1.8.

2.15.2 Adopted model and services

Two models were picked for informing our Smart Home setup, which are the AAL model (Rawashdeh et al., 2017) and the Home Energy Management System (HEMS) (Joo & Choi, 2017). These models were briefly highlighted in Section 2.2.2 and a framework for AAL was displayed in Section 2.4.3, Figure 2.5.

The reason for picking these models was on the basis that they speak directly to our research focus as outlined in Chapter 1, Section 1.8, and Figure 1.6, which is stated as a focus on a solution that can be applied to constrained resources that have the capabilities to interconnect among themselves, with little to no human intervention.

We highly acknowledge the role played by Cloud computing in the setup of our Smart Home space for this research as poised by Hui et al. (2017), hence its scalability was taken in consideration for modelling the Smart Home setup.

The key services for consideration in describing our Smart Home setup are those espoused by Tao et al. (2018) such as managing temperature, humidity and lightning control, air conditioning, lights and gas remote control, hence the ontology presented in Figure 2.7 was adopted entirely for this research.

What was out of the scope of this research was addressing the inherent challenges involved in setting up and running a Smart Home space. We therefore proceeded on the assumption that such challenges if encountered are well taken care of to a satisfactory level, outside the scope of our research focus. The only challenges our research focused on are those related to authentication towards data security and privacy protection.

2.16 IoT Focus Area

Our focus in this research was based on IoT applications that facilitate the built up, functioning and maintenance of AAL and ESS to give birth to Smart Home setups.

The main IoT devices of focus were the low cost, low powered and constrained devices without much computational capacity. The reason behind this focus domain was to ensure that we were focusing on practical solutions for a wider populace of people that can afford and that can easily be modelled into a viable business model for practical implementation.

The main functionality of the IoT devices for consideration was their ability to sense and transmit their data via the trusted home agent as displayed in Chapter 4.

As our main focus was towards security of data in transit and at rest, the end-to-end authentication on mechanism is advanced in Chapter 4, and takes into consideration the lightweight attributes outlined in this chapter, Section 2.4 and Section 2.5.

2.16.1 Protocols adopted for our Smart Home devices

Given the constrained nature of the devices, we were considering to be powering up the Smart Home spaces this research was focusing on, the need to pick protocols that suit such description was key as that informed the solution for consideration towards authentication. The comparison of the various applicable protocols was done by Coetzee, Oosthuizen, and Mkhize (2018) (summarised in Table 2.5) and that heavily endorsed our choice of the Constrained Application Protocol (CoAP) protocol as it was ratified by Internet Engineering TaskForce (IETF) Internet standard in 2014, as the protocol for the information age.

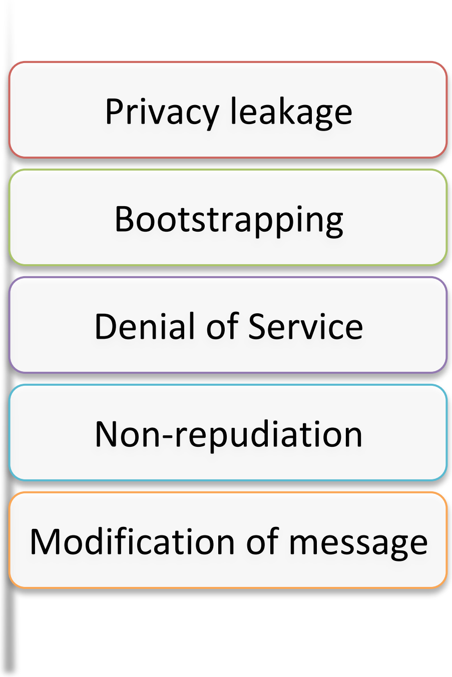
Table 2.4: Protocol comparisons
(Coetzee et al., 2018)

	Message Queuing Telemetry Transport (MQTT)	**Message Queuing Telemetry Transport for Sensor Networks (MQTT-SN)**	**Constrained Application Protocol (CoAP)**
Architecture	Publish/Subscribe via broker (Middleware)	Publish/ Subscribe via broker (middleware)	Client-server (URI-based)
Quality of Service	*QoS 0*: Fire-and-Forget; *QoS 1*: Message delivered at least once; *QoS 2*: Message delivered exactly once	*QoS 1*: Message confirmed by receiver with "Ack"; *QoS 2*: Message delivered exactly once	Confirmable (message confirmed by receiver with "Ack"); Non-Confirmable (fire-and-forget)
Security	Transport Layer Security (TLS)	Depends on network technology	Datagram Transport Layer Security (DTLS)
Transport	Transport Control Protocol (TCP)	User Datagram Protocol (UDP)	UDP

2.16.2 Threats addressed

The threats addressed by this research were those focused on violating data security between device-to-device communications. Such threats related to processes, applications and objects as proffered by Crossman and Liu (2016), that could disrupt the delivering of secure data transfers for AAL and ESS services in a Smart Home space, were considered. We would not claim that all threats related to the described service provision were addressed in this research, but focus was made towards the major threats for proof of concept against the proposed authentication architecture.

The major threats addressed in the proposed architecture are summarised in Figure 2.15 as supported by Ghosh, (2016); Jacobsson, Boldt, and Carlsson (2016); and Wang et al. (2016).



Privacy leakage

Bootstrapping

Denial of Service

Non-repudiation

Modification of message

Figure 2.15: Threats addressed

These threats were picked motivated by the need to secure the nature of personal and sensitive data in the Smart Home environment.

The threat landscape as outlined in Section 2.10, included insider and outsider attacks, replays attacks, man-in-the middle attacks, impersonating attacks and forward security attacks was adopted in full for this research. As precisely stated already in this chapter, the focus of the research was on addressing device level security vulnerabilities, which are summarised in Section 2.11.2, Figure 2.11, as well as focusing on M2M as informed in Section 2.11.2, Figure 2.13.

2.17 Authentication Focus Area

For authentication, our main area of focus was device-to-device communication. The rationale behind that focus area was that a sensor on a homebound patient is capable of transmitting data to the other sensor in a properly setup Smart Home space like adjusting the temperature. If an intruder gets access to such interaction and changes the correct values sent through to the gateway for action, the results could be catastrophic, as decisions will be based on wrong inputs.

Being able to ensure that authentication among the devices is completely administered via a trusted agent in the home setup guarantees data security and effective management of the Smart Home for the required services as and when needed, hence the defined thrust of this research.

From the comparison done in Section 2.13, Table 2.4, we picked Huang et al. (2016), Khemissa and Tandjaoui (2016b) and Shen et al. (2016)'s protocols as probable best options based on their costing values. We did further comparisons of the three as depicted in Table 2.5, based on the threats they addressed. This comparison was focused on the threat landscape highlighted in Section2.10.

It is imperative to note that addressing all the threats using one solution may not be practical, especially with the backdrop of lightweight requirements. We concluded based on this analysis that Shen et al. (2016)'s architecture was suitable for adoption towards the designing of our improved solution that specifically addresses device-to-device authentication at the M2M layer as presented in Chapter 4.

The main focus therefore, for resource-constrained devices was to find a solution that offloads as much as possible of the computational, processing and storing functionalities. As guided by the various authentication architectures and their performance costs in Section 2.17, the best approach for our focused solution was further built and incorporated in Chapter 4.

Guided by the authentication threats in Section 2.16.2, Chapter 5 gives the performance metrics of our proposed authentication architecture

Table 2.5: Device level costing comparison of various protocols

Khemissa et al.'s authentication protocol	✔	✔	✔	✔	✔	✔	
Huang et al.'s authentication protocol	✔	✔	✔	✔			
Shen et al.'s authentication protocol	✔	✔	✔	✔	✔		✔
Threats addressed	*Dictionary attack*	*Man-in-the middle attack*	*Replay attack*	*Modification attack*	*Impersonation attack*	*DoS attack*	*Forward security*

2.18 Overall Research Focus Area

Coming up with lightweight authentication architecture was a way of ensuring data security as it transitions through the various stages of its lifecycle from its source (sensors and actuators – raw data) to destination (gateways and servers - raw data to processed information) and vice-versa. The overall research was focused on proposing the best secure Smart Home spaces that can be advanced to assist the elderly, disabled and people with special needs, with a main focus on ensuring that their personal data is tightly secured and no unauthorised users have access to such data.

As that raw data guides informed decision-making processes (be they for health information purposes or energy saving measures), the Confidentiality, Integrity, and Availability (CIA) has to be preserved at all levels of access, hence these data questions (who, when, where, why and how).

2.19 Chapter Summary

This chapter gave a thorough literature search and key among the findings are the essential features of Smart Homes, the requirements, applications, models, challenges and future projections that gave a solid map on the threats and attack vectors for smart home setups.

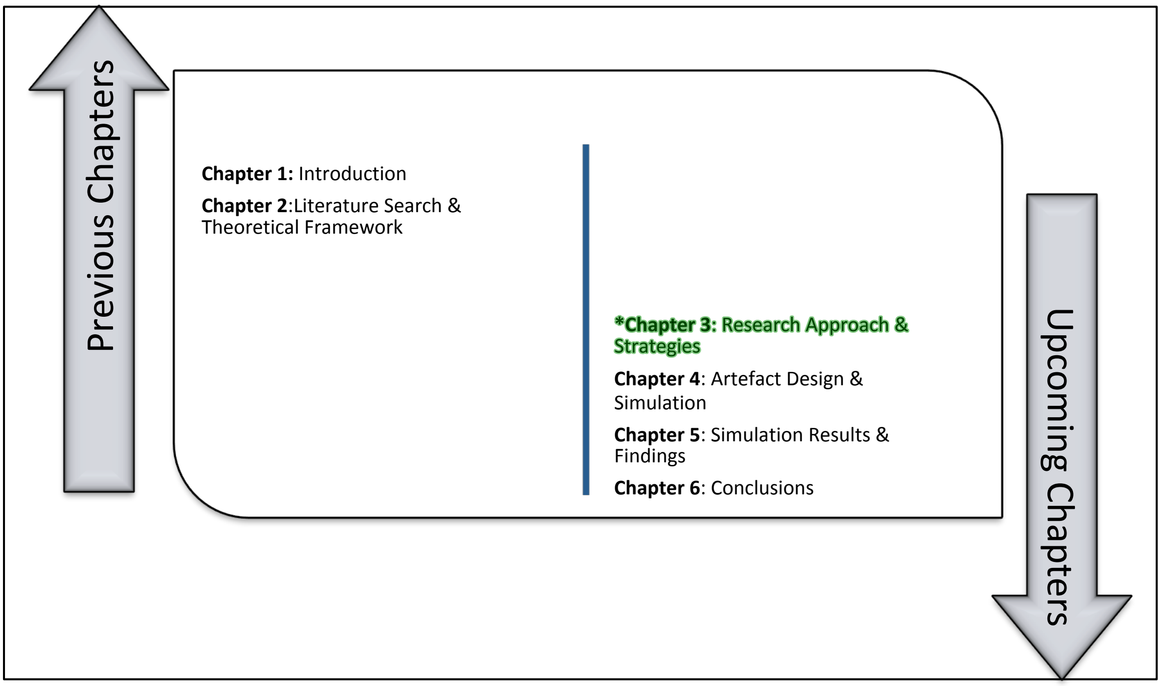
As depicted in section 2.17, an identification of various authentication architectures was done and the best authentication solutions to advance towards addressing as many of the Smart Home security threats as possible, was picked. Outlined in this chapter was coverage of the different authentication architectures that can be found in the IoT domain, and this is by no way an exhaustive list of the various approaches being developed and implemented as this area is receiving wide attention from various angles. A relook at existing authentication protocols helps in improving on newer designs and addressing some of the shortfalls of similar and previous versions. As security remains an evolving discipline, rigid approaches and standardizations for measuring some of the solutions on the ground may not be feasible, henceforth; it is ideal to have an outline of fundamental features to be incorporated in typical solutions.

As part of the focus of this chapter was to identify the best lightweight authentication approaches for Smart Homes, it is ideal to consider a number of key aspects when selecting a solution to advance towards the design of authentication techniques for Smart Homes. There are crosscutting dynamics in the various authentication approaches already in use and borrowing the best features from one solution and combining them with the others gives a recipe for a secure solution.

The costing of probable authentication architectures for consideration helped in the decision of selecting a less cost effective solution to propose for lightweight applications.

Lastly, this chapter presented a summary of the main research area, starting from the main research body of knowledge (Information Assurance and Security) to the specific domain of application that is Smart Home (Data Security). Then finally highlighting on specific security components of focus - authentication. An overarching research focus mapping concludes the chapter. The next chapter unpacks the methodology applied to realise these set research mandates as summarised in this chapter.

CHAPTER 3: RESEARCH APPROACH AND STRATEGIES



Previous Chapters

Chapter 1: Introduction

Chapter 2:Literature Search & Theoretical Framework

***Chapter 3:** Research Approach & Strategies

Chapter 4: Artefact Design & Simulation

Chapter 5: Simulation Results & Findings

Chapter 6: Conclusions

Upcoming Chapters

This chapter details and unpacks the methodology applied for this research. The first part outlines the literature backup on the methodology selected and the research paradigm applied. The second part details how data was collected, which variables were considered and how the data was analysed towards answering the questions outlined in Chapter 1.

3.1 Chapter Overview

This is among the crucial chapters of this thesis as it gives a map of the entire research journey from the beginning to the end. This chapter speaks directly to every set research question/objective of this research by outlining how the research managed to fulfil the objectives and answered the questions as well.

Chapter Organisation: Section 3.2 sets the tone for this chapter by giving a high level overview of the philosophy employed in this research, hence outlining the research paradigm. Section 3.3 highlights the research strategy employed by this research, where Design Science is explained and why it was selected for this research. Section 3.4 details and expands on how each research question or research objective was fulfilled. As an expansion of Section 3.4, Section 3.5 zeroes in on research methods, where details on the methods, tools and data analysis are expanded. Section 3.6 wrap the chapter by highlighting how the overall research covered in this thesis ought to be evaluated entirely.

3.2 Research Paradigm

The research paradigm used for this research was the Constructivist paradigm, using Design Science as the high level methodology, which then informed the methods that were used. Design Science research involves two primary activities to improve and understand the behaviour of aspects of information systems; (1) the creation of new knowledge through the design of novel or innovative artefacts (things or processes), and (2) the analysis of the artefacts is used and or performed (Hevner, March, Park, & Ram, 2004; March & Storey, 2016). For analysis of the security architecture, data analysis called for both qualitative and quantitative research methods, which were employed as depicted in Figure 3.1 and Figure 3.3.

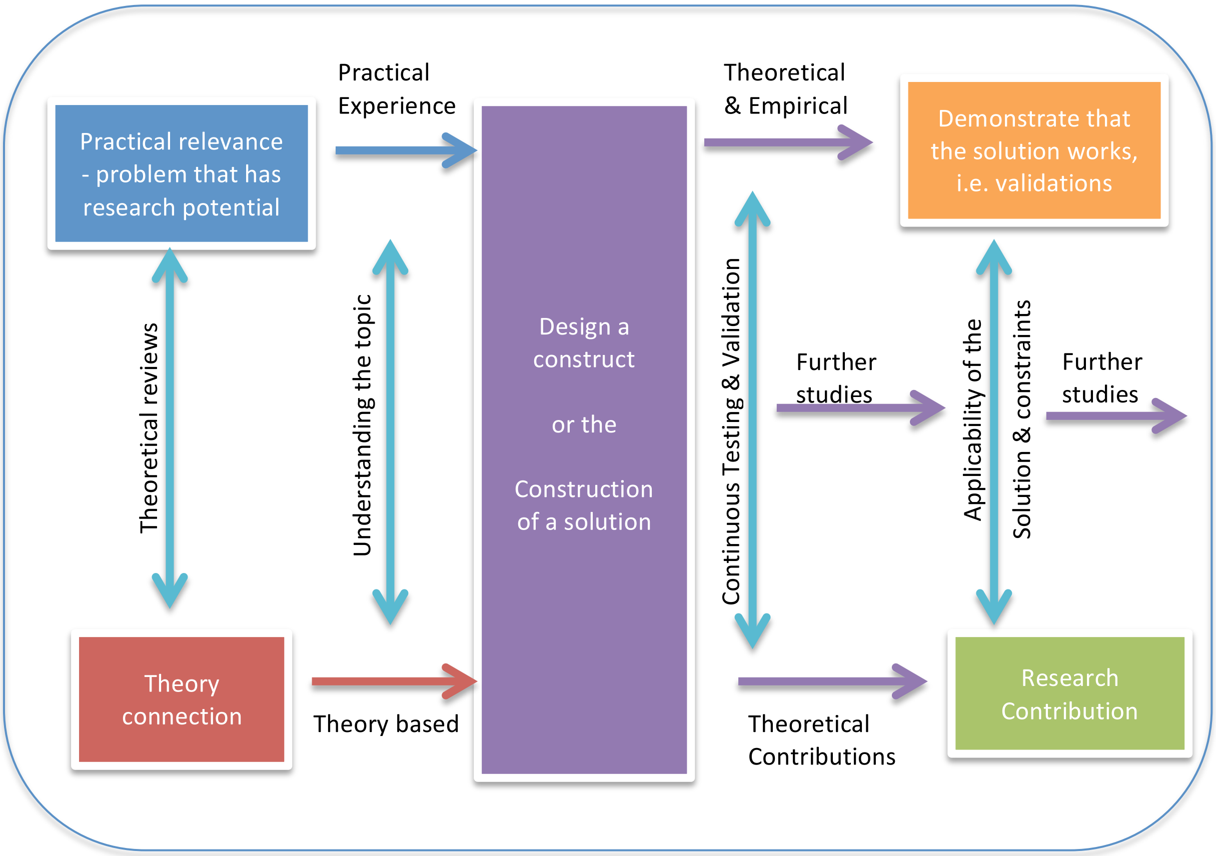


Figure 3.1: Features of Constructive research
(As presented by Oyegoke, 2011))

The need to choose a paradigm was explained by Kuhn (1970), when mention was made to the fact that, "science can only progress when it has a paradigm to be able to choose the research phenomena, ground a theory and state a framework" (p. 18). The focus on the Constructivist paradigm and its deemed relevance to this research has its basis on the construction of a solution that is based on the "subject's interaction with the world" matters as in security related research (Gray, 2014). Moreover, the flexibility of either lies in being qualitative or quantitative or both, as well as being goal-oriented and case based (Oyegoke, 2011).

A well-defined constructivist paradigm has to match the problem and the solution, together with the theoretical knowledge (Oyegoke, 2011). Considering the research objectives outlined in Chapter 1, Section 1.4, the need to match the problem of resource-constrained devices in the IoT and their need for a security solution could best be modelled with the constructivist research paradigm. This is supported by Oyegoke (2011) who proffers that; core element of the constructive approach is the design construct phase. This phase is often heuristic by nature with stricter theoretical justifications. This suited this research as most of the existing solutions to similar problems have and mostly could be concluded based on expertise and published works.

The constructivist paradigm recommends proof of concept and according to Oyegoke (2011), the novelty and actual functional solution needs to be demonstrated, and it is a rigorous approach (Tobin & Begley, 2004). The approach spans through construction, application and operationalisation, and these require innovativeness, creativity and transparency (Gioia, Corley, & Hamilton, 2013). The attributes informed the design of the architecture presented in Chapter 4.

The illustration given in Figure 3.1 summarises how the constructive research approach, which works by identifying the practical relevance of the problems that have research potential through theoretical literature, reviews and substantiated with practical experience, which in this research was demonstrated through the simulation of state-of-the-art data security, under the CIA triad, using formal methods.

This approach comprised of the epistemology, theory and technical issues, which provided the philosophical stance and gave context to and informed the study. The construct can be validated through triangulation of different approaches depending on the work at hand (Oyegoke, 2011). Most importantly, this process is not linear as illustrated in Figure 3.3, but it is a dynamic and interactive process between different phases, which speaks directly to the choice of Design Science as a high level methodology employed in this work.

A practical display of how the constructive research approach has been implemented in this research is presented in Figure 3.2 below.

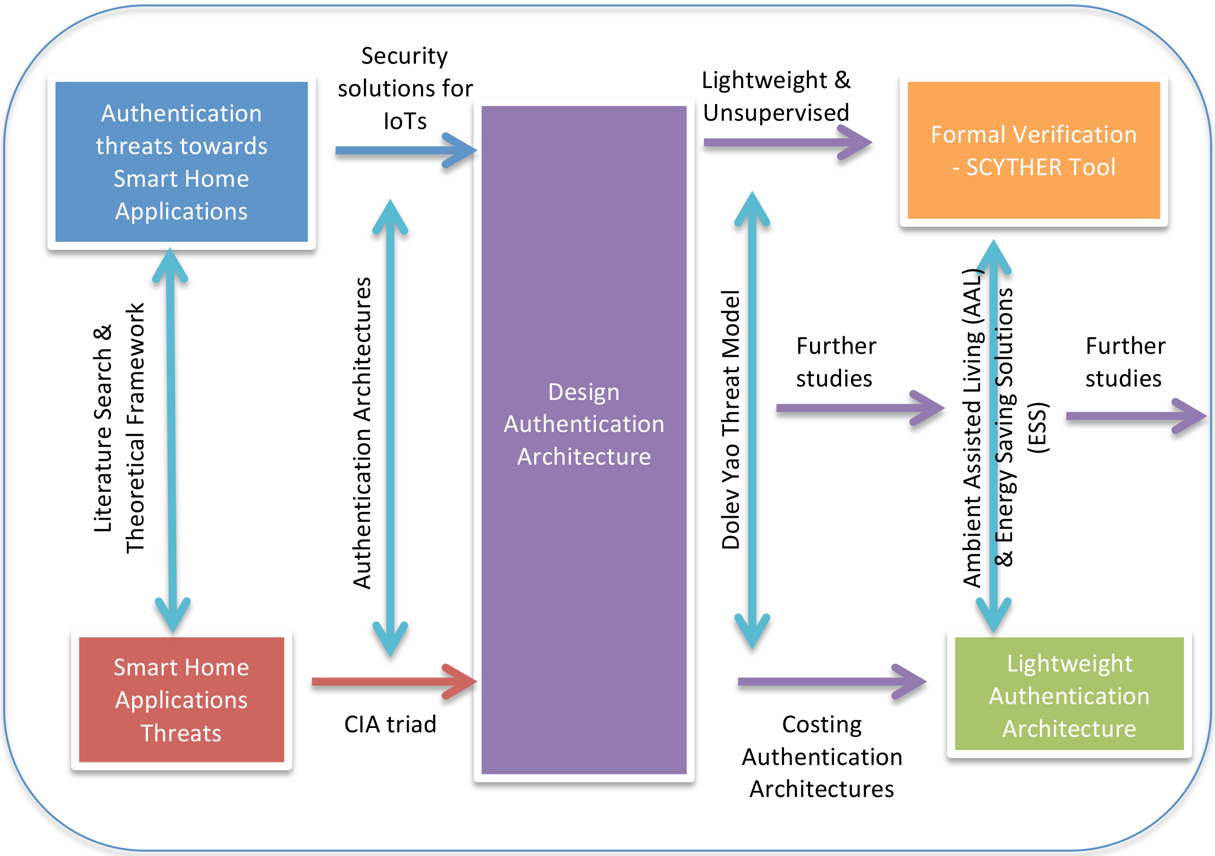

Authentication threats towards Smart Home Applications
Security solutions for IoTs
Lightweight & Unsupervised
Formal Verification - SCYTHER Tool
Literature Search & Theoretical Framework
Authentication Architectures
Design Authentication Architecture
Dolev Yao Threat Model
Further studies
Ambient Assisted Living (AAL) & Energy Saving Solutions (ESS)
Further studies
Smart Home Applications Threats
CIA triad
Costing Authentication Architectures
Lightweight Authentication Architecture

Figure 3.2: Application of the constructive research paradigm in this work

3.3 Research Strategy

The detailed application of the various methodological approaches in this research can logically be followed through their application on a step-by-step process in fulfilling the set research questions and ultimately realising the corresponding research objectives as summarised in Section 3.4. To effectively apply all the relevant methods to answer the stated research questions, the proposed research framework was Design Science research and this guided the entire research process. The modified adoption of the proposed research process by Offermann, Levina, Schonherr, and Bub (2009) is as summarised in Figure 3.3.

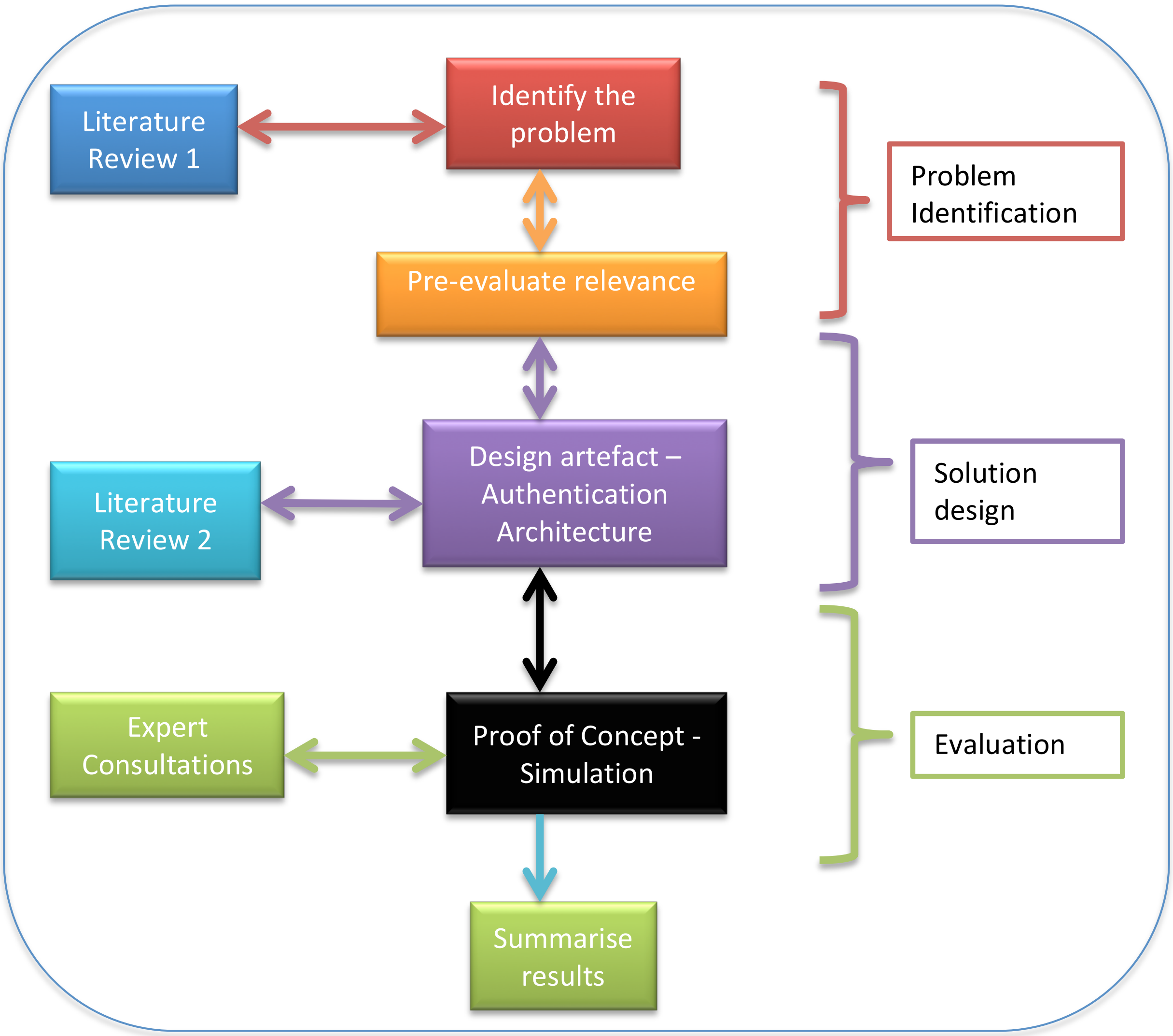


Figure 3.3: Research process using Design Science approach

Design Science research is presented by Winter (2008) as one that gives relevance and rigour if it is applied effectively to a particular problem under consideration. Many researchers underscore the need to combine research perspectives with corresponding methodologies over and above rigour and relevance as key pillars of Design Science (Offermann et al., 2009).

The emphasis that Design Science research places on the need to vary research methods as supported by Hevner and Chatterjee (2010), made it a suitable approach for the work carried out. In this research, coming up with a lightweight solution for unsupervised IoT in Smart Home applications called for a detailed evaluation of the artefact developed and guiding the process of reaching towards a conclusion. The flexibility of Design Science to support both quantitative and qualitative data research methods enabled the answering of the set of questions for this research in a more comprehensive way (Kaplan & Duchon, 1988; Offermann et al., 2009).

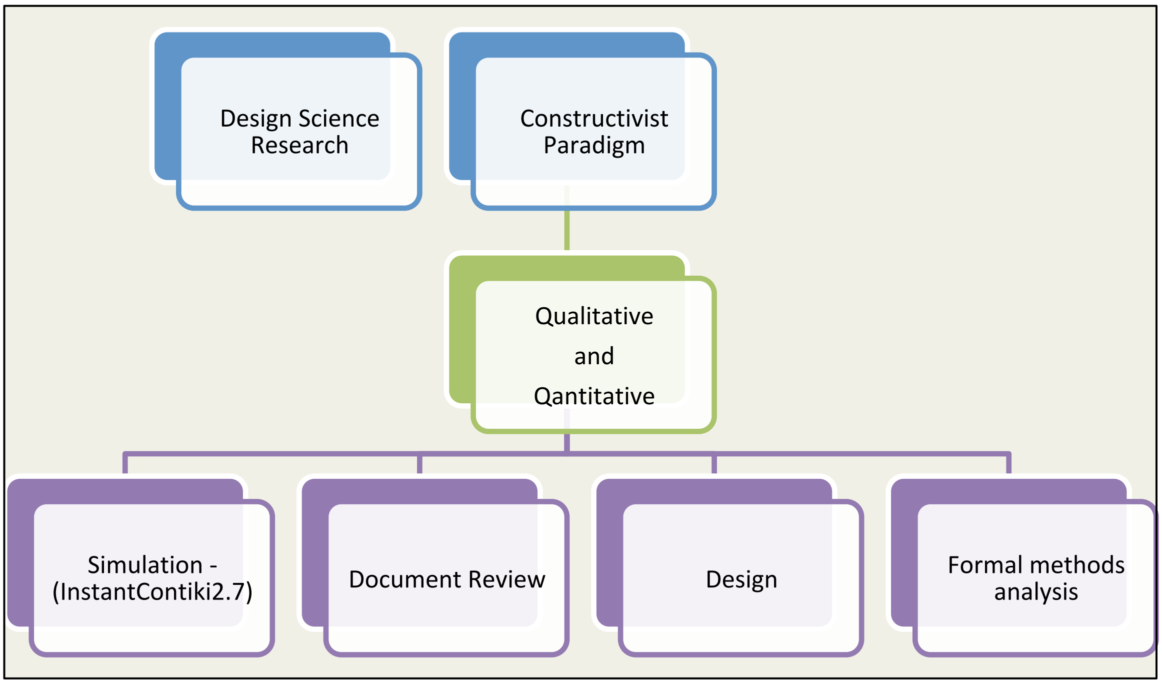


Figure 3.4: The Research Epistemological Perspective overview

Cross (2007), as cited in Offermann et al. 2009, p. 8), argues that “so we might conclude that design science refers to an explicitly organised, rational and wholly systematic approach to design; not just the utilisation of scientific knowledge or artefacts, but design being in some sense a scientific activity itself.” This argument therefore gives the interlink that can be formed between the constructivist paradigm and Design Science in research that typically involves the construction of a solution to a defined problem in a scientific approach. The specific application to this research of the Design Science model is depicted in Figure 3.5 below

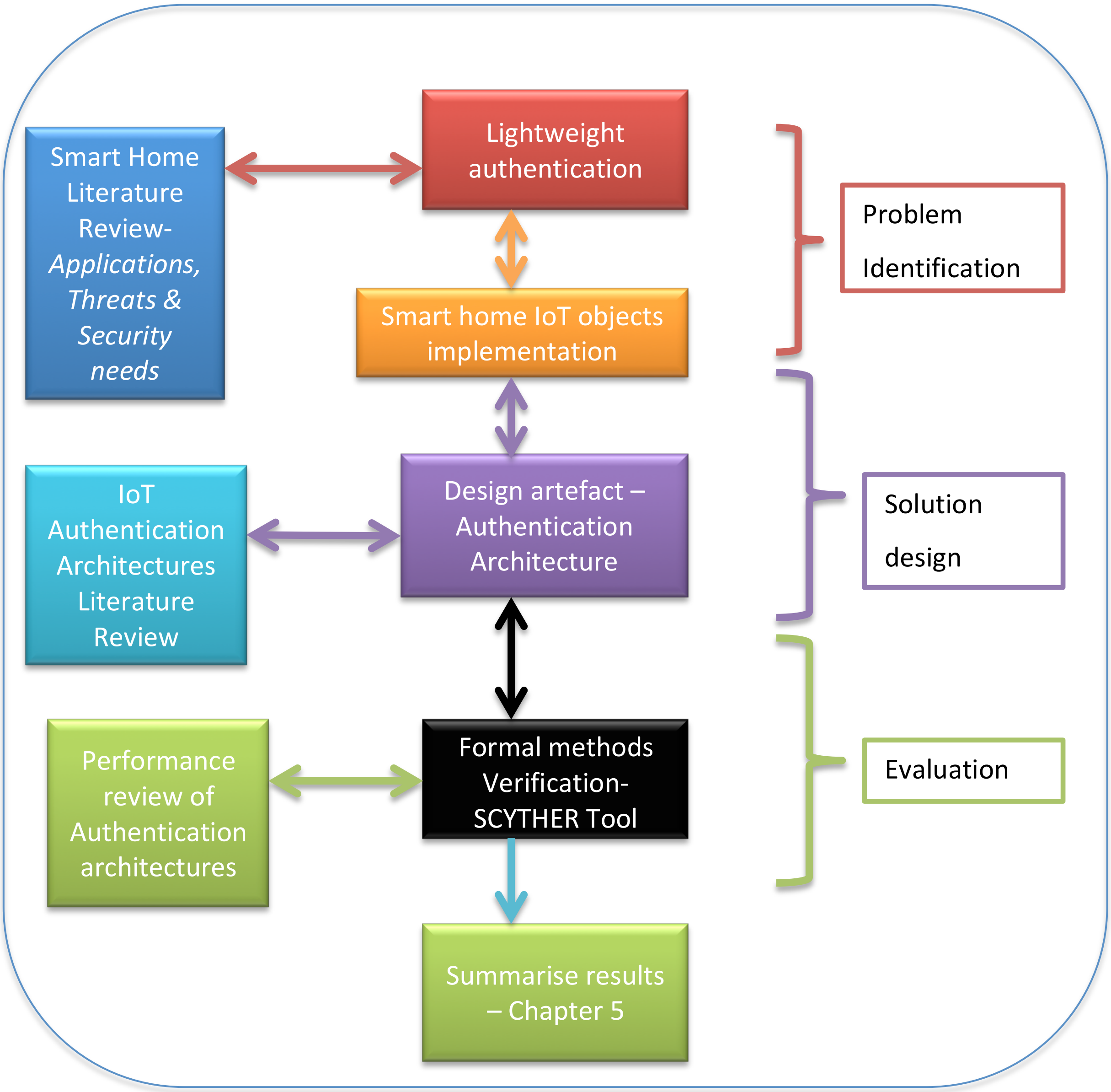

Smart Home Literature Review- *Applications, Threats & Security needs*
Lightweight authentication
Smart home IoT objects implementation
Problem Identification
IoT Authentication Architectures Literature Review
Design artefact – Authentication Architecture
Solution design
Performance review of Authentication architectures
Formal methods Verification- SCYTHER Tool
Evaluation
Summarise results – Chapter 5

Figure 3.5: The actual application of Design Science to this research

3.3.1 Challenge driven research approach

Research that is purely from a theoretical angle without any societal relevance lacks innovation and is not engaging enough (Rwegasira et al., 2018). Guided by the need to focus on research that has societal relevance, the approach employed in this research was to focus on the bigger vision of SDGs (SDGs, 2017). From the context of SDGs, our focus on Smart Homes was then not from a purely theoretical perspective but from a practical point of view. The need to look at Assisted Living Spaces and Energy Saving Solutions and how to ensure their security was motivated by the shared societal needs as enshrined in the SDGs.

The model proposed for application of the challenge driven approach is summarised in Figure 3.6, which is an adaption of the approach employed by Rwegasira et al. (2018).

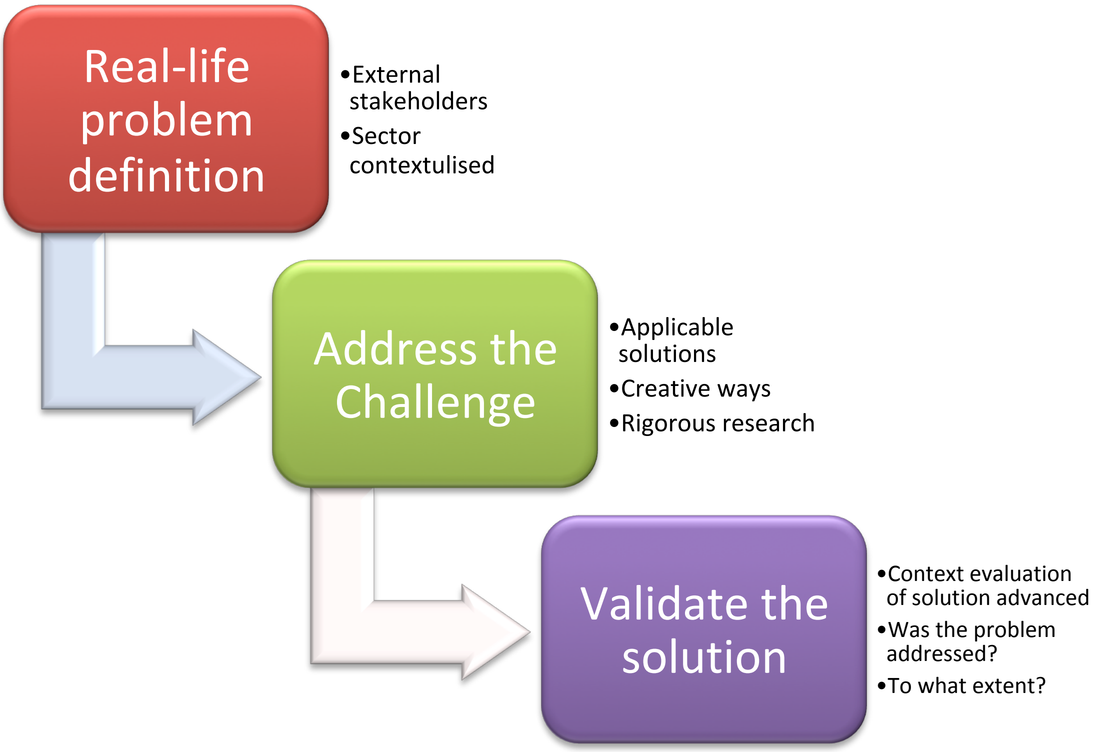
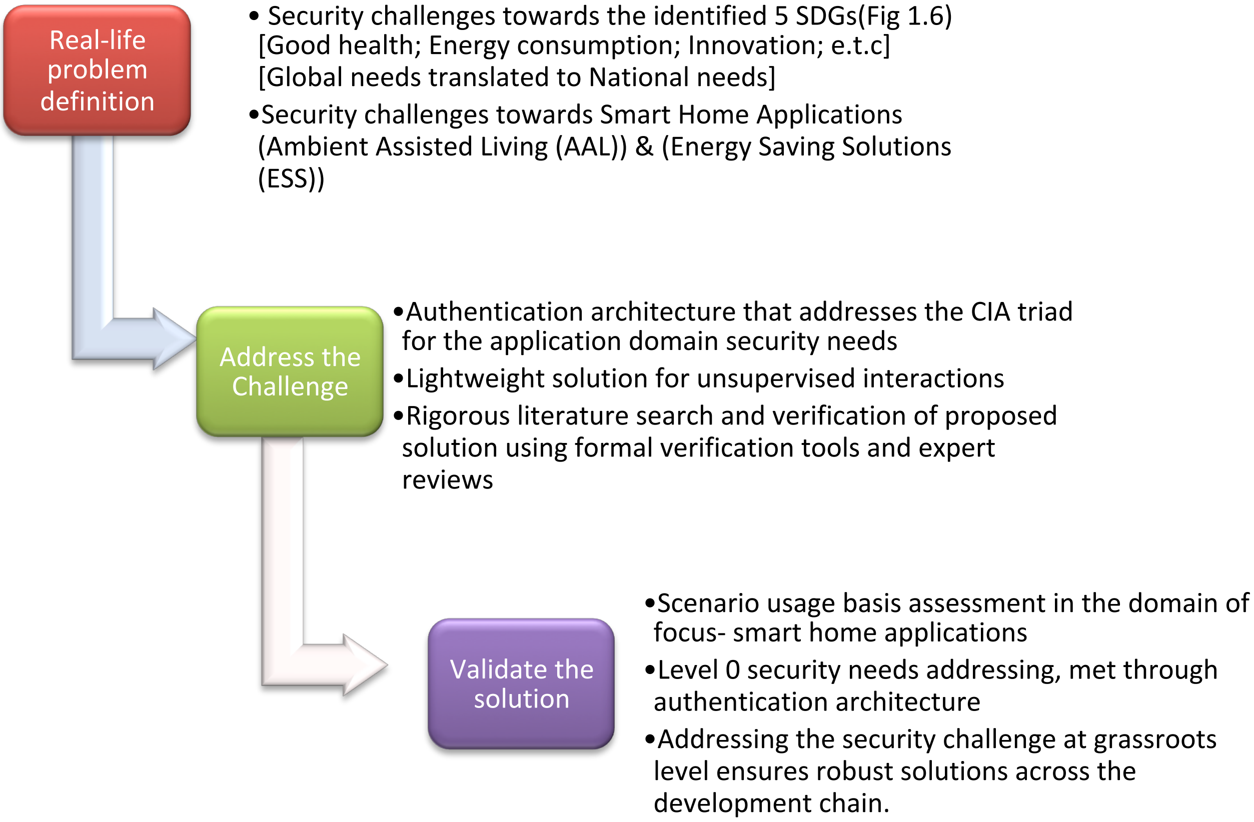


Figure 3.6: Challenge Driven Approach

As depicted in Figure 3.7, the actual application of the Challenge Driven Approach to this research as summarised in Chapter 1 was that of ensuring relevance to tangible causes such as the SDGs.



- Security challenges towards the identified 5 SDGs(Fig 1.6) [Good health; Energy consumption; Innovation; e.t.c] [Global needs translated to National needs]
- Security challenges towards Smart Home Applications (Ambient Assisted Living (AAL)) & (Energy Saving Solutions (ESS))

- Authentication architecture that addresses the CIA triad for the application domain security needs
- Lightweight solution for unsupervised interactions
- Rigorous literature search and verification of proposed solution using formal verification tools and expert reviews

- Scenario usage basis assessment in the domain of focus- smart home applications
- Level 0 security needs addressing, met through authentication architecture
- Addressing the security challenge at grassroots level ensures robust solutions across the development chain.

Figure 3.7: Challenge Driven Approach as applied to this research

3.3.2 Dolev Yao Model

The Dolev Yao model is the oldest model available that is still relevant in assessing the threat landscape of given application environments. As supported by (Backes, Cervesato, Jaggard, Scedrov, & Tsay, 2011), the Dolev Yao model offers computationally and cryptographically sound results. It is used among others, on the verification of wireless and wired networks as confirmed by Pöpper, Tippenhauer, Danev, & Capkun (2011)

The advantage of offering formalisation in explaining the capabilities of an adversary is one key attribute that renders the Dolev Yao model worth considering as supported by Halpern & Pucella, (2012). The reason why we adopted the Dolev Yao model for this research was partly on that basis of having a formalised adversary model.

We appreaciate some of the drawbacks of the Dolev Yao Model as highlighted by Halpern & Pucella, (2012) that it cannot handle probabilistic notions such as an adversary attempting to guess the keys. To ensure that this drawback was not going to affect our authentication protocol verification, the selected SCYTHER tool has features that go beyond the Dolev Yao modeling unlike its competiting and dropped alternatives such as the AVISPA, Casper and ProVerif, which are formal methods that allow flexiblity in their adoption of the Dolev Yao Model, in describing the adversaries.

Despite the critisism offered on the Dolev Yao model, there is wide appreciation of the fact that, almost all logics are based on the very model (Halpern & Pucella, 2012; Pöpper et al., 2011). There is proof of many extensions of the model too, such as the cyber-physical Dolev Yao attacker model (Pöpper et al., 2011). To confirm the wide acceptablity of the Dolev Yao model, Martina, dos Santos, Carlos, Price, & Custódio (2015) posits that it is the most widely accepted attacker model for the analysis of security protocols.

3.4 Research Approach

Table 3.1 below is a detailed summary of how each of the research objectives and the research questions were addressed, by highlighting the tools, methods, and the outcomes that guided the adequate fulfilment of the set targets.

Table 3.1: Summary of research methodology application

#	Research Objective	Research Question	Methods/Tools	Expected Outcome
1	Identify the potential authentication threats to IoT Smart Home applications	What are the potential authentication threats to IoT in Smart Home applications?	Literature review of technical and scientific data sources. Qualitative data analysis	Authentication threats to IoT Smart Home applications
2	Analyse current IoT authentication architectures that suit Smart Home applications	What are the available authentication mechanisms for IoT and their relative performance?	Literature review of technical and scientific data sources. Qualitative data analysis	Authentication architecture Protocol performance metrics and functional specifications
3	Design a lightweight IoT secure authentication architecture for Smart Home applications	How can Smart Home IoT objects be authenticated in a computationally efficient, secure, and correct manner?	Quantitative data analysis Formal methods	Artefact – Simulation of its functionality Comparative results from experts A lightweight IoT architecture
4	Evaluate the proposed secure solution for correctness and computation efficiency	What performance evaluation approach and strategy will best validate the architecture?	Simulation – Proof of concept Expert consultations	Validated results on efficiency and scalability

3.5 Research Methods

As a highlight of the various methods and tools employed to answer the research questions, this section details the sampling methods used, the data collection approach and ultimately how data was analysed.

3.5.1 Sampling methods

The appropriate sampling population and simulation runs executed fulfil Objective 3 (Design a lightweight authentication architecture for Smart Home applications) and partly Objective 4 (Evaluate the proposed secure solution for computation efficiency and scalability). The sampling approach employed in the simulation of the architecture was based on the range of runs that can be applied in testing the robustness of the architecture’s functionality when intruders are given more room to explore every possible attack vector. A snowballing sampling approach (Stephanie, 2017) was then appropriate to employ for this exercise.

3.5.2 Data collection

Qualitative data was collected from scientific and technical sources through literature reviews. The secondary data collected as depicted in Table 3.1, was used in light of Objective 1, Objective 2, and partly Objective 4. As indicated on the expected outcome column in Table 3.1, the nature of data collected from secondary sources guided the answering of respective research questions. Quantitative data collected from the simulated nodes that depicted an abstraction of a Smart Home setup tested the resource efficiency of the presented architecture in Chapter 4.

3.5.3 Simulation

The research needed to model AI; hence, the choice of a simulation platform guided the need to select an Agent Based Modelling (ABM) as an approach. An ABM closely explains the features that formulate an AI based setup.

The qualities that deemed agents appropriate to simulate Smart Home behaviours is their autonomous, self-contained and interacting nature (Macal & North, 2008). As depicted in Figure 3.8, an ABM interacts with its environment and the roles of an agent are clearly summarised.

There are various ABM applications as summarised by Macal and North (2008, p. 93) in Table 1 of their paper. A dedicated prototyping agent-based environment applied in this research in the form of REcursive Porous Agent Simulation Toolkit (REPAST) Simphony was chosen based on its scalable nature compared to NetLogo, Starlogo, and MATLAB.

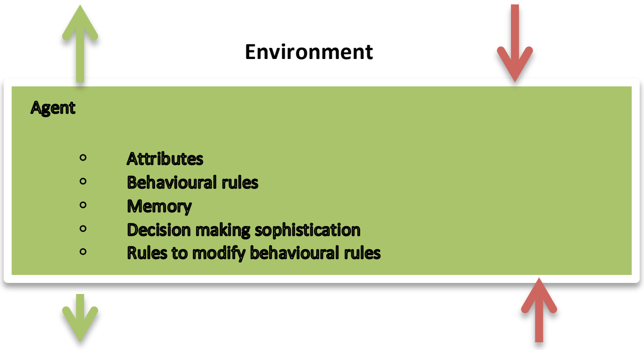

Environment
Agent
Attributes
Behavioural rules
Memory
Decision making sophistication
Rules to modify behavioural rules

Figure 3.8: A typical agent

3.6 Research Analysis Tools

The typology for analysis of the secondary data for Objectives 1 and 2 was the amplified analysis (Gray, 2014). The assorted data analysis (Gray, 2014) was applied towards meeting Objective 4. Simulation run using existing platforms as informed from the qualitative data analysis, was used to validate the designed architecture. The experimental design guided by best practices in security design, which are enshrined in the CIA triad, were the basis of evaluating the authentication architecture. Descriptive statistics (Gray, 2014) were used to analyse the quantitative data. Analytic induction analysis then helped to identify adoptable patterns for a secure architecture design.

The evaluation on the impact of attacks on IoT simulated using SCYTHER as well as the proposed authentication architecture-using InstantContiki 2.7, helped in simulating the Smart Home environment.

To test the authentication capacity of the IoT devices, scenarios were created (as depicted in Chapter 5, Section 5.2) in a simulated environment and computational efficiency was measured, which was tested against similar solutions on authentication, which would have been applied in the same simulated environment.

3.6.1 The SCYTHER tool

The SCYTHER tool is a verification, falsification and analysis tool for security protocols (Cremers, 2008). As posited by Cas Cremers (2008) at the time of his writing, there was still ongoing work towards formal approaches for protocol construction, which were backed by formal logic. The SCYTHER tool therefore filled that gap.

Based on the novel features of SCYTHER, we selected the tool for formal verification of the protocol behind our architecture, particularly the authentication component. Such features as giving a platform for unbound verification with guaranteed termination, analysis of infinite sets traces in terms of patterns and multi-protocol analysis, formed the basis of protocol validation. An important feature that also determined its selection compared to existing verification tools like AVISPA and ProVerif was its ability to analyse classes of attacks and model possible protocol behaviours. Such functionality was attained with an unbound number of protocol sessions proved correctness.

From the analysis done by Cremers, Lafourcade, and Nadeau (2009), the SCYTHER was the fastest verification tool which did not make use of approximation methods as it outperformed AVISPA and ProVerif.

3.6.2 Application of the SCYTHER Tool to this research

We had to convert our architecture's functional model into a Security Protocol Description Language (SPDL) format, based on the semantics of High Order Logic (HOL). The SCYTHER was able to verify the security claims as represented in Chapter 8. By validating the security claims, a protocol measured for its security level (see Chapter 5, Section 5.2).

Table 3.2 is a summary of how the verifications were tested, based on the SCYTHER tool.

Table 3.2: Verification using SCYTHER
(adopted from Cremers, 2014))

Function	Description of how it was tested
Verification of claims	Using SPDL, specifications of the properties that build up a security authentication architecture applied as claim events in a role based approach (Typical Alice and Bob security representation). We then used SCYTHER to verify or falsify the claims based on conditions set.
Automatic claims	In cases where there was no claim set, the tool was able to generate its own. Upon setting automatic claims, the tool was able to proceed with the verification process.
Characterisation	Each protocol role was characterised, thereby enabling analysis, henceforth providing finite trace representations of executions that defined the terms of roles.

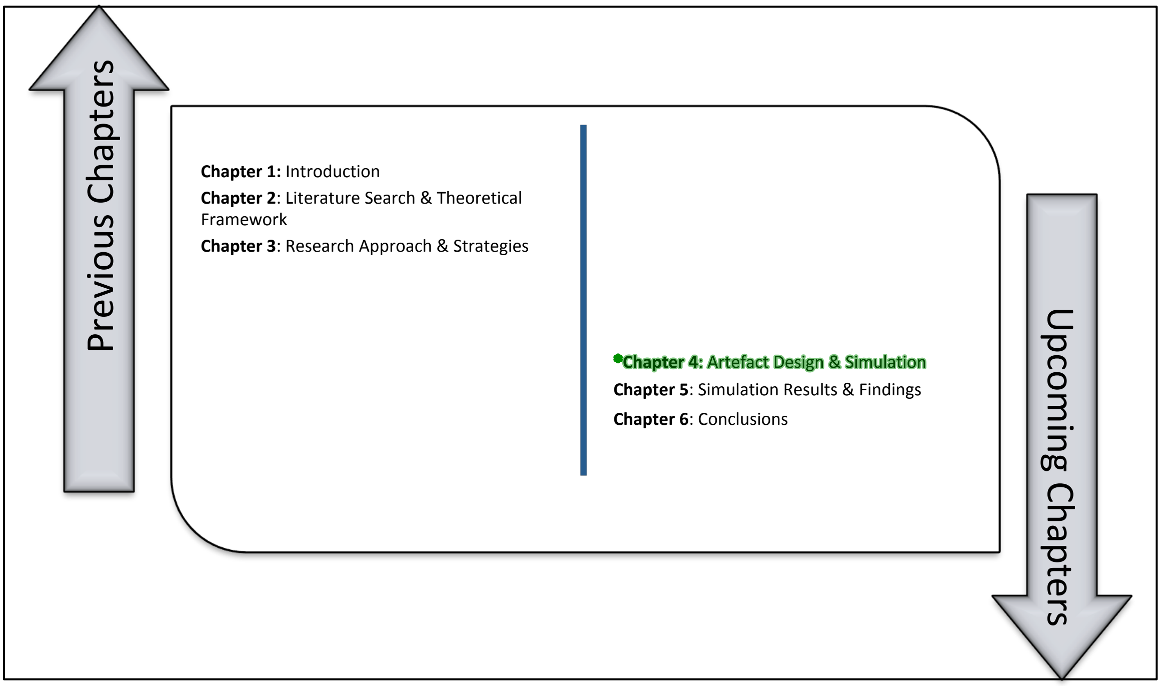
3.7 Evaluation of Research

Conclusions drawn from the comparison results had done quantitatively from the simulation environment on the different authentication architectures already in use under Smart Home applications and relatively close applications as detailed in Chapter 2. Considering the costing analysis done in Chapter 2, Section 2.13 when the related authentication approaches were selected for this research, it is apparent that our proposed authentication architecture is lightweight on the device level yet secure by leveraging the agent-based model through the introduced Smart Home agent (see Chapter 4, Section 4.3.3).

3.8 Chapter Summary

In this chapter, the high-level research paradigm outlined, and the overall research approach explained are key points to note. Details on how the research executed the methodology towards realising the stated objectives or set questions were detailed in Table 3.1 as presented in Section 3.4. The methods and tools used as well as the expected outcomes for each respective research milestone were also highlighted in this Chapter. The research methods section summarised the sampling methods, data collection methods and how data was analysed to draw conclusions on this research. As a cap to the overall chapter, section 3.6 outlined how the entire research evaluation was advanced.

CHAPTER 4: ARTEFACT DESIGN AND SIMULATION



Previous Chapters
Chapter 1: Introduction
Chapter 2: Literature Search & Theoretical Framework
Chapter 3: Research Approach & Strategies
●**Chapter 4: Artefact Design & Simulation**
Chapter 5: Simulation Results & Findings
Chapter 6: Conclusions
Upcoming Chapters

As part of research Objective 3: "Design a lightweight IoT secure authentication architecture for Smart Home applications," this chapter details the proposed architecture. The simulation of the architecture under different Smart Home security scenarios is detailed in this chapter. The approaches for testing are outlined here.

4.1 Chapter Overview

The authentication architecture proposed in this work originates from the basis of looking at lightweight solutions. The lightweight attributes taken into consideration are cost of computation, storage capacity and processing time.

Figure 4.1 is a representation of the ideation of the process of coming up with the Authentication architecture. This is not the actual architecture presented in this work but the first prototype that inspired the thinking behind the final architecture.

The proposal of an agent component on the refined architecture (Figure 4.2) based on transfering the main authentication functionality to a trusted layer was ideal. The existing Kerberos authentication architecture, which is effectively used today by many industries including big corporates such as Microsoft and others, validated the architectural choice. An agent-based approach promised the ability to reduce the needed computation on the actual things in the Smart Home network and on the virtual storage side.

Chapter Organisation: Section 4.2 lays the foundation on how the presented authentication architecture was formulated. After laying the foundation, the detailed systematic functionality and various defined functions in Section 4.3 guided the process of the architecture design. To guide the reader to follow the whole process on the execution of the architecture simulation, the section that serves that purpose is Section 4.4. Section 4.5 gives a summary pointing towards some typical Smart Home security scenarios that helped in the optimisation of the architecture. As a precursor to Chapter 5, Section 4.6 bridges this chapter and what the reader should expect to encounter in the next chapter. The overall summary of the Chapter is in Section 4.7.

4.2 The Proposed Authentication Architecture - prototype 1

There are three main key attributes that we concluded to be vital in the formulation of the authentication architecture, which are the thing, the virtual storage and the interface among the various communication patterns on any given home setup.

Considering that the things are a subset of M2M, representing M2M as a separate component was meant to show that there are various attributes for consideration, to reflect the heterogeneity of the Smart Home network. Considering the representation in Figure 4.1, there is more emphasis on the various protocols to take into consideration. These various protocols are taking into consideration the various components of Smart Home devices, that is from manufacturer defined protocols, network protocols and application protocols, just to mention a few. This creates a complicated representation, hence the need to think about how best to minimise the complexity as that will be costly in terms of computation and processing time.

This is the main reason why the prototype in Figure 4.1 needed to be refined to eliminate the computational costs, processing time, and end to end overload of the devices in the Smart Home setup. The focus was on coming up with a lightweight solution.

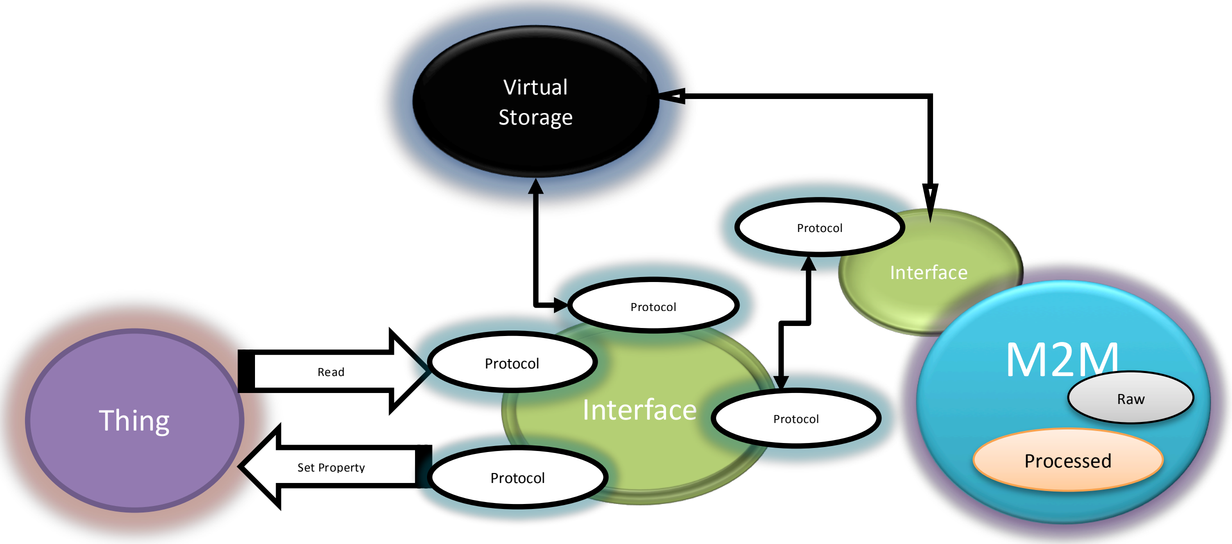


Figure 4.1:Prototype 1- proposed Authentication Architecture

4.3 The Proposed Authentication Architecture

We assume there are three roles in the proposed authentication architecture, which are to be assumed by the Virtual storage (**V_n**), the Thing (**T_n**) and the Smart Home Agent (**SHA**), which is a trusted security layer and will be running both instances of **V_n** and **T_n**. **n** is a unique identification of different things in the Smart Home space. **T_n** represents digital signatures as a form of unique identification. However, for the purposes of demonstration and proof of concept, natural numbers were used. To enable proper following of the proposed architecture, Table 4.1 is a summary of notations used to explain the steps and to also visually present the architecture.

Table 4.1: The notations used for AA

Notation	Interpretation
V_n	Virtual storage unique identity
T_n	Thing's unique identity
T_nID_r	Thing's SHA identity request
V_nID_r	Virtual server's SHA identity request
V_nN	A random number chosen by the virtual storage
T_nN	A random number chosen by the thing
k	A security parameter chosen by SHA
$\oplus$	XOR operation
h(-)	A secure one-way hash function
||	String concatenation operation
V_nTS	Timestamp of the virtual storage
T_nTS	Timestamp of respective thing from 1 to n
T_nS	Secure unique ID generated by SHA for Thing n
V_nS	Secure unique ID generated by SHA for Virtual storage n
$SHATST_n$	Timestamp sent to thing from SHA
$SHATSV_n$	Timestamp sent to virtual storage from SHA
SHATS	Timestamp of Smart Home agent

The Virtual storage is responsible for providing services for the Thing(s) and the authorised Smart Home Agent (**SHA**) is a trusted layer which generates security parameters and distributes an identity (**ID)** to the authorised user and the virtual storage. The Things and Virtual storage may be distributed but **SHA** is running an instance of each as a replica of its platform. We assume a perfect update of the current state of the various components on this architecture. **SHA** is visualised as the middleware for the overall architecture implementation and operation.

The proposed architecture is divided into the bootstrapping phase and the authentication phase. The bootstrapping phase is composed of the request-reply phases, which are described in the following series of steps (Section 4.3.1).

4.3.1 Bootstrapping phase

Bootstrapping is one of the most crucial levels of IoT's life cycle as sometimes that is where security threats are encountered if not properly setup. This phase ensures the identities of the Thing as they join the home network registered with **SHA**. The reason for the registration with **SHA** is to ensure that the Smart Home setup moves beyond default (often unchanged passwords) from manufacturers as the only security feature. The initial phase will be a request phase, which unfolds as outlined below.

A. The request phase

Step 1: **Handshaking stage** - **SHA** generates a random number for the Thing requesting to be added to the home network and another corresponding one for the Virtual storage, hence $\mathbf{V_nN}$ (for the Virtual server) and $\mathbf{T_nN}$ (for the Thing).

Justification: The need to register the Virtual storage is motivated by the reasoning that the home environment consists of unique IoT powered objects and these may have different manufacturers. To ensure that when updates are going to be pushed from different vendors to the various gadgets in the Smart Home space, they are from authorised providers only.

Step 2: The Thing and the Virtual storage generates identity request $\mathbf{(V_nID_r)}$ and $\mathbf{(T_nID_r)}$ respectively.

Justification: The need to have the Thing and the Virtual storage requests separately is to create a mutual authentication model, such that when there is need to authenticate either of the combinations, **SHA** will verify either forward or backward.

Step 3: The Thing and the Virtual storage server send **{T_nID_r , T_nN}** and **{V_nID_r, V_nN}** to the **SHA** respectively.

Justification: The need for both **V_n** and **T_n** to send their respective random numbers is to allow verification by **SHA** on the reply phase.

B. The reply phase

Step 1: According to the received request, the **SHA** will check the legitimacy and then generate an **ID** or discard the request.

Step 2: If the request passes the verification, **SHA** will generate the identity **T_nS** and **V_nS**, a security parameter **k** and a timestamp **$SHATST_n$** and **$SHATSV_n$** for the Thing and the Virtual storage respectively. SHA generates k, as a digital certificate for the Thing, which is a unique identifier, which validates the Thing.

Step 3: To ensure the possibility of verifying the communication during the authentication phase as well as decreasing the computation on the Thing side mainly, **SHA** will compute:-

$$A= h(T_nS || k) \oplus T_nN \qquad [4.1]$$

and

$$B= h(V_nS || k) \oplus V_nN \qquad [4.2]$$

SHA will then send **{T_nS, B, k, $SHATST_n$}** and **{V_nS, A, k, $SHATSV_n$}** to the Thing and the Virtual storage respectively.

4.3.2 The authentication phase

The authentication phase witnesses two main operations as follows:-

A. Thing Authentication Phase

Step 1: The Thing sends **$\{T_nS, T_nTS, T_nN\}$** to **SHA**.

Note: The timestamp and the random number are fresh values.

Step 2: After receiving the parameter combination from the Thing, **SHA**, by invoking the Virtual storage instance, will check if the **T_nTS** is valid then compute:-

$$P_{TA} = A \oplus T_nN \qquad [4.3]$$

and

$$P_{TB} = h\ (T_nS||k) \qquad [4.4]$$

Step 3: if **P_{TA}** = **P_{TB}**, the Thing is confirmed to pass the authentication, otherwise, **SHA** ensures that this thing is flagged as illegal and denies it access to its requests.

B. Virtual Storage Authentication Phase

Step 1: The Virtual storage sends **$\{V_nS, V_nTS, V_nN\}$** to SHA.

Note: The timestamp and the random number are fresh values.

Step 2: After receiving the parameter combinations, **SHA** will check if **V_nTS** is valid or not. If **V_nTS** is valid, **SHA** with the aid of the thing instance will compute: -

$$P_{vA} = B \oplus V_nN \qquad [4.5]$$

and

$$P_{vB}= h(V_n \,||\, k) \qquad [\ 4.6]$$

Step 3: If **$P_{vA} = P_{vB}$**, the Virtual storage is confirmed to have passed the authentication.

4.3.3 Visual display of the architecture

The representation given in Figure 4.2 is the visual display of the Authentication Architecture (herein dubbed **AA**). The communication between Virtual storage and **SHA** has two events labelled (**A**) and (**B**), these are an added feature that our architecture capitalises on to achieve mutual authentication between **(T_n)** and **(V_n)** at any instance after registration has been completed, hence facilitating proper authentication of **T_n** by **SHA**.

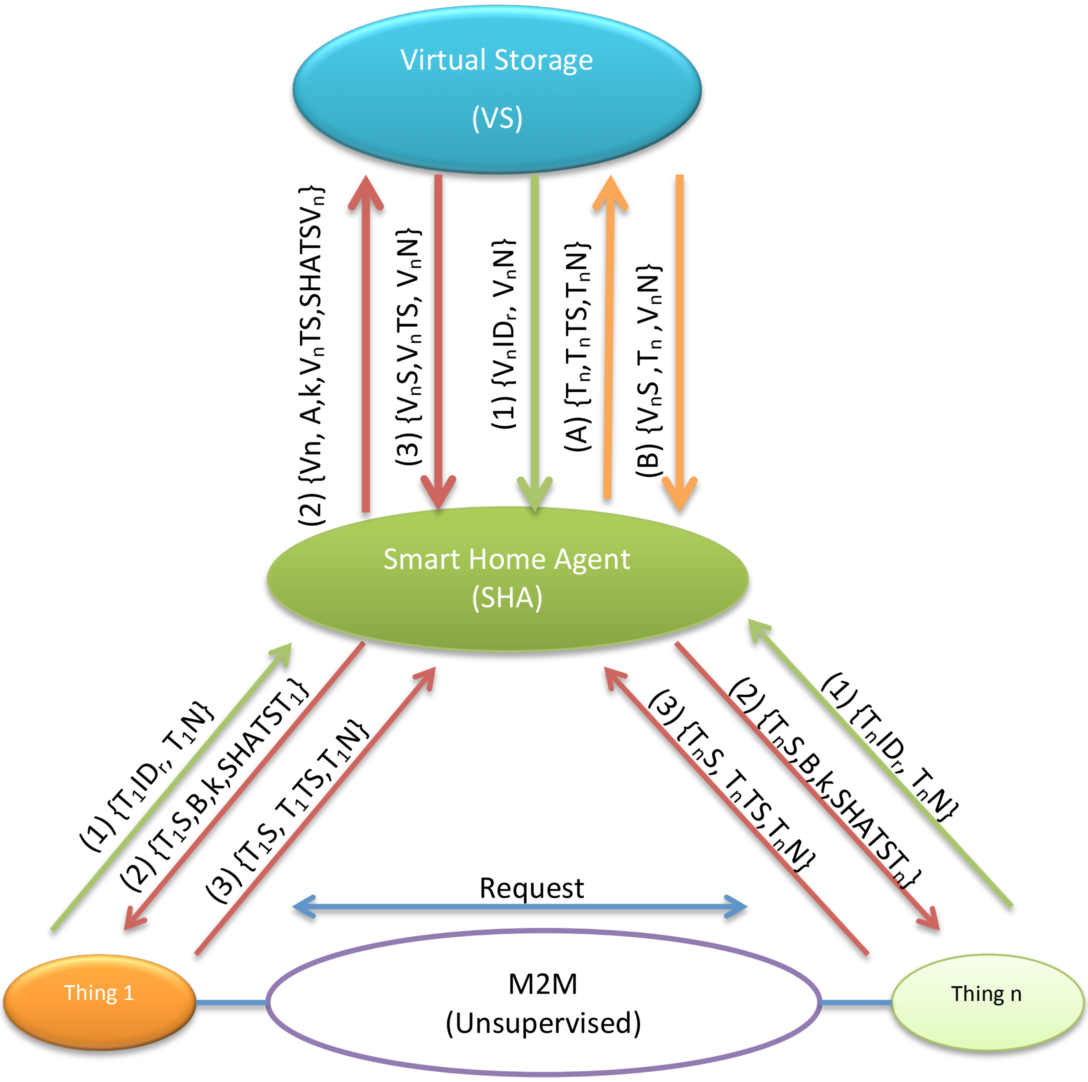

Virtual Storage
(VS)
(2) {Vn, A,k,V_nTS,SHATSV_n}
(3) {V_nS,V_nTS, V_nN}
(1) {V_nID$_r$, V_nN}
(A) {T_n,T_nTS,T_nN}
(B) {V_nS ,T_n ,V_nN}
Smart Home Agent
(SHA)
(1) {T_1ID$_r$, T_1N}
(2) {T_1S,B,k,SHATST_1}
(3) {T_1S, T_1TS,T_1N}
(3) {T_nS, T_nTS,T_nN}
(2) {T_nS,B,k,SHATST_n}
(1) {T_nID$_r$, T_nN}
Request
Thing 1
M2M
(Unsupervised)
Thing n

Figure 4.2: The proposed Authentication Architecture (AA)

4.4 Simulation of the Architecture

In order to simulate the architecture, we presented different scenarios of the Smart Home environment as highlighted in Chapter 2 on the focus of the application domains of choice. To ensure that we had an exhaustive and competitive list of possible scenarios, Figure 4.3 and 4.4 summarise the respective possible functional calls for Smart Home setup supporting AAL and ESS.

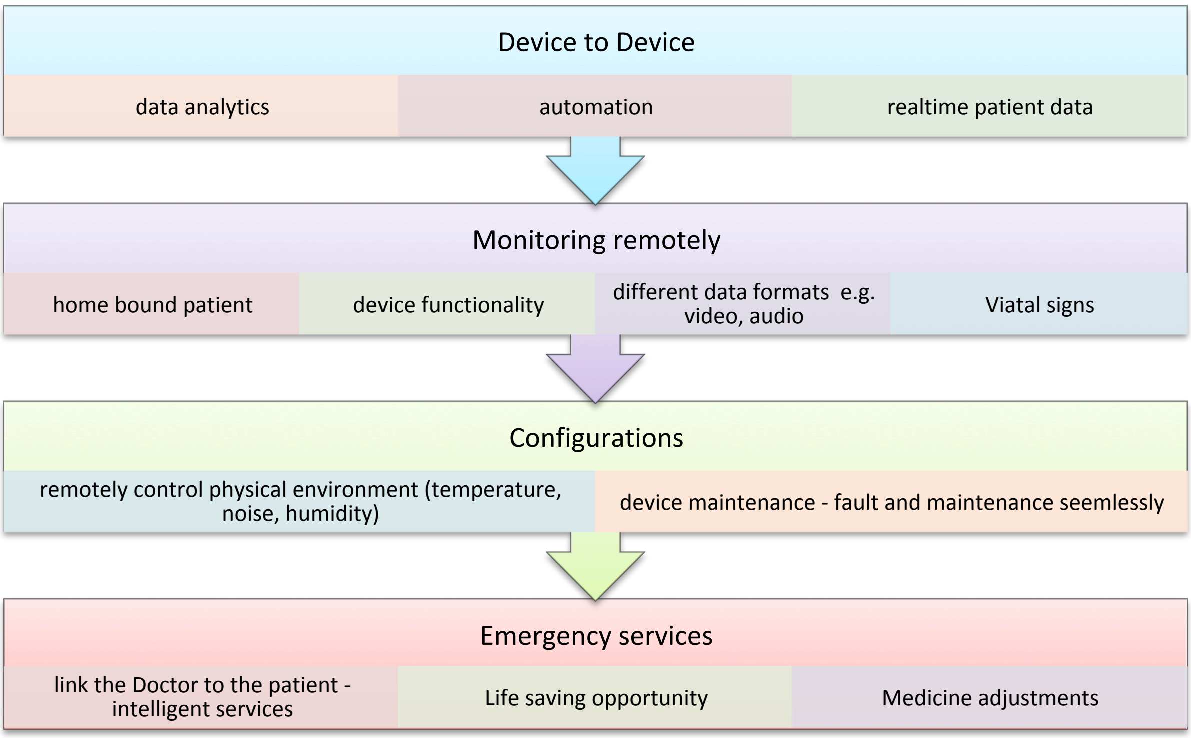

Device to Device
data analytics
automation
realtime patient data
Monitoring remotely
home bound patient
device functionality
different data formats e.g. video, audio
Viatal signs
Configurations
remotely control physical environment (temperature, noise, humidity)
device maintenance - fault and maintenance seemlessly
Emergency services
link the Doctor to the patient - intelligent services
Life saving opportunity
Medicine adjustments

Figure 4.3: AAL possible functions in a Smart Home setup

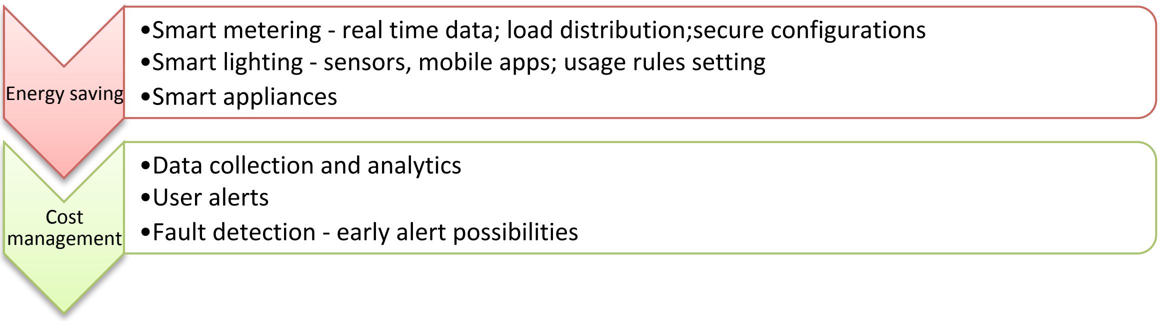

Energy saving
•Smart metering - real time data; load distribution;secure configurations
•Smart lighting - sensors, mobile apps; usage rules setting
•Smart appliances
Cost management
•Data collection and analytics
•User alerts
•Fault detection - early alert possibilities

Figure 4.4: ESS possible applications in a Smart Home setup

4.4.1 Sequence Modelling of the AAL and ESS

As summarised in Figure 4.5, our architecture is logically presented in such a way that, any picked functionality from an Ambient Assisted Living (AAL) and Energy Saving Solution (ESS) can be modelled.

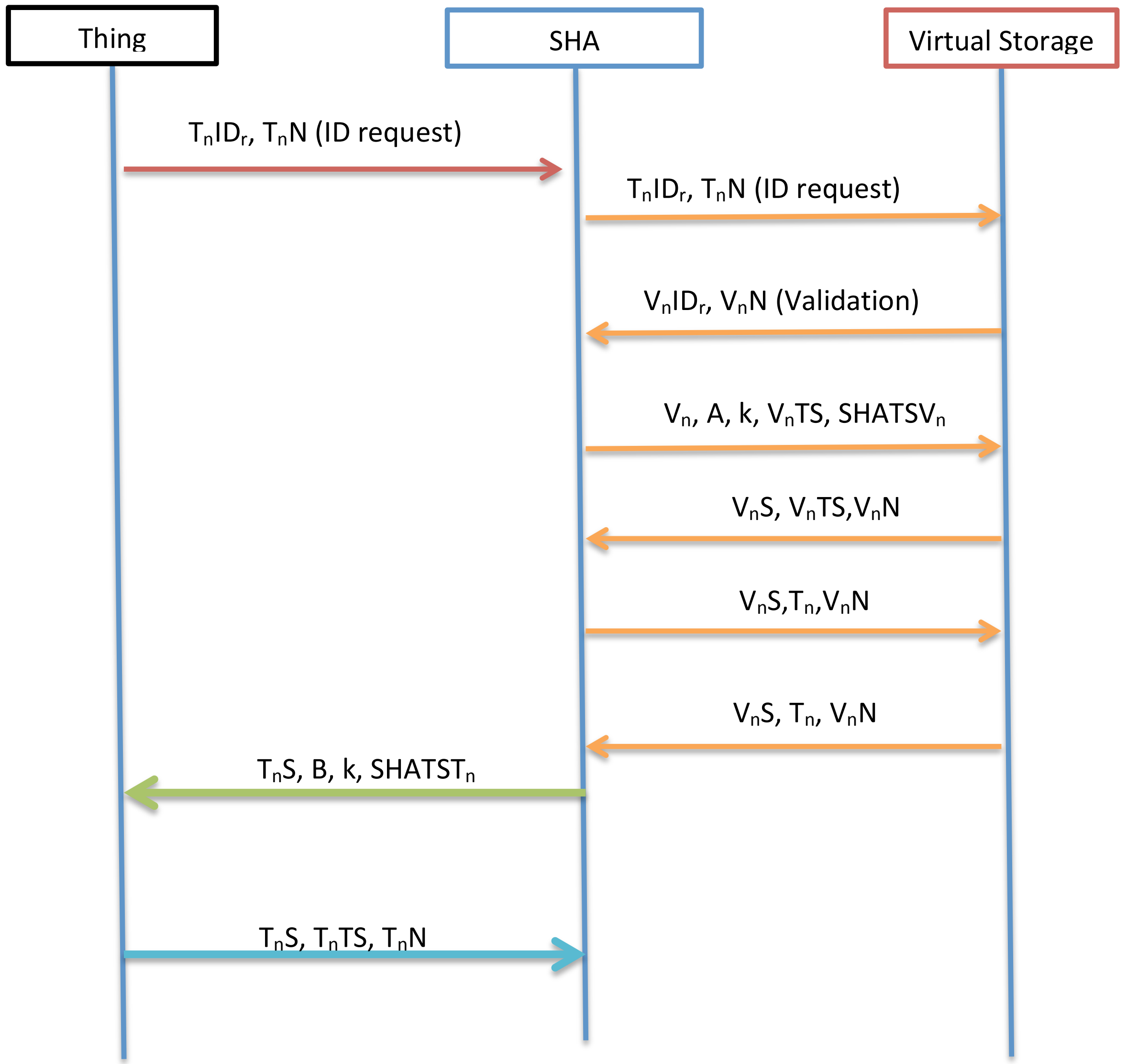


Figure 4.5: Sequence diagram for modelling AAL and ESS

As depicted in Figure 4.5, our proposed architecture functionally operates with fewer loads on the device level, emphasising the need for a lightweight solution for authentication. There are few number of operations pushed to the device level as compared to those between SHA and Virtual Storage.

4.5 Smart Home Security Scenarios

The security scenarios that helped the moulding of the architecture presented in this work were not confined to properly modelled settings. An informal approach to contextualise some typical scenarios was used. The reason for a random approach is the unpredictable behaviour of inhabitants of a Smart Home at any given moment as highlighted by Amiribesheli, Benmansour, and Bouchachia (2015); Guesgen and Marsland (2016) ; Orpwood (2012); Tran, Marsland, Dietrich, Guesgen, and Lyons (2010). We therefore had different hypothetical cases for consideration, which were as close to reality as possible. The following are sample scenarios, which were considered.

4.5.1 AAL Scenario 1

In this scenario, we modelled a setup where there is a homebound patient who is monitored for vital signs remotely by the family doctor. The family doctor mostly operates from his/her private practice. The focus of this scenario was to depict how the patient's environment is managed and monitored through IoT enabled devices, strategically mounted inside the house and around their body. In essence, this scenario gives a simplified setup where there is not much heterogeneity in terms of functionality but coordinated efforts towards one goal, though the devices are functionally and strategically unique.

The Dolev Yao (1983) threat model (detailed in Chapter 5, Section 5.3) was then applied to the setup. As our main research focus was on authentication, we remark that no security concerns were highlighted in all the scenarios presented and any results analysed in Chapter 5.

4.5.2 AAL and ESS Scenario 2

As a more function intense environment, Scenario 2 was modelled in such a way that different sets of application demands for IoT devices enabling the required AAL setup were reflected. We presented a setup where we had a homebound patient, two children (one going to kindergarten and the other to primary school). This presented a setup that had different sources of data requests. The family doctor would be interested in monitoring his/her patient and at the same time the parents of the children would also want to monitor both their home bound patient and the children at any moment, especially during school pickup and drop off times for children, and medicine intake at scheduled times for their home bound patient.

This created a demanding setup where requests could be prompted at any given time and the need to validate the authenticity of the requests became critical. In this scenario, the different sensors and actuators building up the smart space were activated at varying intervals. This created a heterogeneous setup from the functional perspective and from the architectural side as well. The different actions by the inhabitants of our modelled typical AAL setup triggered different sharing and coordination of actions by the devices at the M2M level.

4.5.3 Other scenarios

To create as closely as possible to a real Smart Home setup, whichever scenario we initially started with was modified at different dimensions guided by the domain of AAL and ESS. As such, no constant setup was always modelled. Therefore, we ended up drawing some key possible applications for both AAL and ESS, which are already summarised in Figure 4.3 and Figure 4.4

4.6 Testing of the Security Features on the Architecture

Using the SCYTHER tool as highlighted in Chapter 3, the architecture was remodelled into a Security Protocol Description Language (SPDL). The SPDL version of the architecture is presented in Chapter 5 for analysis, as that was the main input to the security analysis of the authentication architecture presented in Figure 4.2, using formal methods.

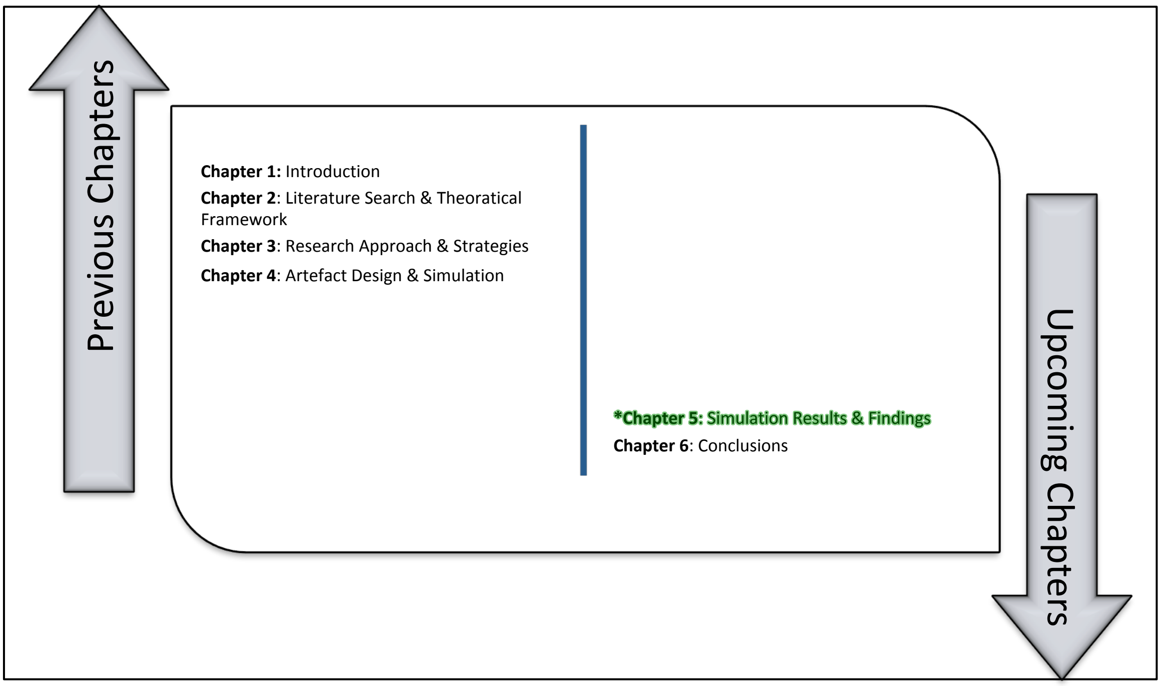
4.7 Chapter Summary

This chapter gave an account of the process of coming up with the authentication architecture from the initial unrefined prototype to the recommended architecture. The proposed architecture was then presented which was preceded by an explanation of the key components that formulate the authentication architecture, which are the bootstrapping phase and the authentication phase. The highlight of the roles played by the various actors in the authentication architecture and the visual display of the architecture was presented in this Chapter.

Detailed in this chapter is the explanation and outline of how the simulation of the architecture was done. To give a contextual functional representation of the application domain, the AAL and ESS scenario setups and possible applications are highlighted.

How the security features were tested which is a precursor to Chapter 5, was also highlighted in this chapter. Therefore, the next chapter presents the testing process and analyses the results thereof.

CHAPTER 5: SIMULATION RESULTS AND FINDINGS



Previous Chapters
Chapter 1: Introduction
Chapter 2: Literature Search & Theoratical Framework
Chapter 3: Research Approach & Strategies
Chapter 4: Artefact Design & Simulation
***Chapter 5:** Simulation Results & Findings
Chapter 6: Conclusions
Upcoming Chapters

As the pinnacle of this research work, this chapter provides the findings from the simulation outlined in chapter 4. This chapter is mainly focused on meeting the requirements of research Objective 4: "Evaluate the proposed secure solution for correctness and computational efficiency."

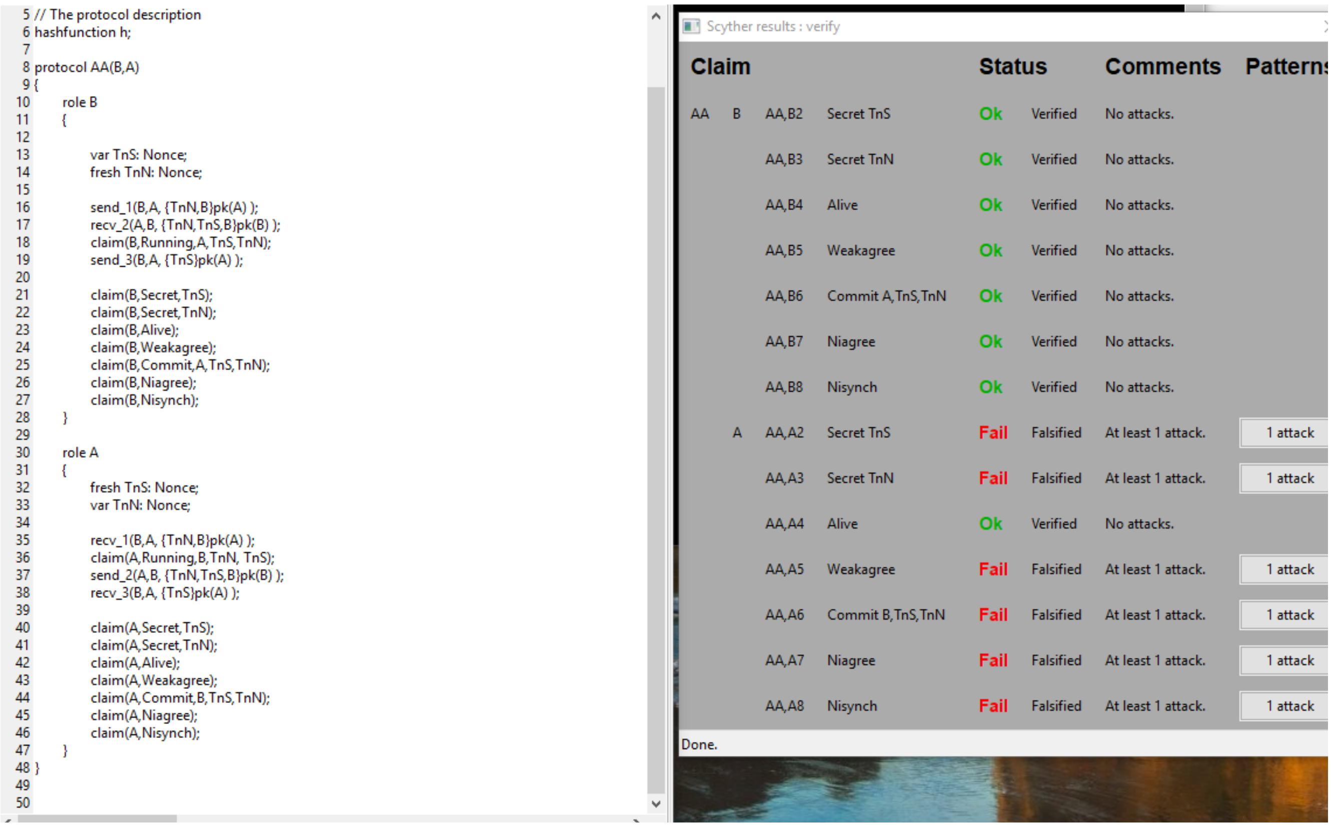
5.1 Chapter Overview

Any research is measured on the output that it presents on the table. The novelty of this research can be validated with what is presented in this chapter. Based on the simulation runs for our proposed authentication architecture, which is the main deliverable of this work, some key conclusions were reached. Formal methods for analysis were employed to draw some inferences. We remark that the results presented here may not be exhaustive but they do outline the key focal points that validate our work to a satisfactory level. Based on expert reviews from snippets of work published and still to be published in high impact conferences and journals, we were able to optimise our architecture and use state of the art simulation tools currently in use in industry and academic circles.

Chapter Organisation: The chapter sets off by reviewing the results of the simulation scenarios in Section 5.2. Of interest in terms of results analysis is what Section 5.3 summarises in light of the Dolev Yao model, whose results were observed while running the simulation for different stages of optimisation of the architecture. Key security features were tested on our proposed architecture and this is presented in Section 5.4. On a comparison basis, our architecture was tested for lightweight features, which is summarised in Section 5.5 and Computational efficiency and scalability, summarised in Section 5.6. The CIA triad analysis, which was the theoretical framework that our architecture was designed around, is reviewed in Section 5.7, where the completeness of the **AA** architecture (herein our proposed Authentication Architecture) is tested. Section 5.8 serves as a wrap up of the main points of this Chapter.

5.2 Scenario Simulation Results

This section provides a presentation of the journey of designing and optimising the authentication architecture, with particular focus on how the SCYTHER tool managed to help in that journey. As can be observed from Figure 5.1 to Figure 5.13, the raw process of handling threats and hardening the architecture till it could meet the intended security needs is highlighted.



```
// The protocol description
hashfunction h;

protocol AA(B,A)
{
        role B
        {

                var TnS: Nonce;
                fresh TnN: Nonce;

                send_1(B,A, {TnN,B}pk(A) );
                recv_2(A,B, {TnN,TnS,B}pk(B) );
                claim(B,Running,A,TnS,TnN);
                send_3(B,A, {TnS}pk(A) );

                claim(B,Secret,TnS);
                claim(B,Secret,TnN);
                claim(B,Alive);
                claim(B,Weakagree);
                claim(B,Commit,A,TnS,TnN);
                claim(B,Niagree);
                claim(B,Nisynch);
        }

        role A
        {
                fresh TnS: Nonce;
                var TnN: Nonce;

                recv_1(B,A, {TnN,B}pk(A) );
                claim(A,Running,B,TnN, TnS);
                send_2(A,B, {TnN,TnS,B}pk(B) );
                recv_3(B,A, {TnS}pk(A) );

                claim(A,Secret,TnS);
                claim(A,Secret,TnN);
                claim(A,Alive);
                claim(A,Weakagree);
                claim(A,Commit,B,TnS,TnN);
                claim(A,Niagree);
                claim(A,Nisynch);
        }
}
```

Scyther results : verify

Claim				Status		Comments	Pattern
AA	B	AA,B2	Secret TnS	Ok	Verified	No attacks.	
		AA,B3	Secret TnN	Ok	Verified	No attacks.	
		AA,B4	Alive	Ok	Verified	No attacks.	
		AA,B5	Weakagree	Ok	Verified	No attacks.	
		AA,B6	Commit A,TnS,TnN	Ok	Verified	No attacks.	
		AA,B7	Niagree	Ok	Verified	No attacks.	
		AA,B8	Nisynch	Ok	Verified	No attacks.	
	A	AA,A2	Secret TnS	Fail	Falsified	At least 1 attack.	1 attack
		AA,A3	Secret TnN	Fail	Falsified	At least 1 attack.	1 attack
		AA,A4	Alive	Ok	Verified	No attacks.	
		AA,A5	Weakagree	Fail	Falsified	At least 1 attack.	1 attack
		AA,A6	Commit B,TnS,TnN	Fail	Falsified	At least 1 attack.	1 attack
		AA,A7	Niagree	Fail	Falsified	At least 1 attack.	1 attack
		AA,A8	Nisynch	Fail	Falsified	At least 1 attack.	1 attack

Done.

Figure 5.1:Screenshot of the protocol description with attacks

Based on the first initial runs of the formal evaluation of the architecture, as can be observed from Figure 5.1, six (6) attacks are shown. What could be picked from the identified attacks was lack of security features that could enhance the deemed security requirements of our architecture. We could pick that the protection of the thing's allocated ID by SHA; there was a need to enhance the security parameters thereof. The fact that **TnS** and **TnN** are compromised; the whole architecture was at risk hence all security claims could not be validated.

After selecting a successful attack, for example one on secret **TnS**, the trace maps shown in Figures 5.2, 5.3 and 5.4 were displayed in that order. We could visually see the point of attack as shown in Figures 5.3 and 5.4 (which is a continuation of Figure 5.3, hence Part A and Part B suffix). The ability to visually display the attack traces is one strength we could pick from how the SCYTHER tool functions, hence separating it from existing alternatives. Visuals helped in making informed decisions as the challenges could be observed clearly.

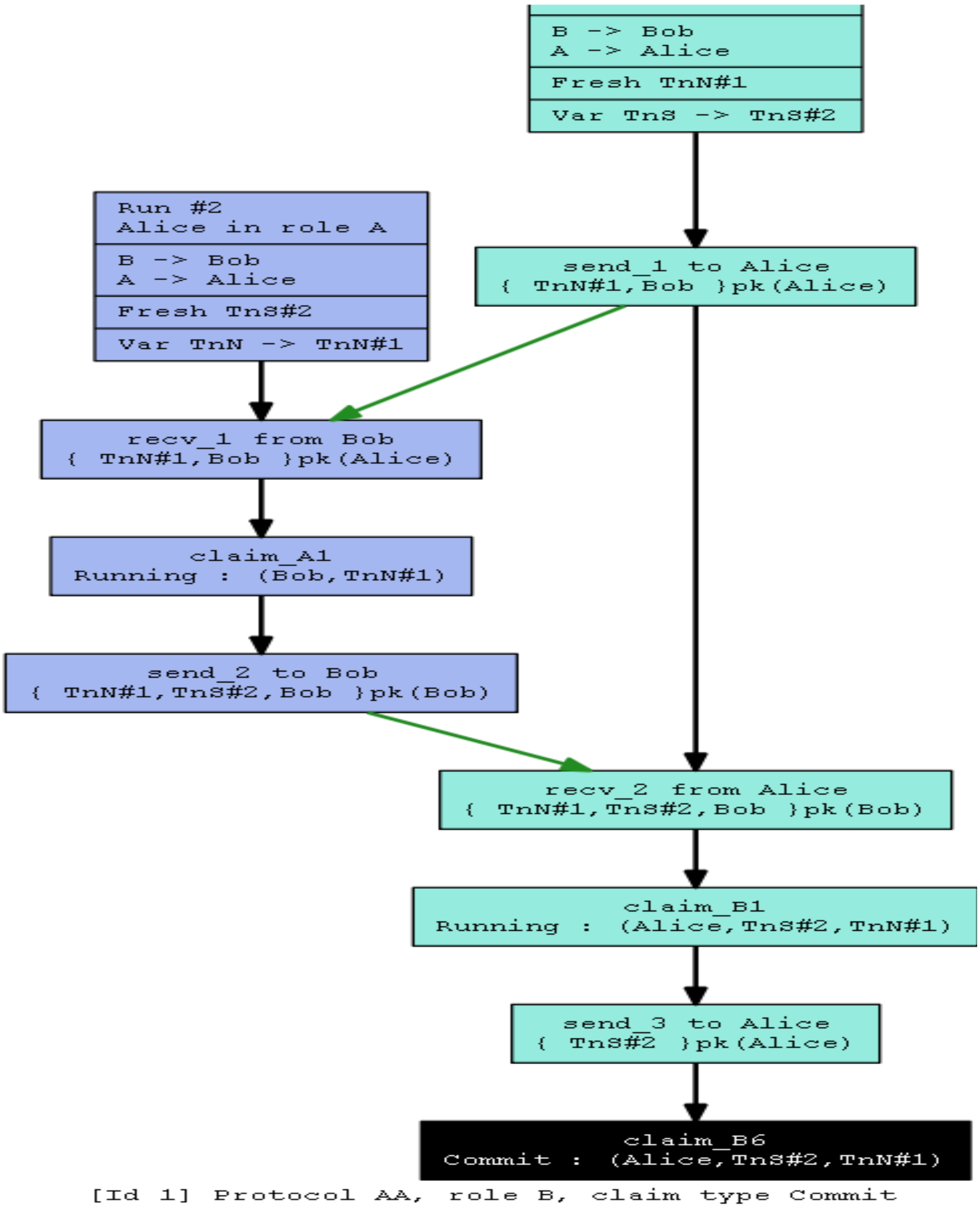


Figure 5.2: The trace pattern for bootstrapping (protocol with attacks)

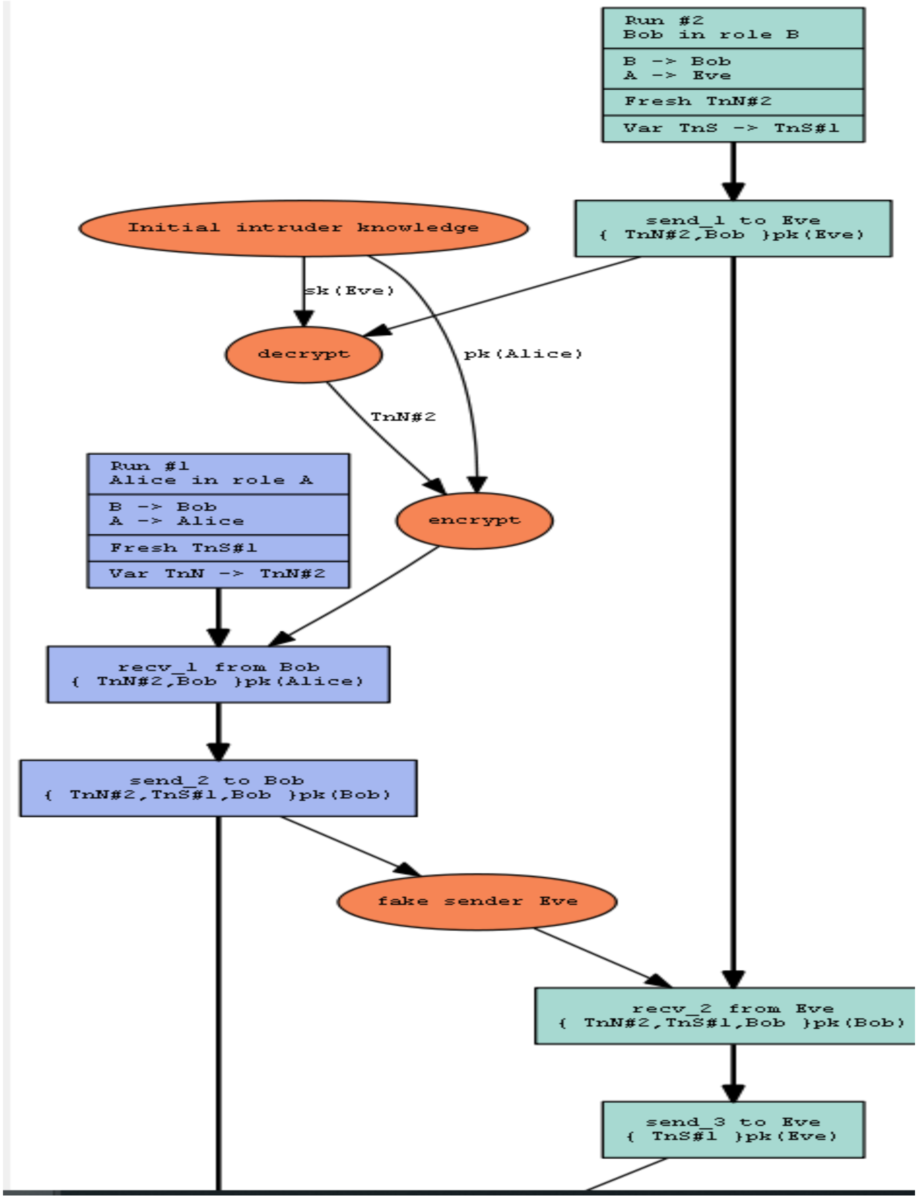


Figure 5.3: Trace pattern with attacks- Part A

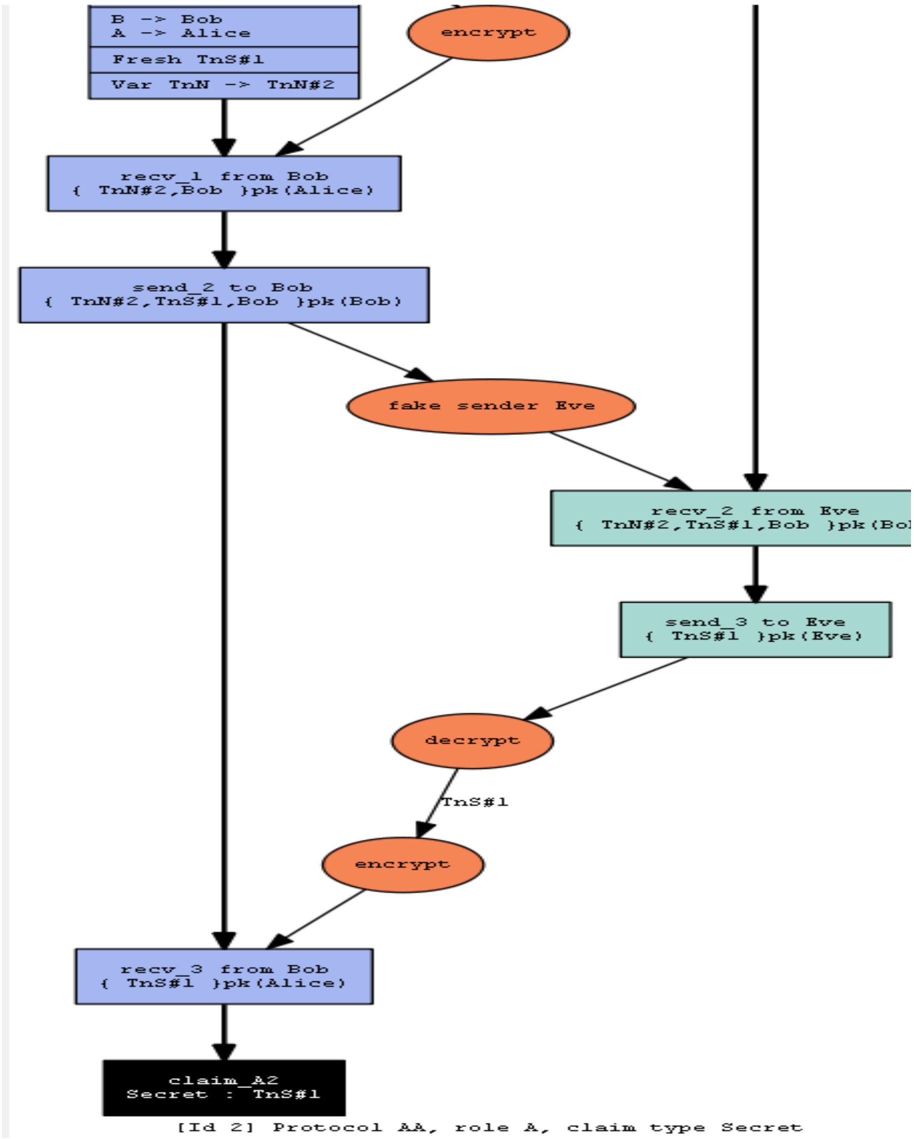


Figure 5.4:Trace pattern with attacks – Part B

Checking the characterisation of the protocol with attacks as displayed in Figure 5.5 helped to understand where the roles of authentic functionalities of our protocol for the architecture were violated. In this scenario, the moment a request for an ID was sent to SHA, lack of adequate security parameters enabled an intruder 'Eve' to inject a fake ID that was then sent to Thing n. Unknowingly, Thing n accepted that ID as if it was coming from SHA, and that compromised the entire architecture.

Using the SCYTHER tool, we could set different parameters for testing, ranging from the verification parameters where we had to set the maximum number of runs; in our case we varied our runs incrementally in multiples of 5, from 5 up to 100 runs. Figure 5.6 shows the screen for setting the simulation parameters. On advanced features, we opted for best attacks and also checked for all attacks. Another variable that could be set was the maximum number of patterns per claim; this could give the different possible attack vectors an adversary could make use of. We had to choose 10, as that was exhaustive enough, otherwise if a protocol will have more than 10 attack patterns, it is as good as un-implementable, because the time it takes to troubleshoot might as well be used to construct a fresh protocol.

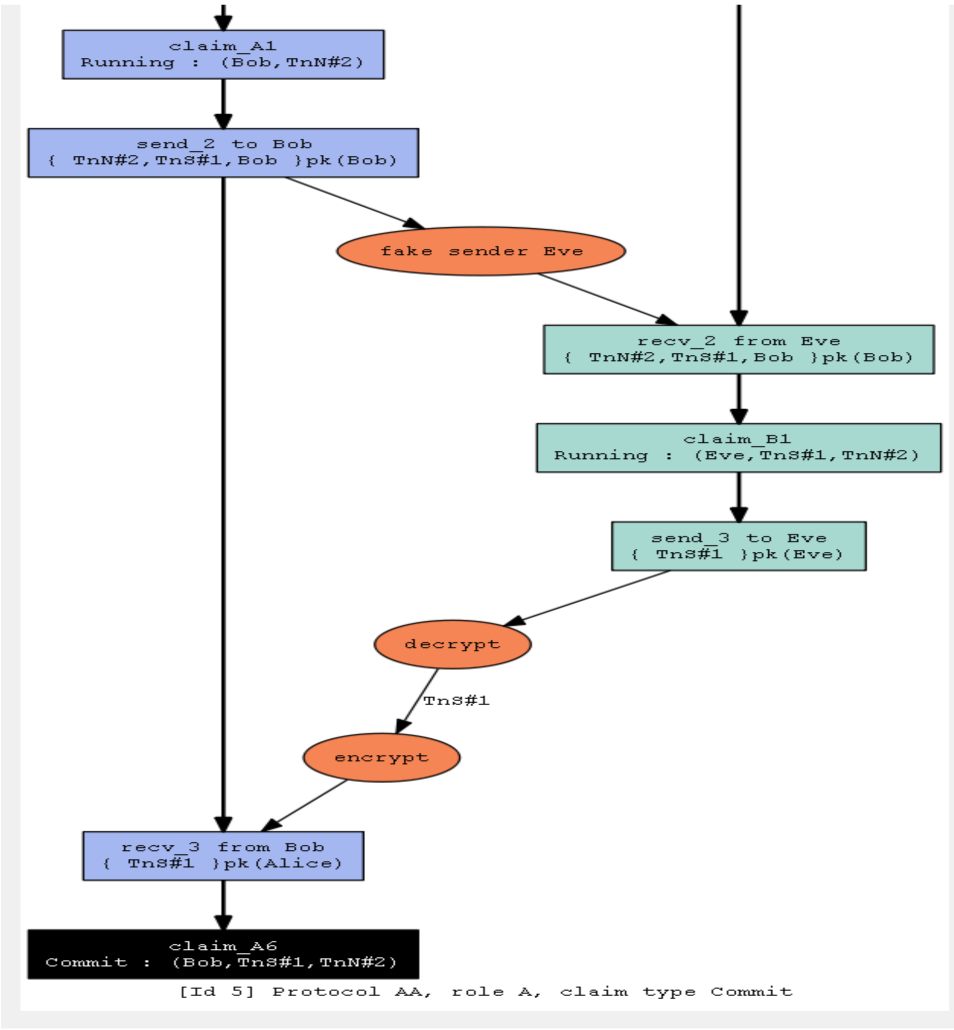
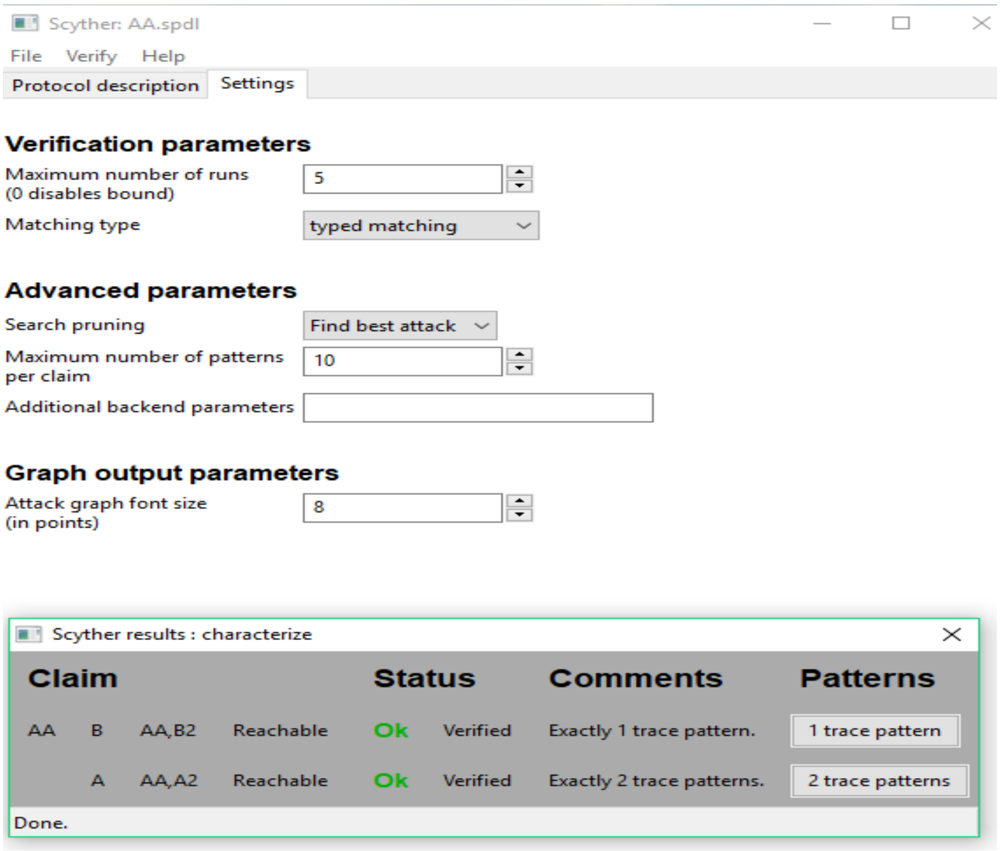


Figure 5.5:Characterisation (protocol with attacks)

In the case of an unsecure protocol that we started with, we only had 2 trace patterns picked as displayed at the bottom of Figure 5.6 for the Authentication phase that experienced serious attacks.



Verification parameters

Maximum number of runs (0 disables bound): 5

Matching type: typed matching

Advanced parameters

Search pruning: Find best attack

Maximum number of patterns per claim: 10

Additional backend parameters:

Graph output parameters

Attack graph font size (in points): 8

Claim				Status		Comments	Patterns
AA	B	AA,B2	Reachable	Ok	Verified	Exactly 1 trace pattern.	1 trace pattern
	A	AA,A2	Reachable	Ok	Verified	Exactly 2 trace patterns.	2 trace patterns

Done.

Figure 5.6: Settings of simulation parameters

After verifying the identified attacks, the trace patterns shown in Figures 5.7, 5.8 and 5.9 were displayed, signalling the magnitude of one error and how its effects could disrupt the proper functionality of our proposed architecture.

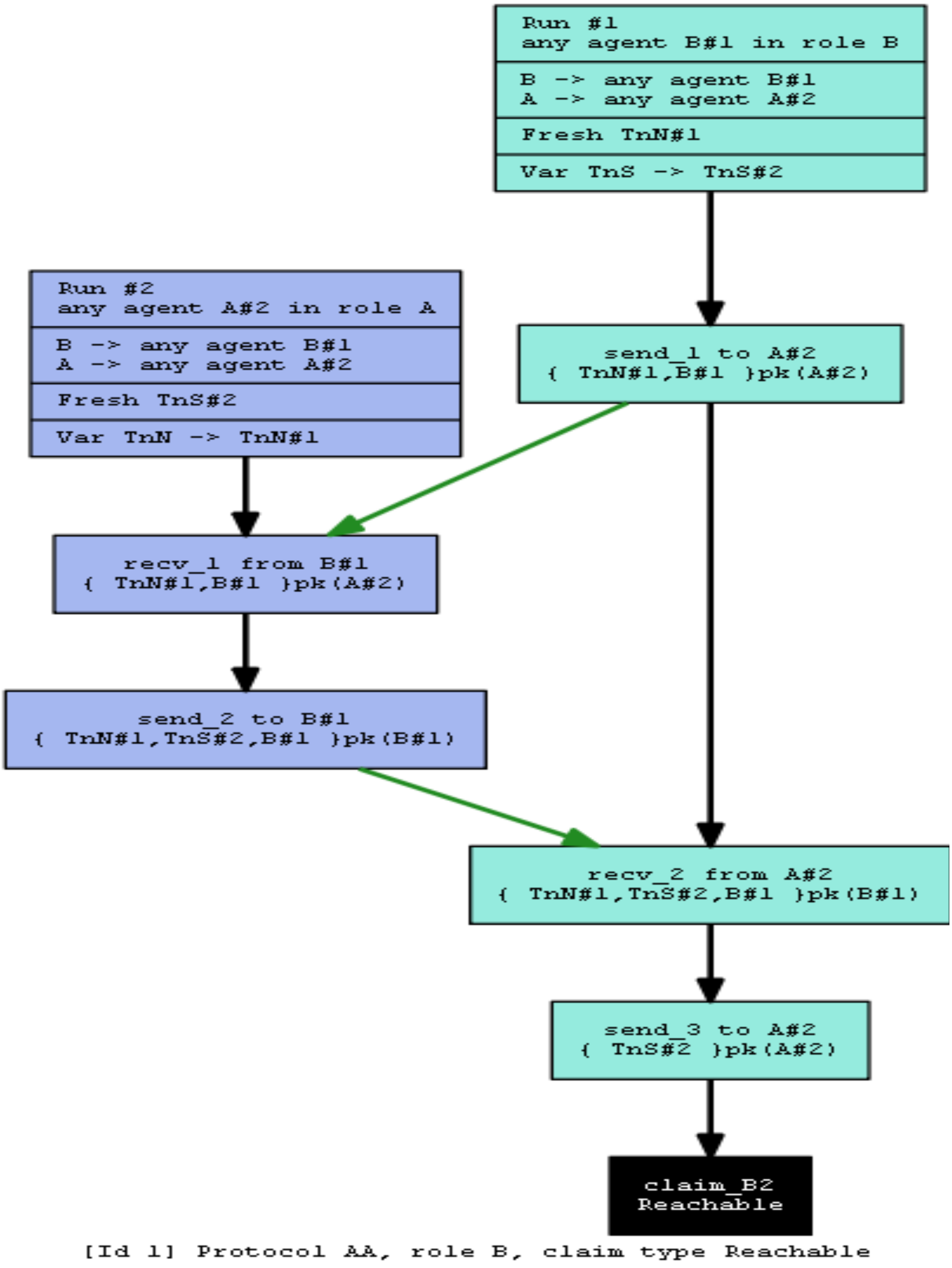


Figure 5.7: Trace pattern 1 (with attacks)

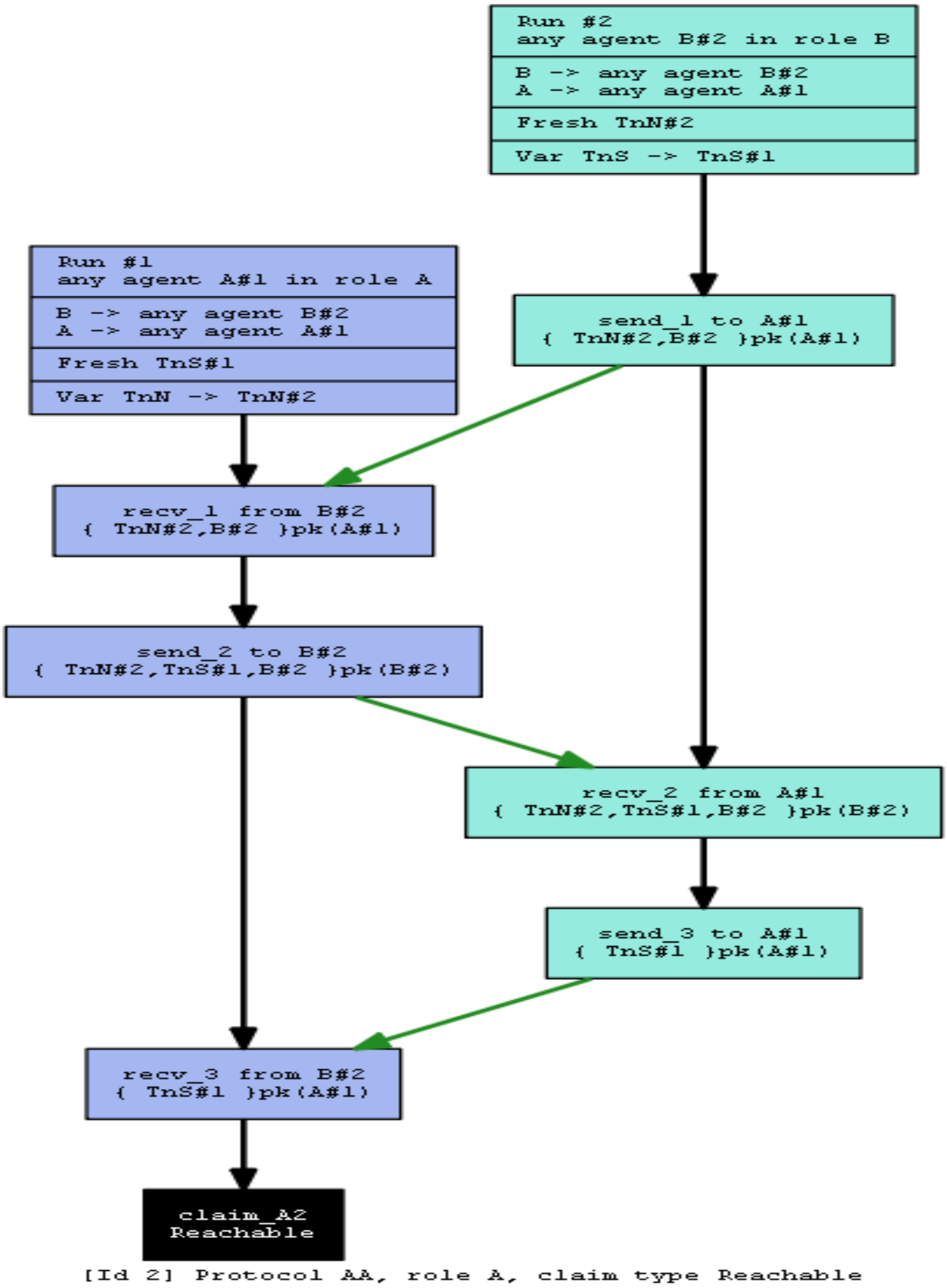


Figure 5.8: Trace pattern 2 (with attacks)

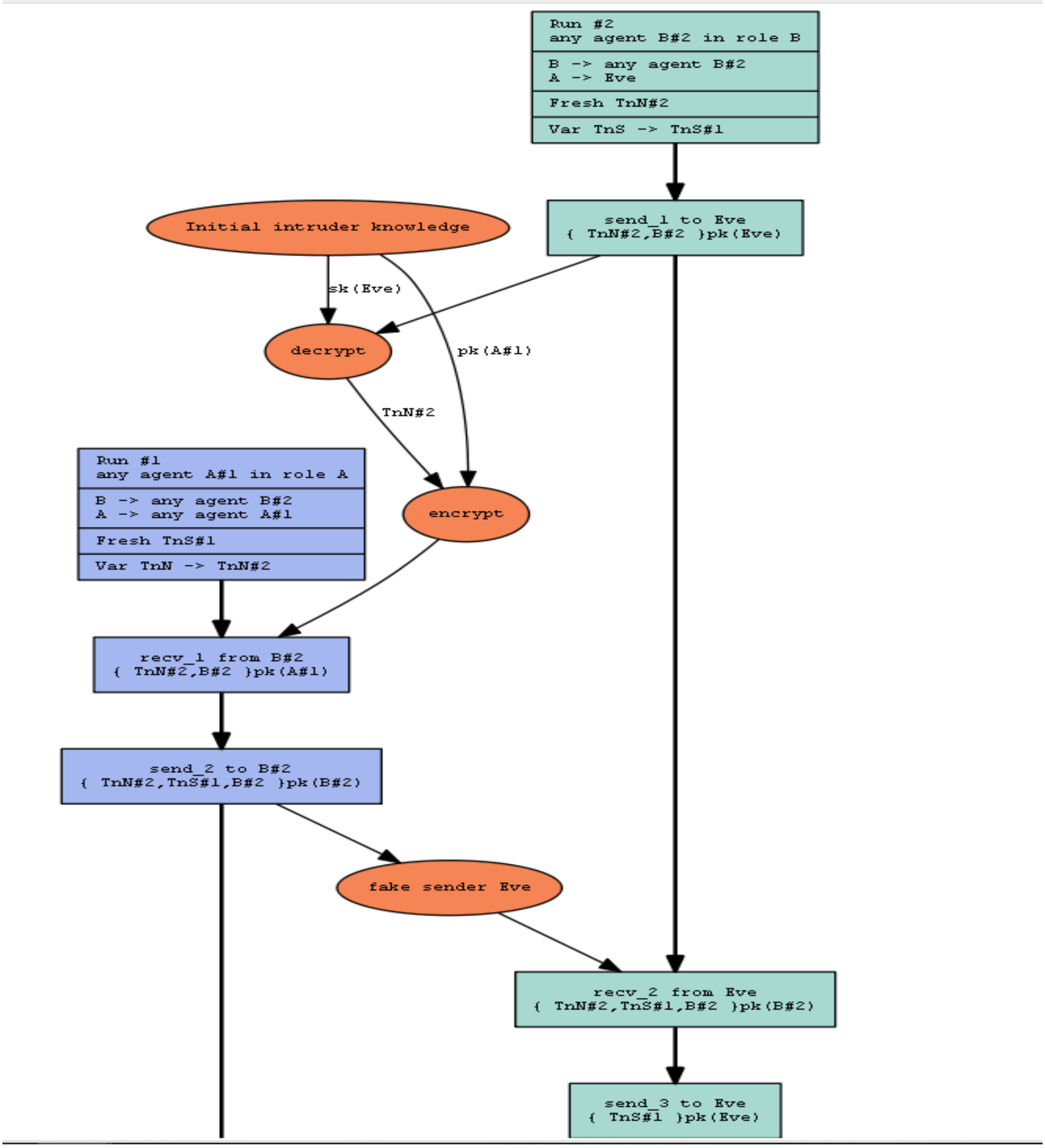
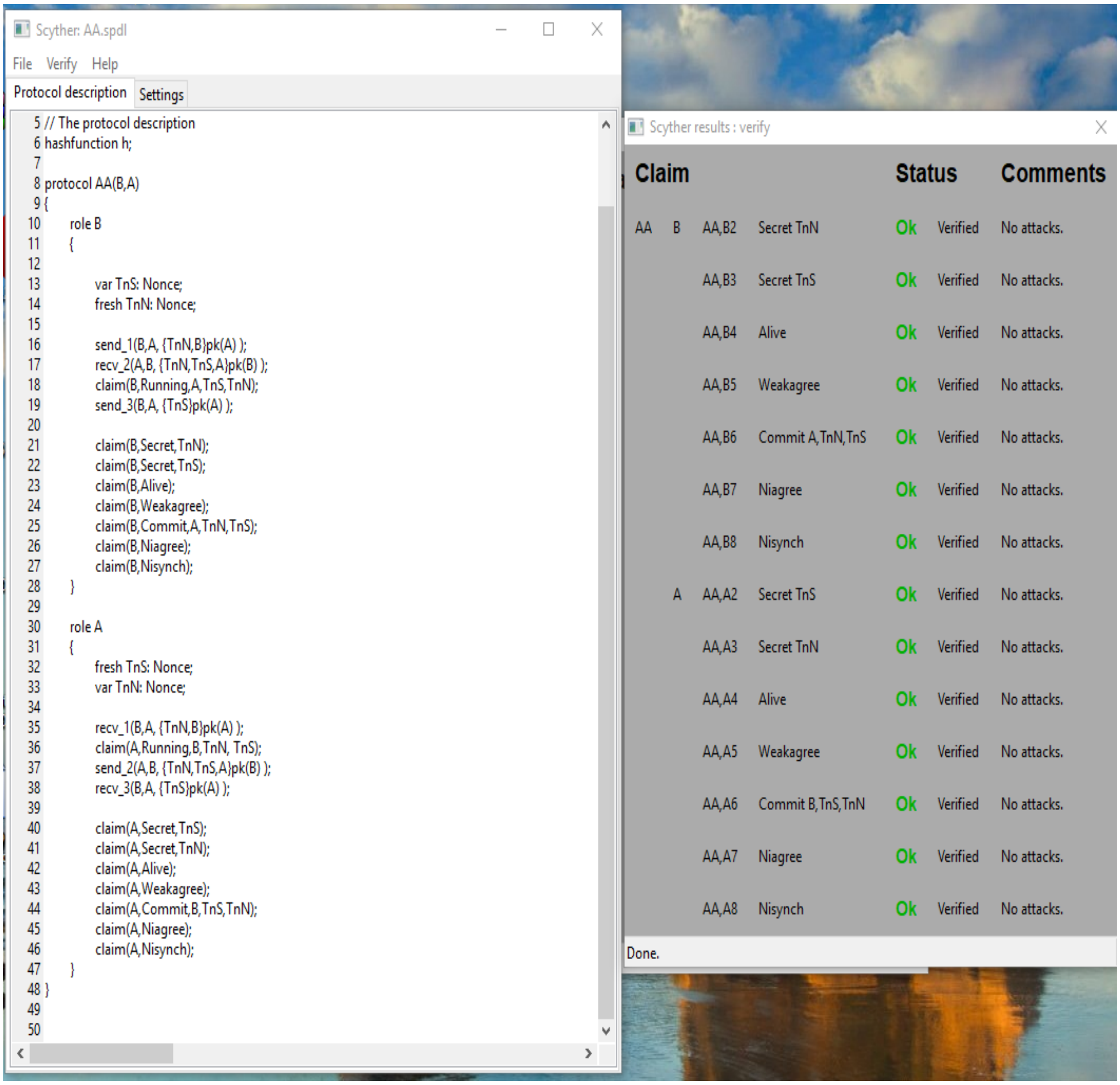


Figure 5.9: Trace pattern with attacks

We then had to address the attacks identified, enabling us to produce an attack free architecture as the protocol description came out clean of SCYTHER as shown in Figure 5.10.

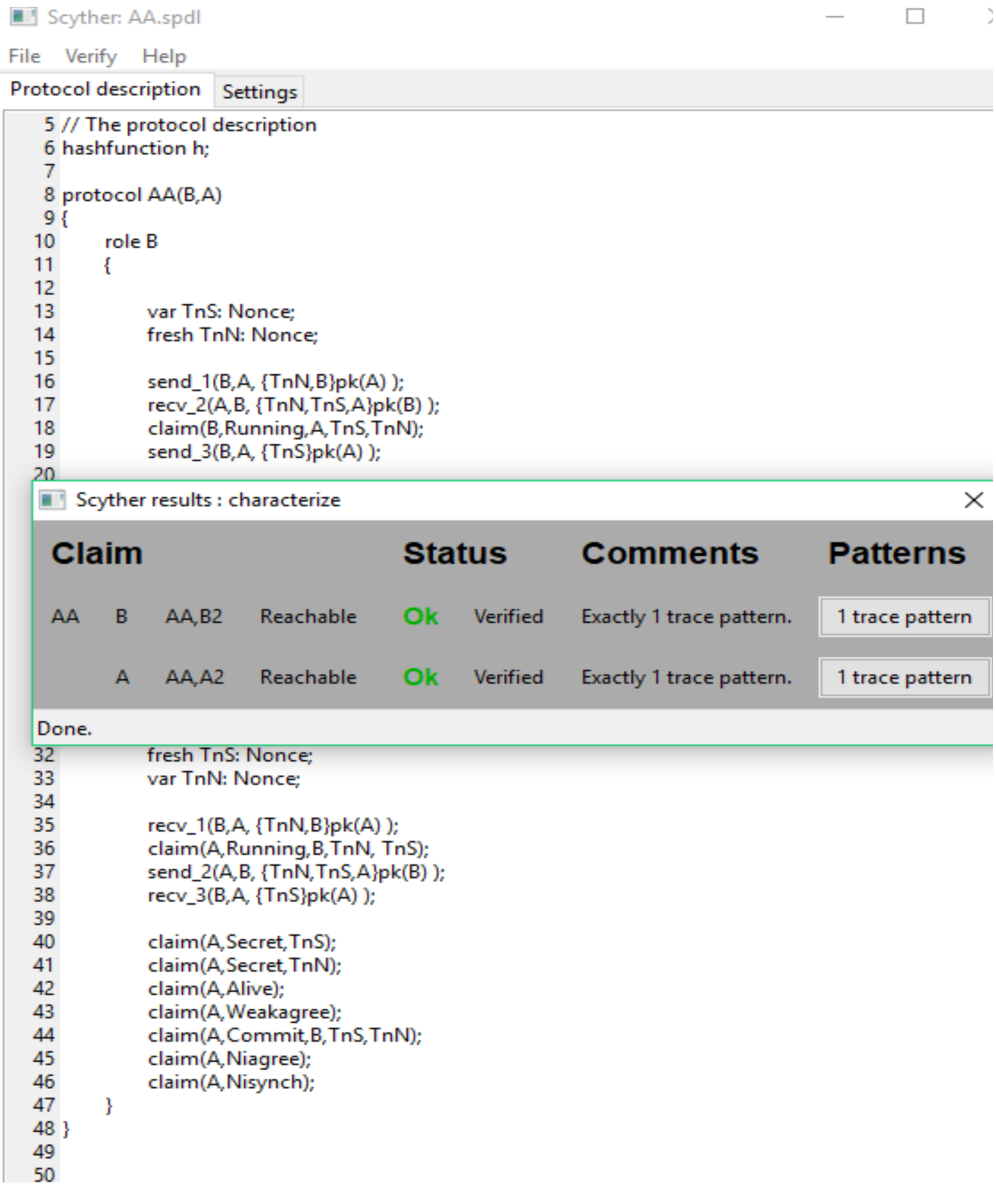


```
// The protocol description
hashfunction h;

protocol AA(B,A)
{
	role B
	{

		var TnS: Nonce;
		fresh TnN: Nonce;

		send_1(B,A, {TnN,B}pk(A) );
		recv_2(A,B, {TnN,TnS,A}pk(B) );
		claim(B,Running,A,TnS,TnN);
		send_3(B,A, {TnS}pk(A) );

		claim(B,Secret,TnN);
		claim(B,Secret,TnS);
		claim(B,Alive);
		claim(B,Weakagree);
		claim(B,Commit,A,TnN,TnS);
		claim(B,Niagree);
		claim(B,Nisynch);
	}

	role A
	{
		fresh TnS: Nonce;
		var TnN: Nonce;

		recv_1(B,A, {TnN,B}pk(A) );
		claim(A,Running,B,TnN, TnS);
		send_2(A,B, {TnN,TnS,A}pk(B) );
		recv_3(B,A, {TnS}pk(A) );

		claim(A,Secret,TnS);
		claim(A,Secret,TnN);
		claim(A,Alive);
		claim(A,Weakagree);
		claim(A,Commit,B,TnS,TnN);
		claim(A,Niagree);
		claim(A,Nisynch);
	}
}
```

```
Claim                                Status        Comments
AA  B  AA,B2  Secret TnN             Ok  Verified  No attacks.
       AA,B3  Secret TnS             Ok  Verified  No attacks.
       AA,B4  Alive                  Ok  Verified  No attacks.
       AA,B5  Weakagree              Ok  Verified  No attacks.
       AA,B6  Commit A,TnN,TnS       Ok  Verified  No attacks.
       AA,B7  Niagree                Ok  Verified  No attacks.
       AA,B8  Nisynch                Ok  Verified  No attacks.
    A  AA,A2  Secret TnS             Ok  Verified  No attacks.
       AA,A3  Secret TnN             Ok  Verified  No attacks.
       AA,A4  Alive                  Ok  Verified  No attacks.
       AA,A5  Weakagree              Ok  Verified  No attacks.
       AA,A6  Commit B,TnS,TnN       Ok  Verified  No attacks.
       AA,A7  Niagree                Ok  Verified  No attacks.
       AA,A8  Nisynch                Ok  Verified  No attacks.
Done.
```

Figure 5.10: Attack free protocol

Figure 5.11 shows only 1 trace pattern for the bootstrapping (role B) and the authentication phase (role A). This was a clear indication that there are no other possible routes of communication; hence the architecture could be rendered as secure.



```
// The protocol description
hashfunction h;

protocol AA(B,A)
{
	role B
	{

		var TnS: Nonce;
		fresh TnN: Nonce;

		send_1(B,A, {TnN,B}pk(A) );
		recv_2(A,B, {TnN,TnS,A}pk(B) );
		claim(B,Running,A,TnS,TnN);
		send_3(B,A, {TnS}pk(A) );
```

Scyther results : characterize

Claim				Status		Comments	Patterns
AA	B	AA,B2	Reachable	Ok	Verified	Exactly 1 trace pattern.	1 trace pattern
	A	AA,A2	Reachable	Ok	Verified	Exactly 1 trace pattern.	1 trace pattern

Done.

```
		fresh TnS: Nonce;
		var TnN: Nonce;

		recv_1(B,A, {TnN,B}pk(A) );
		claim(A,Running,B,TnN, TnS);
		send_2(A,B, {TnN,TnS,A}pk(B) );
		recv_3(B,A, {TnS}pk(A) );

		claim(A,Secret,TnS);
		claim(A,Secret,TnN);
		claim(A,Alive);
		claim(A,Weakagree);
		claim(A,Commit,B,TnS,TnN);
		claim(A,Niagree);
		claim(A,Nisynch);
	}
}
```

Figure 5.11: Trace patterns for role B and A respectively

In a visual approach prompting for the trace pattern for the bootstrapping phase for the attack free protocol as displayed in Figure 5.12, it could be noted that there are no differences with the initially presented trace pattern in Figure 5.2, since the bootstrapping phase for the protocol with attacks did not affect the bootstrapping phase.

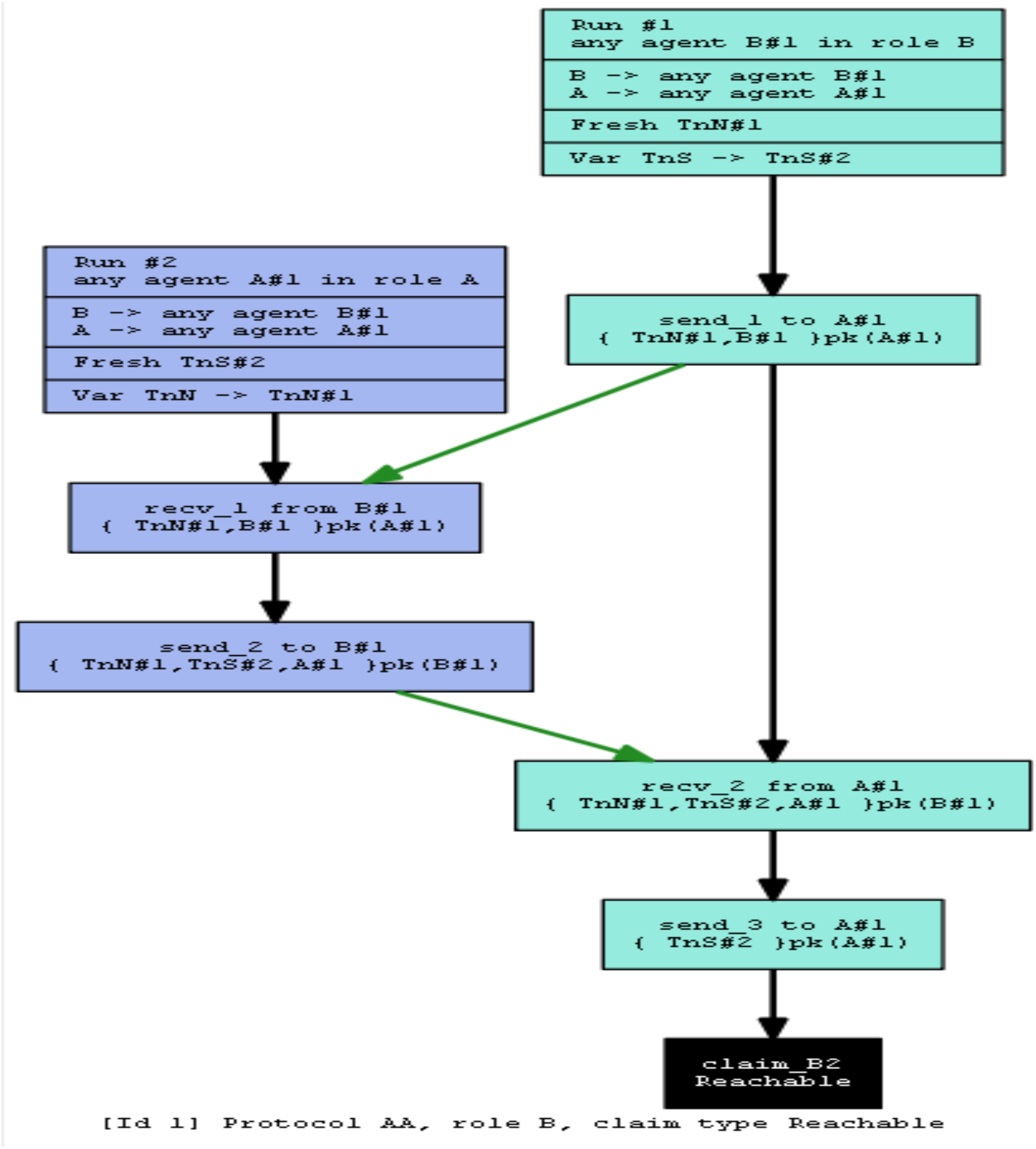


Figure 5.12: Trace pattern for Bootstrapping (protocol without attacks)

In the same fashion, Figure 5.13 displays the trace pattern for an attack free authentication phase. This indicates that Thing n will be able to send a request to SHA and have that request processed securely.

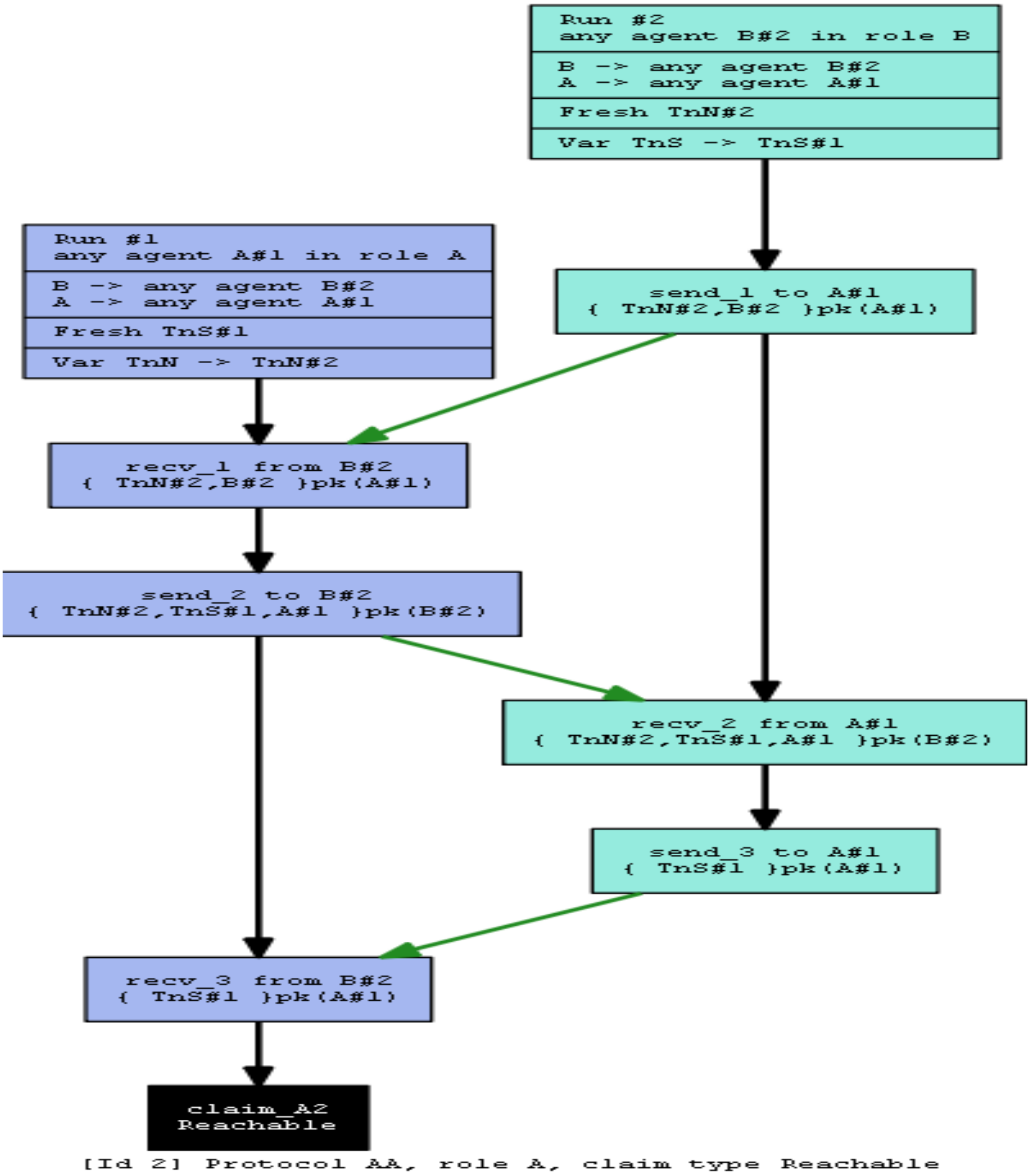
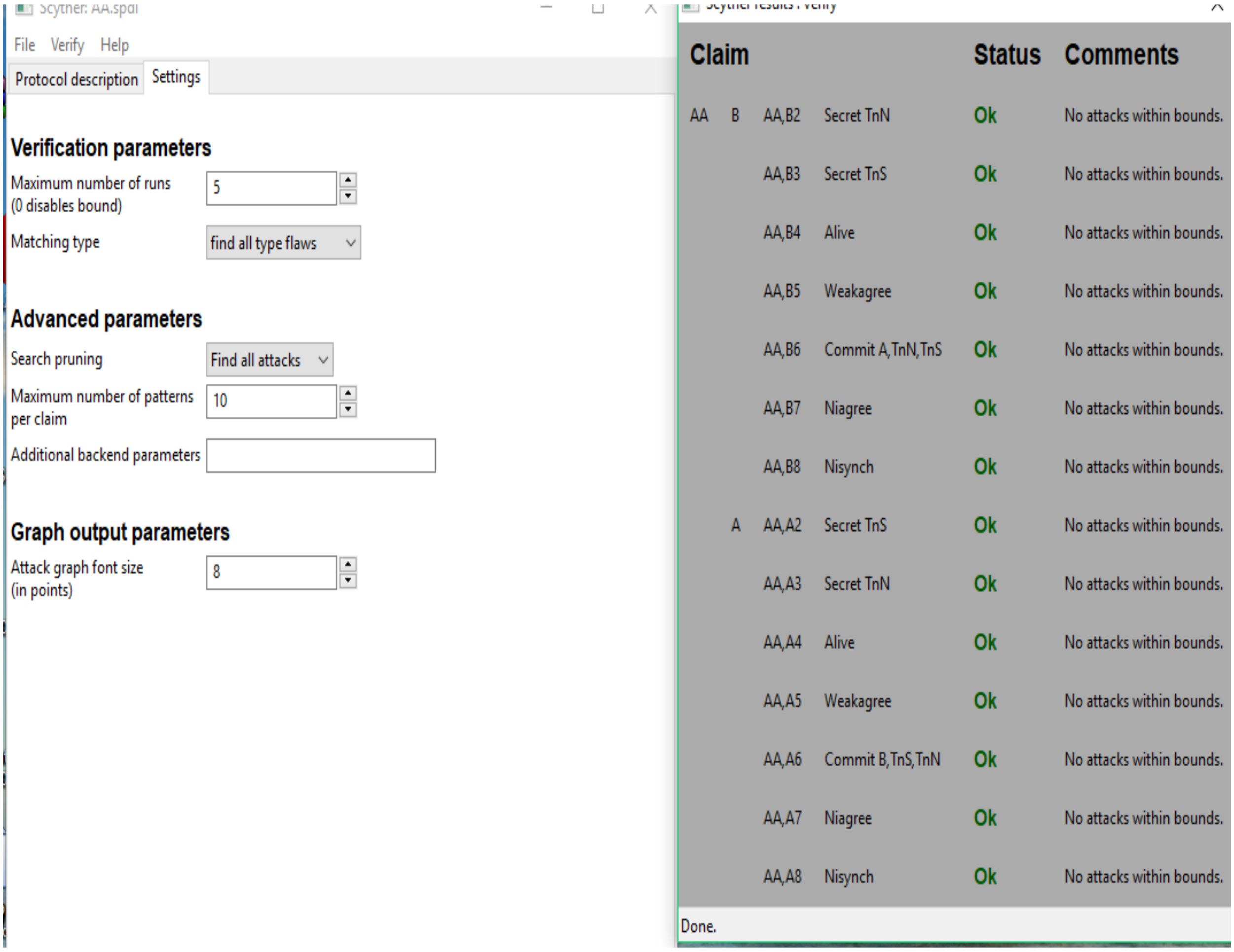


Figure 5.13: Trace pattern for Authentication (protocol without attacks)

Figure 5.14 is a display of the initial runs before incrementally varying the runs to the maximum of 100 in multiples of 5 as earlier mentioned. Still we got the same results for each run, which helped us conclude that our protocol for **AA** was now secure.



Verification parameters

Maximum number of runs (0 disables bound): 5

Matching type: find all type flaws

Advanced parameters

Search pruning: Find all attacks

Maximum number of patterns per claim: 10

Additional backend parameters:

Graph output parameters

Attack graph font size (in points): 8

Claim				Status	Comments
AA	B	AA,B2	Secret TnN	Ok	No attacks within bounds.
		AA,B3	Secret TnS	Ok	No attacks within bounds.
		AA,B4	Alive	Ok	No attacks within bounds.
		AA,B5	Weakagree	Ok	No attacks within bounds.
		AA,B6	Commit A,TnN,TnS	Ok	No attacks within bounds.
		AA,B7	Niagree	Ok	No attacks within bounds.
		AA,B8	Nisynch	Ok	No attacks within bounds.
	A	AA,A2	Secret TnS	Ok	No attacks within bounds.
		AA,A3	Secret TnN	Ok	No attacks within bounds.
		AA,A4	Alive	Ok	No attacks within bounds.
		AA,A5	Weakagree	Ok	No attacks within bounds.
		AA,A6	Commit B,TnS,TnN	Ok	No attacks within bounds.
		AA,A7	Niagree	Ok	No attacks within bounds.
		AA,A8	Nisynch	Ok	No attacks within bounds.

Done.

Figure 5.14: Simulation settings

5.3 AA Architecture Review in the Context of the Dolev Yao Model

The essence of looking at possible attack models for our architecture was based on the underlying reasoning presented in Chapter 3. Ideally, the Dolev Yao model employs a black box model of cryptography, where an assumption is made of perfect cryptography. In that model of perfect cryptography, an intruder could not break cryptographic algorithm without the correct key pairs.

The Dolev Yao model also enforces the Kerckhoff’s principle. The principle, which maintains that the encryption and decryption algorithms are not secret as such, thus all the details except the keys are available to public knowledge hence they are easily accessible by the intruder.

The other quality worth noting from the Dolev Yao model is the empowerment endowed on the intruder. The intruder could act as a normal user of the network and we can consider that as one of the reasons why it was valid to consider this model as a true test of security. In our research context we found it appropriate to consider the Dolev Yao model as it could closely model a realistic representation as all Things in the smart space may not be all legit.

With the powers extended to the intruder, they can control the network hence being able to read all unencrypted messages, as well as intercept and send messages.

The fact that the Dolev Yao model presents an all-powerful intruder provided a relatively realistic representation of the probable real threat environment. In that sense, if the architecture was able to ensure security of the authentication process under this model, then it could reasonably be applied to the real world, without loss of generality, hence the assumption that the chosen cryptographic mechanisms are in good working terms.

The following section tested some of the possible scenarios, guided by the Dolev Yao model as outlined already in Chapter 3.

5.4 Testing of Security Features – Results

The following attacks were considered under different intruder actions based on our proposed architecture and the evaluations are summarised for each possible scenario here.

5.4.1 Outsider attack

We considered a scenario where an intruder may intend to intercept the communication between $\mathbf{T_1}$ (refrigerator) and the Smart Home Agent (**SHA**) by gaining the identity of $\mathbf{T_1}$. Thus the intruder can try to obtain ($\mathbf{T_1}$, $\mathbf{ID_r}$, $\mathbf{T_1N}$). In this case, it is difficult for the intruder to authenticate with **SHA** because $\mathbf{T_1}$ is protected by the random number ($\mathbf{T_1N}$) chosen by $\mathbf{T_1}$ as it initiated its communication with **SHA**.

Finding 1: **AA** is secure against outsider attacks by virtue of embracing the use of random numbers in protecting the bootstrapping process

5.4.2 Replay attack

We consider the possibility of an interception of the communication between the Virtual Storage (**VS**) and **SHA** during the authentication phase hence the attacker could obtain (**V_nS, V_nTS, V_nN**). This could be an attempt to login to **SHA**, hence the intruder may resend (**V_nS, V_nTS, V_nN**) to **SHA**. However, the successful authentication of the resent parameters by the intruder will be impossible because the timestamp **V_nTS** and the random number **V_nN** are not constants as they change with every authentication instance. It is going to be the same scenario, if for argument's sake, the intruder gains access to (**V_nS, V_nTS, V_nN**).

Finding 2: From this analysis, we maintain that replay attack would not be possible in our proposed architecture, as the use of fresh values for timestamps and random numbers is being enforced

5.4.3 Insider attack

In this scenario we considered the possibility of a rogue thing planted in the Smart Home, which imitate the actual **T_2** (temperature sensor). The rogue temperature sensor tries to login to the **SHA** by intercepting the communication between the original temperature sensor and **SHA** to obtain **B** (**_Equation 4.2, Chapter 4_**). The intruder will try and use a new time stamp **$SHATST_2$'** to produce a fake authentication (**T_nS, B, k, $SHATST_2$'**). When this is sent by the intruder imitating **SHA**, this will be an unsuccessful attack because **$SHATST_2$'** will not be able to validate **B** as **B'≠ B**.

Finding 3: **AA** is secure against insider attacks by making use of hash functions to protect the validation **k** and a set of parameters

5.4.4 Man-in-the middle attack

We considered a scenario where an intruder attempts to modify the values of **P_v** *(see Chapter 4, Equation 4.5 and 4.6 for more details*), to advance their own fake parameters for this to be possible, since: -

P_{vA} = B$\oplus$ ***V_nN*** *(see Chapter 4, equation 4.5)*

and

***P_{TA} = A⊕ T_nN** (see Chapter 4, equation 4.3)*

As well as **P_{vB} = h (V_n||k)** *(see Chapter 4, equation 4.6)*

The need to have the random parameter **T_nN** or **V_nN** and security parameter **k** which are exactly as the ones being used by the communicating entities is impossible as they have to satisfy the freshness requirement, hence not the same always.

Finding 4: **AA** is secure against man-in-the middle attack as it employs and enforces fresh values for the random numbers being used on the architecture both during bootstrapping and at authentication

5.4.5 Impersonating attack

We considered a setup where an intruder makes use of their fake **T_3'** to impersonate the legal **T_3** (door sensor) for the Smart Home application, in an attempt to access **SHA**. The rogue **T_3'** cannot pass the authentication phase as it may not possess the correct random number **T_3N** to ensure **P_T = P_T** (*see equation 4.3, Chapter 4*). In the same vein, an illegal **SHA** will not pass the authentication.

Finding 5: Making use of the hash function and fresh values for random numbers makes **AA** secure against impersonating attacks

5.4.6 Forward security

The proposed authentication architecture makes use of different identities for the Things, which are generated by **SHA** in a setup where rogue devices during the authentication phase might have gained access to **V_nTS** and **V_nN**, hence try to authenticate with **SHA** using these parameters. This will be unsuccessful because (**Vn||$_k$**) (*See Chapter 4, equation 4.6*) is protected by one-way hash function. In a similar setup, during **SHA** authentication phase, it is the same argument that it won't be possible to authenticate.

Finding 6: AA can be safely passed for addressing forward security which is made possible through the use of hash functions and combining security parameters with the identity of authenticating parties as well as making use of fresh timestamps for every instance of communication

5.5 Lightweight Features Assessment

Comparing similar authentication schemes (Jen-Ho et al., 2013; Shen et al., 2016; Yang & Lin, 2014) as already outlined in Chapter 2, the proposed scheme (**AA**) was evaluated in terms of cost versus the performance of other schemes. It was demonstrated that the proposed scheme **(AA)** is less expensive especially at the device level and the overall performance of the scheme in terms of total authentication cost, hence it can be safely concluded that **AA** is lightweight as displayed in Table 5.1.

Table 5.1: Thing side computation comparison

Scheme Computation	Yang et al. (1)	Yang et al. (2)	Shen et al.	AA
XOR (x)	4	2	1	0
Hash Function (y)	6	4	1	0
Concatenation function (z)	4	6	1	0
Computation Cost	4x+6y+4z	2x+6y+6z	1x+1y+1z	0x+0y+0z

5.6 Computational Efficiency Analysis

Evaluating the parameters such as the exclusive or operations, string concatenation and hash functions, a performance review of the proposed architecture against similar schemes as highlighted in Section 5.5, shows that it is lightweight even at the virtual storage side as displayed in Table 5.2.

Table.5.2: Virtual Storage side computation comparison

Scheme Computation	Yang et al. (1)	Yang et al. (2)	Shen et al.	AA
XOR (x)	*4*	*2*	*1*	*1*
Hash Function (y)	*6*	*4*	*1*	*1*
Concatenation function (z)	*4*	*6*	*1*	*1*
Computation Cost	*4x+6y+4z*	*2x+6y+6z*	*1x+1y+1Z*	*1x+1y+1z*

5.7 The Architecture - CIA triad Analysis

"The CIA triad provides a very simple and convenient model for both discovering and representing the security needs of your IoT device" (Baker, n.d., p. 6). Despite existing principles on security such as the CIA, the five pillars of information assurance (which are Confidentiality, Integrity, Availability, Authenticity and Non-repudiation) and Parkerian Haxad (Confidentiality, Integrity, Availability, Authenticity, Possession and Utility), CIA remains by far the most widely used (Maple, 2017).

The constraints on power impact, most significantly on efforts to maintain confidentiality and integrity in terms of IoT systems (Maple, 2017), was one challenge we had to battle with in our architecture. A way to handle this was to ensure that every computational or processing demand be moved away from the device as displayed in Table 5.1.

Authentication within IoT is critical, since an adversary can authenticate as a legal device and gain access to any data (compromising confidentiality), modify (compromising Integrity) and delete or restrict access (compromising availability) (Maple, 2017). As such, **AA** had to ensure that these three aspects were addressed by selecting parameters that could handle the CIA components partly or in full, as long as overall, all aspects were covered for a complete security package.

Table 5.3 gives a summary of how the proposed authentication scheme was able to meet the CIA requirements.

Table 5.3: CIA Review of ***AA***

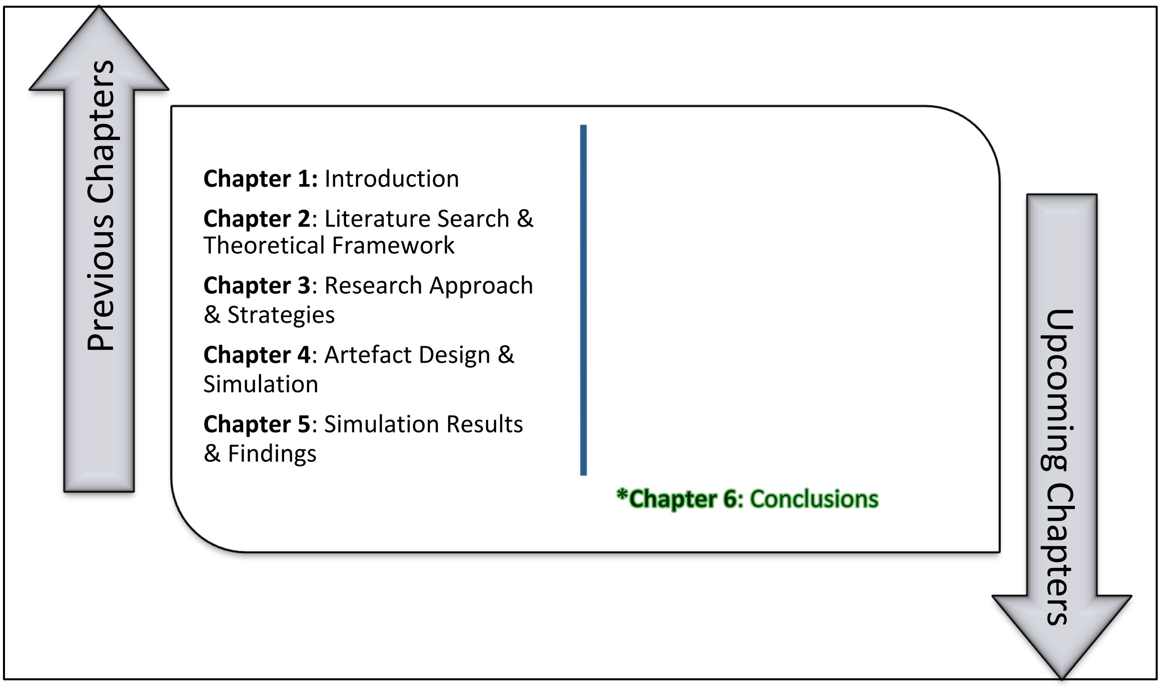
Parameter on AA	Confidentiality	Integrity	Availability
Random numbers	Addressed	Addressed	
Hash function	Addressed	Addressed	Addressed
Unique ID	Addressed	Addressed	
Timestamps		Addressed	Addressed
Mutual authentication		Addressed	Addressed

We could remark at this point that most of the parameters selected for **AA** were strong in addressing the integrity arm of the CIA triad.

5.8 Chapter Summary

This chapter gave the simulation scenarios by highlighting the set of parameters that were used to test security features of the authentication architecture proposed in this work. Guided by the Dolev Yao security threat model, the chapter details the key security features that the architecture was constructed around. Some of the key security threats against which the architecture was tested against are outsider attacks, replay attacks, man-in-middle attacks, impersonation attacks and forward security. Testing results for the architecture's lightweight-ness were presented in this chapter. Also a measure of the computational efficiency and probable scalability of the architecture were covered too. Finally, the architecture's security components were reviewed in terms of the CIA triad.

CHAPTER 6: CONCLUSIONS



Previous Chapters

Chapter 1: Introduction

Chapter 2: Literature Search & Theoretical Framework

Chapter 3: Research Approach & Strategies

Chapter 4: Artefact Design & Simulation

Chapter 5: Simulation Results & Findings

***Chapter 6:** Conclusions

Upcoming Chapters

Like any story that has a beginning, this research also has an end. This chapter serves as a summary of the findings from the research by giving some key conclusions and recommendations for further studies and improvements in the same domain. The chapter revisits the research objectives and highlights the envisaged findings and contributions as informed by the results obtained.

6.1 Chapter Overview

This chapter gives an outline of the overall research journey by mainly focusing on the presented results in Chapter 5. These results are a reflection of the focus of this work and the envisaged contributions drawn from them. As a highlight on the relevance of the work presented here, there is a revisit on the link to the domain of Smart Home applications. A summary of the entire research in light of the contributions to the main body of information security is given.

In this chapter, a detailed summary of the key contributions and findings from Chapter 1 to Chapter 5 is presented. This serves as a quick reference point for the reader to gain a grasp of what each chapter was focusing on and what to eventually expect from the chapter. A revisit of the overall research objectives is done with the intention of showing the extent to which the very objectives contributed to the overall research deliverables.

Designed around the notion of sharing the author's personal experience of the research journey, this chapter contains a reflection basis on the broader contribution of the work in an in-disciplinary arena. Lastly, the chapter provides some recommendations for future studies in the same domain.

Chapter Organisation: To give a context of the entire research journey, each Chapter is revisited in section 6.2 by giving a summary and key findings presented in the specific chapter, which pointed to some key contributions from the review of either scientific publications or from simulations done. In a more focused analysis, section 6.3 gives a summary of the overall research objectives and highlights how each objective contributed to the research's deliverables. Section 6.4 is a key summary towars the contribution of this research to the greater body of knowledge.

Section 6.5 highlights the research contributions in light of other disciplines besides Computer Science, hence displaying the bigger picture of this research. Section 6.6 gives an overall evaluation of the research, giving an indication of the position this research ought to be viewed upon in context and out of context. Section 6.7 acknowledges that there are some limitations to our research and how they can be addressed going forward as explained in Section 6.8. Section 6.9 underscores some recommendations as informed by the direction of this research for IoT security solutions in smart application security design. Overall, the chapter is then summarised in Section 6.10.

6.2 Findings Presented in Chapters

We now revisit each chapter and summarise the key findings towards addressing the research problem and set research questions and the link between each chapter and the results presented in this thesis.

6.2.1 Chapter 1 - Introduction: Summary of findings

The following key aspects have been discussed in Chapter 1: - an overview of the phenomenon of IoT as the main pillar and broad research area for this work. Potential research gaps where the focus of this research emanated from, an outline of the research problem formulated for this research work as well as research questions and objectives. The conceptual framework of the research, defining the rationale of the research, and marking the delimitation of the research as well as the scope were key highlights in Chapter 1.

Based on what was presented in Chapter 1, the main findings to highlight from the completed activities towards the overall research focus can be summarised as follows:-

- **Contextual problem identification on challenges in IoT design and deployment** - Authentication identified as the main focal point to enable addressing the security challenges. We strongly support the claim that our focus will be instrumental in addressing many security loopholes in IoT applications, if resources channelled towards addressing authentication as a precursor to all other security challenges are properly utilised.

- **Research gap identification and focused solution design approach** – Guided by the process of identifying existing and topical research gaps in IoT domain, this research managed to present procedural approaches to tackle some of the challenges through application of Design Science Research and Formal Methods.

6.2.2 Chapter 2 – Theoretical Framework: Summary of findings

Chapter 2 gave a rounded walk-through of Smart Home environments literature by first laying the background through digging into the history of Smart Homes, and built on top of that history by providing working definitions under varying contexts. To highlight the essential features of Smart

Homes, the chapter looked at the requirements, applications, models, challenges and future projections for Smart Homes. As such, the following are main findings from Chapter 2: -

- **Detailed modelling and understanding of Smart Homes** - From Chapter 2’s content, we can safely conclude that this research contributed towards the detailed modelling and understanding of what it entails to have a Smart Home and how such a convenient space can fall victim to the very components that makes it what it is.
- **Specifications comprised of security awareness package** - We also deemed, based on the descriptions and outlines presented in Chapter 2, which architectures can have a requirements specification of what physical structure can expect to design for practical implementation towards robust security designs for Smart Home applications. Also guided by the different models and future projections highlighted, Smart Home setups are easier to visualise. We also emphasise the security awareness created to the different stakeholders of Smart Homes.

In Chapter 2, a presentation of the detailed summary of the various threats and attacks that can be attributable to Smart Home IoT applications was presented. Identifying such threats and eventually categorising them helped in designing solutions implementable to practically address some of the threats.

- **Security awareness** - Given the thrust of Chapter 2, we can highlight security awareness as a key contribution from this Chapter. Not only is a Smart Homeowner or potential owner sensitised on what to watch out for, but he/she is also given a hint on what to pay attention to when looking at solutions for their Smart Homes.

- **Security threats and attack taxonomy** - In a technical context, Chapter 2 helped in creating security threats and attack taxonomy for Smart Home IoT applications which can be used for further solutions design.

Outlined in Chapter 2 are some of the different authentication architectures in the IoT domain. As the focus of the Chapter was to identify the best lightweight authentication approaches for Smart Homes, we considered a number of key aspects when selecting a solution to advance towards the design of authentication techniques for Smart Homes. There are crosscutting dynamics in the various authentication approaches already in use and borrowing the best features from one solution and combining with the other gave a recipe for a secure solution presented in this work.

The costing of probable authentication architectures for consideration helped in the decision of selecting a cost effective solution to propose for lightweight applications.

- **Reinforcing of the reuse concept** – The process of deciding on the best features to include in the authentication architecture presented in this work reinforced the concept of reuse which is one of the most effective approaches in computing that enable reducing development time and immediate application of solutions for results.

- **Creating of a process model** – As a key contribution from Chapter 2, a process model has been created, which is the costing approach for possible authentication architecture across different IoT domains where lightweight features could be tested in an effective and level basis.

Chapter 2, lastly gave a quick summary of the main research area starting from the main research body of knowledge to the specific domain of application, that is Smart Home; then finally highlighting on specific security components of focus - authentication. An overarching research focus mapping concluded the chapter.

It is in this chapter that a critical analysis of literature was done, and a highlight of the research gap was discussed as informed by literature reviews covered in earlier sections of Chapters 2.

As the main findings, from the synthesis of literature covered in Chapter 2, the following can be highlighted: -

- **A unique approach for refining literature content** - Literature sources were summarised in a focused manner in such a way that a clear outline of the research questions could be shaped.

As a contextual term peculiar to this research, we therefore conclude that Chapter 2 created a funnel for refining the research focus hence it presents best practices in research approach. We may start with a large base of different literature sources but eventually we need to streamline our focus towards the specific research area.

6.2.3 Chapter 3 – Research approach and strategies: Summary of findings

An outline of the high-level research paradigm and the overall research approach was explained in Chapter 3. To detail on how the execution of the research towards realising the stated objectives or set questions, Table 3.1 as presented in Section 3.4 covered that. Table 3.1 gives a highlight of the methods and tools used as well as the expected outcomes for each respective research milestone. The research methods section summarised the sampling methods, data collection methods and how data was analysed to draw conclusions on this research.

- **Pragmatic research approach** - Central to positioning of Chapter 3 in this research is its pragmatic approach to research design. Employing different philosophies and paradigms for research in Computer Science is not common practice. We strongly believe that through Chapter 3 our research was able to introduce a unique approach of conducting research using the constructivist paradigm and Design Science Research as high-level methodological approaches. Employing the Challenge Driven Approach (CDA) made our focus more practical than theoretical.

6.2.4 Chapter 4 – Artefact design and simulation: Summary of findings

An account of the process of coming up with the authentication architecture from the initial unrefined prototype to the proposed authentication architecture. The proposed architecture was presented, preceded by an explanation of the key components that formulate the authentication architecture, which are the bootstrapping phase and the authentication phase. Chapter 4 gives a highlight of the roles played by the various actors in the authentication architecture and the visual display of the architecture. As key contributions, we can mention the following: -

- **A secure Authentication Architecture** – A presentation of the main deliverable of this research, which is lightweight authentication architecture for unsupervised IoT applications in Smart Home applications.
- **A contextual functional representation of AAL and ESS** - the AAL and ESS scenarios setups and possible applications are highlighted.
- **Testing of security features using formal methods** – An articulation of how testing of the security features using the SCYTHER tool for formal verification of the architecture was done. This presented alternatives for future research in the same domain.

6.2.5 Chapter 5 - Simulation results and findings: Summary of findings

Chapter 5 presented simulation scenarios by highlighting the set of parameters that were used to test security features of the authentication architecture proposed in this work. Guided by the Dolev Yao security threat model, the chapter detailed the key security features the architecture was constructed based on. Some of the key security threats against which the architecture was tested against are outsider attacks, replay attacks, man-in-middle attacks, impersonation attacks, and forward security. A presentation of the testing results for the architecture's lightweight-ness was done. In addition, a measure of the computational efficiency and probable scalability of the architecture was covered too. Finally, the review of the architecture's security components in terms of the CIA triad was completed.

As key contributions from the chapter, we can highlight the following:-

- **Quantitative performance evaluation of the architecture** – By comparing the performance metrics of the Authentication Architecture against relatively similar architectures, this helped in optimising the performance index of the presented architecture.
- **Formal verification of the functionality of the architecture** – By analysing the SCYTHER results, an exploration of different attack vectors was completed. This created a template for security protocol verification in an efficient manner. We are confident that given similar protocol descriptions, we could assess their security levels and we were able to pass valuable recommendations.

6.3 Research objectives revisited - Findings and contributions

Among the key findings and contributions of our work is addressing the challenge of identity management as a precursor to authentication of the communicating devices in IoT platforms. The role played by the Smart Home Agent (SHA) as a trusted agent brought about some key solutions to some of the aspects highlighted in the literature regarding IoT security design. We also appreciate the scalability played by Agent Based Modelling in coming up with the architecture. We now revisit the set objectives and highlight how each of them unveiled some key findings and the contributions harvested from the set objectives.

6.3.1 Objective 1: Identify the potential authentication threats

From this objective, a critical review of literature on authentication threats carried out informed us on different approaches employed in an attempt to handle some of the threats. Of note is the varied nature of approaches that various researchers explored. Sometimes a lack of contextualisation of such threats created an open platform, which was marred with many unsolved challenges. In this research we focused more on the threats that are peculiar to IoT applications in the Smart Home domain, which made it easier to understand the extent of the threats and to harness their impacts.

Zooming into authentication threats helped in identifying early stage threats that can hamper the effective implementation of security solutions to overall architecture design. Unlike a setup of focusing merely on IoT threats in general, they are wide and cut across many disciplines. What we discovered from the literature review is that the threats that are prevalent in IoT are not only confined to IoT but also relate to conventional applications. However, solutions applicable to conventional applications cannot directly be applied to IoT applications without some modifications, and in some cases creating completely new solutions altogether.

The main contributions from this objective are shared in the following peer-reviewed conference publications also available in Appendix 2 and 3.

- Gamundani, A. M. (2015). An impact review on Internet of things attacks. In *Proceedings of 2015 International Conference on Emerging Trends in Networks and Computer Communications, ETNCC 2015*, 17-20 May 2015, Windhoek, Namibia. https://doi.org/10.1109/ETNCC.2015.7184819
- Gamundani, A. M., Phillips, A., & Muyingi, H.N., (2018). An overview of potential authentication threats and attacks on Internet of Things (IoT): A focus on Smart Home Applications. In *Proceedings of the 11th IEEE International Conference on Internet of Things (iThings- 2018) Halifax, Canada*. http://cse.stfx.ca/~iThings2018/acceptedlist.htm

6.3.2 Objective 2: Analyse current IoT authentication architectures

The detailed review of existing authentication architectures from a broad IoT application space to a more focused setup on Smart Homes revealed the following findings for this research.

There is quite a reasonable number of lightweight solutions advanced under different IoT application domains. However, the parameters for measuring lightweight-ness differ from application to application, and as such, there is no standardised approach for demarcating the various magnitudes of lightweight solutions. What we then had to focus on in this research was the resource-constrained parameters of the devices we envisaged to be operational in a Smart Home space mainly focusing on computational capacity and storage capacity.

We also discovered that of the various lightweight authentication architectures there are no standard protocols being uniformly used. It was difficult to weigh which options scale better than the other when the parameters are unique. As a way of creating a level playfield, after discovering that most very lightweight protocols and architectures employed hash functions as a means of advancing robust security solutions to resource constrained devices, we introduced a comparison on a costing basis.

Costing of various authentication schemes on a comparison basis became one of the major contributions towards fulfilling this objective that our research relates to.

The various authentication architectures assessed provided a rich theoretical foundation for the design of an improved lightweight authentication architecture that borrowed different features from various validated functional similar architectures.

The main contribution from the objective is shared in the following publication, presented in full under Appendix 4.

- Gamundani, A. M., Phillips, A., & Muyingi, H.N., (2018). A review and costing of Lightweight Authentication schemes for Internet of Things (IoT): Towards design of an authentication architecture for Smart Home applications. *In Proceedings of the 6th International Workshop on Applications and Techniques in Cyber Security 2018 (ATCS 2018), in Conjunction with SecureComm 2018, Singapore.*

6.3.3 Objective 3: Design a lightweight IoT secure authentication architecture

The identification of the challenges common to Smart Homes and IoT applications in general both at the perception and transmission layers helped in the informed design and customisation of an authentication solution that could suit the constrained devices in such setups.

The need for secure data collection, transmission and storage around the home environment and the exchange of such data helped in contextualising the operation environment that the architecture was supposed to be deployed under.

A focus on the unsupervised nature of devices, which have capabilities below normal operations in conventional setups, was a challenge this research had to address. Unlike many research focuses, focus on unsupervised devices was rare; henceforth this could mark another key contribution of this research in IoT security design.

Handling the computational power and storage constraints in IoT as a hindrance to robust security advancements to full scale was another key challenge to solve. Conventional solutions generally are not applicable to constrained devices hence this research recommended the focus on a trusted layer that has relatively reasonable computational capacity instead of focusing on devices with limited resources.

A pragmatic approach to security design for constrained things in IoT that can operate with no human intervention had to face privacy issue concerns. We share some of the value propositions and key contributions in this regard in one of the peer-reviewed conference publication, presented in Appendix 5.

- Gamundani, A. M., Phillips, A., & Muyingi, H.N., (2018). Privacy preservation and security dilemma: Relationship proposition for IoT authentication. In *Proceedings of the International Conference on Recent Innovations in Electrical, Electronics & Communication Engineering – (ICRIEECE), India.*

Handling authentication as a key component to other security pillars and embracing it as a buffer layer for advancing robust solutions was motivated on the basis that it has powers to open and close doors to intruders in any given network setup.

Identifying socially relevant applications in the Smart Home applications in the form of Assisted Ambient Living (AAL) space and Energy Saving Solutions (ESS) was key. Being able to combine these in a single critical Smart Home setup drove the need to link such defined needs to the globally agreed United Nations Sustainable Development Goals (UN-SDGs) in the bigger vision of mapping the research towards viable and critical solutions.

Effectively combining the Challenge Driven Approach (CDA) and marrying it with technical approaches towards advancing viable societal needs in the form of AAL and ESS is among the key contributions this research managed to present.

As a key finding, we noted that, Artificial Intelligence (AI) is going to play an important role in the growth of Smart Home applications and related IoT applications in conventional domains directly linked to Smart Homes such as smart cities, smart health and smart grids for example.

6.3.4 Objective 4: Evaluate the proposed secure solution for correctness and Computational efficiency

Embracing the power of the SCYTHER tool for verification, falsification and security testing of various possible attacks that could be attributed to the authentication architecture in this work is among the key milestones this research managed to record, which is helpful to future research in the same direction.

Testing of insider, impersonation, replay, and man-in-the middle attacks of the authentication architecture using formal methods, under the auspices of the Dolev Yao model is one of the methodological contributions of this research worth recording.

A clear vision on the research contribution towards hardening security solutions in personal area networks and gradual implementation into the bigger vision of smart cities could be gained from this work, hence a good basis for advancing security design solutions from the first line of defence, which is authentication in a bottom-up approach.

6.4 Contribution to the greater body of knowledge

This research contributes directly to the greater body of knowledge, which is the information assurance and security in a number of ways as highlighted below: -

- Scoping of the threat and vulnerability landscape of IoT applications in smart home environments giving a solid background to work on solutions towards addressing such threats and vulnerabilities.
- A deep review of authentication aspects in lightweight IoT application domains.
- Costing of authentication protocols in a contextual setup towards advancing security solutions that have lightweight attributes.
- Scalable solution in the form of an authentication architecture that can be customised for various domains of information security.
- An idealistic approach on how to incorporate new trends in technology towards advancing relevant information security and assurance solutions such as AI.

6.5 Wider Research Contributions

This research employed an approach where the main focus was to look at how security can be enhanced by addressing the authentication of devices that will join our Smart Homes. One way of considering this research focus in layman terms is this: If one would have their home, will they allow strangers to access their private information anytime and anyhow? Certainly the answer is No. If that is the case, how then can we protect our personal data from such unwanted access? We would appreciate from these rhetorical questions that a lot of other disciplines are invoked in the process.

In light of that, the wider contributions of this research can be attributed towards the following dimensions, as summarised in Figure 6.1: Social, Economic, Environmental and Technological. Of central focus is how we recommend a pivotal focus in terms of the research direction that our research has to assume if considered in a broader scale, placing emphasis on the different dimensions of focus.

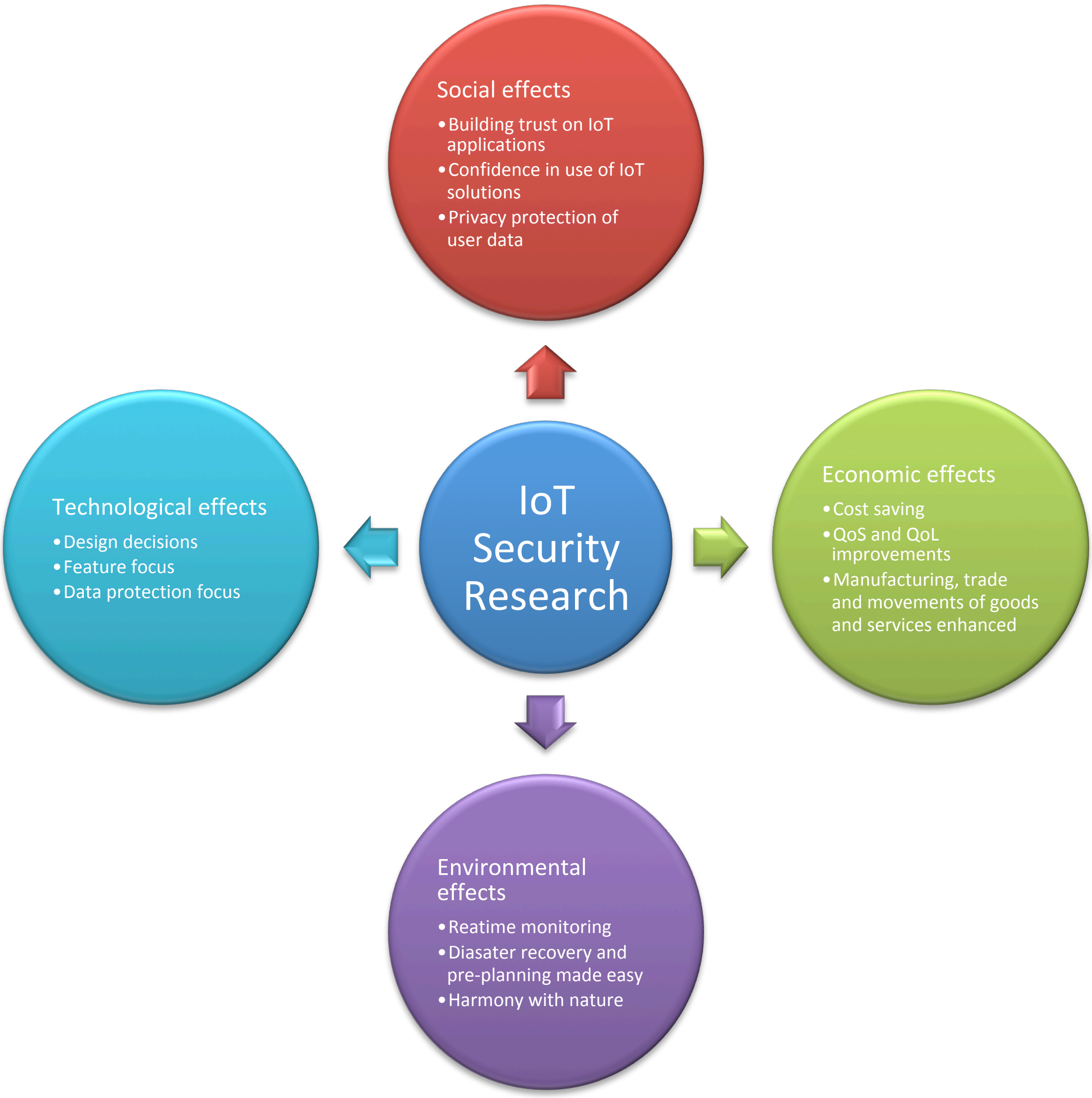

Social effects
•Building trust on IoT applications
•Confidence in use of IoT solutions
•Privacy protection of user data
Technological effects
•Design decisions
•Feature focus
•Data protection focus
IoT Security Research
Economic effects
•Cost saving
•QoS and QoL improvements
•Manufacturing, trade and movements of goods and services enhanced
Environmental effects
•Reatime monitoring
•Diasater recovery and pre-planning made easy
•Harmony with nature

Figure 6.1: The effects of our IoT research in a broader sense

Depending of the focus of attention, the relevance of IoT security research has become one of the crucial aspects to consider in any industry especially if its key benefits are to be reaped without any compromise of data security and privacy.

6.6 Evaluation of the Research Approach

An acknowledgement of the fact that research has so many facets and invokes different schools of thought based on the standpoint of the researcher is made. As such, we remark that approaches that may not have been explored in this work for similar challenges one can pick do not imply that they are irrelevant. In light of that, the philosophy used, the approach used to answer the questions, and their relevance in bringing rigour and thoroughness to the research was mainly motivated by the best available selections at the time when this research was initiated and their scientific contributions. Many more improved approaches could be applied and enhance the output thereof.

With the multidisciplinary nature of our research as outlined in Figure 6.1, we make it clear at this point that no single approach is enough to address challenges that involve human beings. Appreciating the dynamic nature of human spaces and their insatiable needs will help in making relevant research decisions and selecting methods and approaches that speak towards valuable inputs in improving Quality of Life (QoL) and Quality of Service (QoS) overall.

6.7 Limitations of the Research

Focus on the scope of Smart Home applications and the selection of authentication as a security component to measure, could be considered the first limitation as there are many aspects to consider when it comes to Smart Home applications and their security needs. We appreciate the fact that one research journey will not be able to solve the surmountable amount of challenges facing humanity in the ever dynamic technological quagmire.

As highlighted by (Maple, 2017), “If the devices are appropriately authenticated, there is still a requirement to authenticate the service, since certain services will have access to certain data” (p. 168). Our work was mainly focused on device authentication and not service authentication; as such we highly recommend further work in the direction of service authentication and a combination of the two as well.

Beyond authentication, this work assumes that access control is going to be discharged in a well-defined approach that is equally secure. This may not be as perfect a setup as being portrayed by this statement, henceforth the need to dig deeper into all activities beyond authentication is of paramount importance.

6.8 Envisaged Future Direction of the Research

Security has been one of the drawbacks raised by different stakeholders, which can slow IoT's potential adoption as proffered by Jha and Sunil (2014) in their whitepaper for L& T Technology services.

A focus on more proactive instead of reactive approaches as lamented by Jha and Sunil (2014), which is a consequence of an after-thought on security in many discussion and planning platforms for IoT applications and services.

With industry 4.0 expected to be in full swing, where IoT applications are expected to be interwoven into each phase of the manufacturing process (Maple, 2017) entails smarter manufacturing processes delivered through intelligent logistics, adding rapid, flexible , and lean manufacturing.

Privacy is one of the hot topics in IoT and it is our hope that future research will look at how the initiated European General Data Protection (GDPR) can be effectively implemented globally so that privacy concerns can be addressed to a satisfactory level. As pointed by Maple (2017), that IoT has the capacity to revolutionise the way we live in sectors ranging from transport to health, from entertainment to our interactions with the government and various other surroundings; that will make life more comfortable and bearable.

6.9 Recommendations for Future Research

From the experience gained through our research journey, we can propose the following fundamental aspects in light of IoT security research in general. IoT applications are now diverse and cut across many domains, as such having a cross sectional approach when considering any IoT related application would give a rich starting point in terms of understanding the overall operations and the shortfalls that may need to be addressed in the field. Guided by the plethora of different devices that build up the world of IoT applications, solutions that will enhance interoperability are well sort after.

We strongly posit that the need for architectures, protocols, frameworks, and solutions that enhance seamless operations of IoT powered applications in any domain are overdue. This was evident through different literature sources as displayed in Chapter 2, of this thesis.

Balancing the trade-off between security and the need for privacy when it comes to applications that collect, transmit or store personal data is one of the issues due for addressing, if IoT applications are going to retain the trust of end users.

As we are solely closing the gap between application domains specifics and opening a level playfield, the need to address IoT security concerns for example, should not be treated in isolation but rather in a holistic approach. A challenge encountered in a Smart Home setup is not confined to that domain alone, but will have its effects propagating to all other domains like smart cities and smart health for instance. The same applies in any direction too.

6.10 Chapter Summary

A reflection from the authors' perspective of the entire research focus and the lessons learnt are packaged in this chapter, where a broader perspective is taken into consideration. There is an appreciation of the fact that any discipline in today's interdisciplinary nature of research should not be treated in isolation, henceforth an emphasis on the need to embrace all possible avenues when looking at solution design for any identified problem.

As outlined in this chapter, the future focus on security in Smart Home solutions will gain momentum and retain meaning if all other dimensional concerns are addressed equally and at the same time as the technological aspects. This indeed presents a complex problem to address, hence a proposition to have whatever piece of the research component to speak directly to any identified challenge with full awareness of the tangible contribution to the overall big picture.

REFERENCES

Abdallah, A., & Shen, X. (2017). Lightweight Authentication and Privacy-Preserving Scheme for V2G Connections. *IEEE Transactions on Vehicular Technology*, *66*(3), 2615–2629. https://doi.org/10.1109/TVT.2016.2577018

Abdullaziz, O. I., Chen, Y. J., & Wang, L. C. (2016). Lightweight authentication mechanism for software defined network using information hiding. *2016 IEEE Global Communications Conference, GLOBECOM 2016 - Proceedings*, 0–5. https://doi.org/10.1109/GLOCOM.2016.7841954

Ahamed, J., & Rajan, A. V. (2016). Internet of Things (IoT): Application Systems and Security Vulnerabilities.

Ahmed, S. H., & Kim, D. (2016). Named data networking-based smart home. *ICT Express*, *2*(3), 130–134. https://doi.org/10.1016/j.icte.2016.08.007

Al-Ali, A. R., Zualkernan, I. A., Rashid, M., Gupta, R., & Alikarar, M. (2017). A smart home energy management system using IoT and big data analytics approach. *IEEE Transactions on Consumer Electronics*, *63*(4), 426–434. https://doi.org/10.1109/TCE.2017.015014

Alaa, M., Zaidan, A. A., Zaidan, B. B., Talal, M., & Kiah, M. L. M. (2017). A review of smart home applications based on Internet of Things. *Journal of Network and Computer Applications*, *97*(February), 48–65. https://doi.org/10.1016/j.jnca.2017.08.017

Amin, R., Islam, S. H., Biswas, G. P., Khan, M. K., Leng, L., & Kumar, N. (2016). Design of an anonymity-preserving three-factor authenticated key exchange protocol for wireless sensor networks. *Computer Networks*, *101*, 42–62. https://doi.org/10.1016/j.comnet.2016.01.006

Amiribesheli, M., Benmansour, A., & Bouchachia, A. (2015). A review of smart homes in healthcare. *Journal of Ambient Intelligence and Humanized Computing*, *6*(4), 495–517. https://doi.org/10.1007/s12652-015-0270-2

Arafin, M. T., Gao, M., & Qu, G. (2017). VOLtA: Voltage over-scaling based lightweight authentication for IoT applications. *Proceedings of the Asia and South Pacific Design Automation Conference, ASP-DAC*, 336–341. https://doi.org/10.1109/ASPDAC.2017.7858345

Arafin, M. T., & Qu, G. (2016). RRAM based lightweight user authentication. *2015 IEEE/ACM International Conference on Computer-Aided Design, ICCAD 2015*, 139–145. https://doi.org/10.1109/ICCAD.2015.7372561

Arasteh, S., Aghili, S. F., & Mala, H. (2016). A new lightweight authentication and key agreement protocol for Internet of Things. *2016 13th International Iranian Society of Cryptology Conference on Information Security and Cryptology (ISCISC)*, 52–59. https://doi.org/10.1109/ISCISC.2016.7736451

Ashibani, Y., Kauling, D., & Mahmoud, Q. H. (2017). A Context-Aware Authentication Framework for Smart Homes. In *2017 IEEE 30th Canadian Conference on Electrical and Computer Engineering (CCECE)*.

Backes, M., Cervesato, I., Jaggard, A. D., Scedrov, A., & Tsay, J. K. (2011). Cryptographically sound security proofs for basic and public-key Kerberos. *International Journal of Information Security*. https://doi.org/10.1007/s10207-011-0125-6

Baek, J., & Youm, H. Y. (2015). Secure and lightweight authentication protocol for NFC tag based services. *Proceedings - 2015 10th Asia Joint Conference on Information Security, AsiaJCIS 2015*, 63–68. https://doi.org/10.1109/AsiaJCIS.2015.35

Baker, A. (Wind R. (n.d.). Maintaining Data Integrity in Database Applications. Retrieved from http://docs.oracle.com/cd/B28359_01/appdev.111/b28424/adfns_constraints.htm#i1006359

Batool, S., Saqib, N. A., & Khan, M. A. (2017). Internet of Things Data Analytics for User Authentication and Activity Recognition. In *2017 Second International Conference on Fog and Mobile Edge Computing (FMEC)* (pp. 183–187).

Bhati, A., Hansen, M., & Chan, C. M. (2017). Energy conservation through smart homes in a smart city: A lesson for Singapore households. *Energy Policy*, *104*(February), 230–239. https://doi.org/10.1016/j.enpol.2017.01.032

Brandt, J. (2015). 50 billion connected IoT devices by 2020. Retrieved from https://www.privacyrisksadvisors.com/news/a50-billion-connected-iot-devices-by-2020-by-jaclyn-brandt/

Brenkus, J., Stopjakova, V., Zalusky, R., Mihalov, J., & Majer, L. (2015). Power-efficient smart metering plug for intelligent households. *Proceedings of 25th International Conference Radioelektronika, RADIOELEKTRONIKA 2015*, (296131), 110–113. https://doi.org/10.1109/RADIOELEK.2015.7129031

Challa, S., Wazid, M., Das, A. K., Kumar, N., Goutham Reddy, A., Yoon, E. J., & Yoo, K. Y. (2017). Secure Signature-Based Authenticated Key Establishment Scheme for Future IoT Applications. *IEEE Access*, *5*, 3028–3043. https://doi.org/10.1109/ACCESS.2017.2676119

Chen, D., Zhang, N., Qin, Z., Mao, X., Qin, Z., Shen, X., & Li, X. Y. (2017). S2M: A Lightweight Acoustic Fingerprints-Based Wireless Device Authentication Protocol. *IEEE Internet of Things Journal*, *4*(1), 88–100. https://doi.org/10.1109/JIOT.2016.2619679

Chen, J., Ma, J., Zhong, N., Yao, Y., Liu, J., Huang, R., … Cao, J. (2014). WaaS: Wisdom as a service. *IEEE Intelligent Systems*, *29*(6), 40–47. https://doi.org/10.1109/MIS.2014.19

Chen, J., & Zhu, Q. (2017). Security as a Service for Cloud-Enabled Internet of Controlled Things under Advanced Persistent Threats: A Contract Design Approach. *IEEE Transactions on Information Forensics and Security*, *6013*(c). https://doi.org/10.1109/TIFS.2017.2718489

Chen, S., Liu, T., Gao, F., Ji, J., Xu, Z., Qian, B., … Guan, X. (2017). Butler, Not Servant: A Human-Centric Smart Home Energy Management System. *IEEE Communications Magazine*, *55*(2), 27–33. https://doi.org/10.1109/MCOM.2017.1600699CM

Cheng, L., Shenwen, L., Yingbo, L., Na, L., & Xuren, W. (2015). A secure and lightweight authentication protocol for RFID. *ICEIEC 2015 - Proceedings of 2015 IEEE 5th International Conference on Electronics Information and Emergency Communication*, (2012), 317–320. https://doi.org/10.1109/ICEIEC.2015.7284548

Cherry, C., Hopfe, C., MacGillivray, B., & Pidgeon, N. (2017). Homes as machines: Exploring expert and public imaginaries of low carbon housing futures in the United Kingdom. *Energy Research and Social Science*, *23*, 36–45. https://doi.org/10.1016/j.erss.2016.10.011

Chiang, Y. T., Lu, C. H., & Hsu, J. Y. J. (2017). A Feature-Based Knowledge Transfer Framework for Cross-Environment Activity Recognition Toward Smart Home Applications. *IEEE Transactions on Human-Machine Systems*, *47*(3), 310–322. https://doi.org/10.1109/THMS.2016.2641679

Coetzee, L., Oosthuizen, D., & Mkhize, B. (2018). An Analysis of CoAP as Transport in an Internet of Things Environment. In *www.IST-Africa.org/Conference2018* (pp. 1–7).

Cremers, C. (2014). *Scyther User Manual*. Retrieved from http://users.ox.ac.uk/~coml0529/scyther/index.html%0AUsers

Cremers, C. J. F. (2008). Unbounded verification, falsification, and characterization of security protocols by pattern refinement. *Proceedings of the 15th ACM Conference on Computer and Communications Security - CCS '08*, 119. https://doi.org/10.1145/1455770.1455787

Cremers, C. J. F., Lafourcade, P., & Nadeau, P. (2009). Comparing state spaces in automatic security protocol analysis. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *5458 LNCS*, 74–94. https://doi.org/10.1007/978-3-642-02002-5-5

Cross, N. (2007). From a Design Science to a Design Discipline: Understanding Designerly Ways of Knowing and Thinking. *Design Research Now*, (1923), 41–54. https://doi.org/10.1007/978-3-7643-8472-2_3

Crossman, M. A., & Liu, H. (2016). Two-factor authentication through near field communication. In *2016 IEEE Symposium on Technologies for Homeland Security, HST 2016*. https://doi.org/10.1109/THS.2016.7568941

Daramas, A., Pattarakitsophon, S., Eiumtrakul, K., Tantidham, T., & Tamkittikhun, N. (2016). HIVE: Home Automation System for Intrusion Detection. *Proceedings of the 2016 5th ICT International Student Project Conference, ICT-ISPC 2016*, 101–104. https://doi.org/10.1109/ICT-ISPC.2016.7519246

Denning, T., Kohno, T., & Levy, H. M. (2013). Computer security and the modern home. *Communications of the ACM*, *56*(1), 94. https://doi.org/10.1145/2398356.2398377

Dolev, D., & Yao, a. (1983). On the security of public key protocols. *IEEE Transactions on Information Theory*, *29*(2), 198–208. https://doi.org/10.1109/TIT.1983.1056650

Fabi, V., Spigliantini, G., & Corgnati, S. P. (2017). Insights on Smart Home Concept and Occupants' Interaction with Building Controls. *Energy Procedia*, *111*(September 2016), 759–769. https://doi.org/10.1016/j.egypro.2017.03.238

Fan, X., Qiu, B., Liu, Y., Zhu, H., & Han, B. (2017). Energy Visualization for Smart Home. *Energy Procedia*, *105*, 2545–2548. https://doi.org/10.1016/j.egypro.2017.03.732

Fanti, M. P., Faraut, G., Lesage, J.-J., & Roccotelli, M. (2016). An Integrated Framework for Binary Sensor Placement and Inhabitants Location Tracking. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, *PP*(99), 154–160. https://doi.org/10.1109/TSMC.2016.2597699

Ford, R., Pritoni, M., Sanguinetti, A., & Karlin, B. (2017). Categories and functionality of smart home technology for energy management. *Building and Environment*, *123*, 543–554. https://doi.org/10.1016/j.buildenv.2017.07.020

Gamundani, A. M. (2015). An impact review on internet of things attacks. In *2015 International Conference on Emerging Trends in Networks and Computer Communications (ETNCC)* (pp. 114–118). IEEE. https://doi.org/10.1109/ETNCC.2015.7184819

Gao, Y., Ma, H., Abbott, D., & Al-Sarawi, S. F. (2017). PUF Sensor: Exploiting PUF Unreliability for Secure Wireless Sensing. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 1–12. https://doi.org/10.1109/TCSI.2017.2695228

Ge, M., Hong, J. B., Yusuf, S. E., & Kim, D. S. (2018). Proactive defense mechanisms for the software-defined Internet of Things with non-patchable vulnerabilities. *Future Generation Computer Systems*, *78*, 568–582. https://doi.org/10.1016/j.future.2017.07.008

Gehrmann, C., Tiloca, M., & Hoglund, R. (2015). SMACK: Short message authentication check against battery exhaustion in the Internet of Things. *2015 12th Annual IEEE International Conference on Sensing, Communication, and Networking, SECON 2015*, 274–282. https://doi.org/10.1109/SAHCN.2015.7338326

Ghosh, P., & Mahesh, T. R. (2016). A Privacy Preserving Mutual Authentication Protocol for RFID based

Automated Toll Collection System. In *Proceedings of 2016 International Conference on ICT in Business, Industry, and Government, ICTBIG 2016*. Published by Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ICTBIG.2016.7892668

Gioia, D. A., Corley, K. G., & Hamilton, A. L. (2013). Seeking Qualitative Rigor in Inductive Research: Notes on the Gioia Methodology. *Organizational Research Methods*, *16*(1), 15–31. https://doi.org/10.1177/1094428112452151

Gope, P., & Hwang, T. (2016a). Authentication Protocol for Securing Real-Time Application Data Access in Wireless Sensor Networks. *IEEE Transactions on Infdustrial Electronics*, *63*(11), 7124–7132.

Gope, P., & Hwang, T. (2016b). Lightweight and Energy-Efficient Mutual Authentication and Key Agreement Scheme with User Anonymity for Secure Communication in Global Mobility Networks. *IEEE Systems Journal*, *10*(4), 1370–1379. https://doi.org/10.1109/JSYST.2015.2416396

Granjal, J., Monteiro, E., & Sa Silva, J. (2015). Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues. *IEEE Communications Surveys & Tutorials*, *17*(3), 1294–1312. https://doi.org/10.1109/COMST.2015.2388550

Gray, D. E. (2014). *Doing Research in the Real World*.

Griffin, P. H. (2015). Security for ambient assisted living: Multi-factor authentication in the internet of things. *2015 IEEE Globecom Workshops, GC Wkshps 2015 - Proceedings*. https://doi.org/10.1109/GLOCOMW.2015.7413961

Gu, Z. L., & Liu, Y. (2017). Scalable group audio-based authentication scheme for IoT devices. *Proceedings - 12th International Conference on Computational Intelligence and Security, CIS 2016*, 277–281. https://doi.org/10.1109/CIS.2016.69

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, *29*(7), 1645–1660. https://doi.org/10.1016/j.future.2013.01.010

Guesgen, H. W., & Marsland, S. (2016). Using contextual information for recognising human behaviour. *International Journal of Ambient Computing and Intelligence*, *7*(1). https://doi.org/10.4018/IJACI.2016010102

Haller, S. (2013). The Things in the Internet of Things. In *Poster at the (IoT 2010). Tokyo, Japan, November*. https://doi.org/10.1201/b13090

Halpern, J. Y., & Pucella, R. (2012). Modeling adversaries in a logic for security protocol analysis. *Logical Methods in Computer Science*. https://doi.org/10.2168/LMCS-8(1:21)2012

Han, J. (2016). Chaining the secret: Lightweight authentication for security in pervasive computing. *2016 IEEE International Conference on Pervasive Computing and Communication Workshops, PerCom Workshops 2016*, 0–2. https://doi.org/10.1109/PERCOMW.2016.7457084

Henderson, A. (2015). The CIA Triad: Confidentiality, Integrity, Availability. *Panmore Institute*. Retrieved from http://panmore.com/the-cia-triad-confidentiality-integrity-availability

Hevner, A., & Chatterjee, S. (2010). Design Research in Information Systems. *IntegratedSeries in Information Systems*, *22*, 9–23. https://doi.org/10.1007/978-1-4419-5653-8

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design Science in Information Systems Research. *MIS Quarterly*, *28*(1), 75–105. https://doi.org/10.2307/25148625

Hofer, T., Schumacher, M., & Bromuri, S. (2015). COMPASS: an Interoperable Personal Health System to Monitor and Compress Signals in Chronic Obstructive Pulmonary Disease. *Proceedings of the 9th International Conference on Pervasive Computing Technologies for Healthcare*. https://doi.org/10.4108/icst.pervasivehealth.2015.259186

Hossain, M., Noor, S., & Hasan, R. (2017). HSC-IoT: A Hardware and Software Co-Verification Based Authentication Scheme for Internet of Things. *Proceedings - 5th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering, MobileCloud 2017*, 109–116. https://doi.org/10.1109/MobileCloud.2017.35

Howell, S., Rezgui, Y., & Beach, T. (2017). Integrating building and urban semantics to empower smart water solutions. *Automation in Construction*, *81*, 434–448. https://doi.org/10.1016/j.autcon.2017.02.004

Huang, J.-J., Juang, W.-S., Fan, C.-I., Tseng, Y.-F., & Kikuchi, H. (2016). Lightweight Authentication Scheme with Dynamic Group Members in IoT Environments. In *Proceedings of the 13th International Conference on Mobile and Ubiquitous Systems: Computing Networking and Services - MOBIQUITOUS 2016*. https://doi.org/10.1145/3004010.3004020

Hui, T. K. L., Sherratt, R. S., & Sánchez, D. D. (2017). Major requirements for building Smart Homes in Smart Cities based on Internet of Things technologies. *Future Generation Computer Systems*, *76*, 358–369. https://doi.org/10.1016/j.future.2016.10.026

Iinatti, J., Member, S., & Ha, P. H. (2017). Smart Home Environments. *Ieee Transactions on Information Forensics and Security*, *12*(4), 968–979.

Jacobsen, R. H., Mikkelsen, S. A., & Rasmussen, N. H. (2015). Towards the use of pairing-based cryptography for resource-constrained home area networks. *Proceedings - 18th Euromicro Conference on Digital System Design, DSD 2015*, 233–240. https://doi.org/10.1109/DSD.2015.73

Jacobsson, A., Boldt, M., & Carlsson, B. (2016). A risk analysis of a smart home automation system. *Future Generation Computer Systems*, *56*, 719–733. https://doi.org/10.1016/j.future.2015.09.003

Janbabaei, S., Gharaee, H., & Mohammadzadeh, N. (2017). Lightweight, anonymous and mutual authentication in IoT infrastructure. *2016 8th International Symposium on Telecommunications, IST 2016*, 162–166. https://doi.org/10.1109/ISTEL.2016.7881802

Jen-Ho, Y., Ya-Fen, C., & Chih-Cheng, H. (2013). A user authentication scheme on multi-server environments for cloud computing. *ICICS 2013 - Conference Guide of the 9th International Conference on Information, Communications and Signal Processing*, 1–4. https://doi.org/10.1109/ICICS.2013.6782791

Jha, A., & Sunil, M. C. (2014). *Security considerations for Internet of Things*.

Jiang, Q. I., Zeadally, S., & He, D. (2017). Lightweight Three-Factor Authentication and Key Agreement Protocol for Internet-Integrated Wireless Sensor Networks, *5*. https://doi.org/10.1109/ACCESS.2017.2673239

Joo, I., & Choi, D. (2017). Considering Consumer ' s Electricity Bill Target. *IEEE Transactions on Consumer Electronics*, *1*(63), 19–27.

Kang, K., Pang, Z. B., & Wang, C. (2013). Security and privacy mechanism for health internet of things. *Journal of China Universities of Posts and Telecommunications*, *20*(SUPPL-2), 64–68. https://doi.org/10.1016/S1005-8885(13)60219-8

Kanuparthi, A., Karri, R., & Addepalli, S. (2013). Hardware and embedded security in the context of internet of things. *Proceedings of the 2013 ACM Workshop on Security, Privacy & Dependability for Cyber Vehicles - CyCAR '13*, 61–64. https://doi.org/10.1145/2517968.2517976

Kaplan, B., & Duchon, D. (1988). Combining Qualitative and Quantitative Methods in lnformation Systems. *MIS Quarterly*, *12*(4), 571–586. Retrieved from http://www.jstor.org

Kara, M., Lamouchi, O., & Ramdane-Cherif, A. (2017). A Quality Model for the Evaluation AAL Systems. *Procedia Computer Science*, *113*, 392–399. https://doi.org/10.1016/j.procs.2017.08.354

Karthi, M., & Harris, P. (2016). A Realistic Lightweight Authentication Protocol for Securing Cloud based RFID System Surekha, 168–171. https://doi.org/10.1109/CCEM.2016.38

Kaur, K., Kumar, N., Singh, M., & Obaidat, M. S. (2016). Lightweight authentication protocol for RFID-enabled systems based on ECC. *2016 IEEE Global Communications Conference, GLOBECOM 2016 - Proceedings*, (Id). https://doi.org/10.1109/GLOCOM.2016.7841955

Khemissa, H., & Tandjaoui, D. (2016a). A Lightweight Authentication Scheme for E-Health Applications in the Context of Internet of Things. *Proceedings - NGMAST 2015: The 9th International Conference on Next Generation Mobile Applications, Services and Technologies*, 90–95. https://doi.org/10.1109/NGMAST.2015.31

Khemissa, H., & Tandjaoui, D. (2016b). A Novel Lightweight Authentication Scheme for heterogeneous Wireless Sensor Networks in the context of Internet of Things. *2016 Wireless Telecommunications Symposium (WTS)}*, 1–6.

Kim, Y. P., Yoo, S., & Yoo, C. (2015). DAoT: Dynamic and energy-aware authentication for smart home appliances in Internet of Things. In *2015 IEEE International Conference on Consumer Electronics, ICCE 2015*. https://doi.org/10.1109/ICCE.2015.7066378

Kishimoto, H., Yanai, N., & Okamura, S. (2017). An anonymous authentication protocol for smart grid. *Proceedings - 31st IEEE International Conference on Advanced Information Networking and Applications Workshops, WAINA 2017*, 62–67. https://doi.org/10.1109/WAINA.2017.41

Kothmayr, T., Schmitt, C., Hu, W., Brünig, M., & Carle, G. (2013). DTLS based security and two-way authentication for the Internet of Things. *Ad Hoc Networks*, *11*(8), 2710–2723. https://doi.org/10.1016/j.adhoc.2013.05.003

Kruusimagi, M., Sharples, S., & Robinson, D. (2017). Living with an autonomous spatiotemporal home heating system: Exploration of the user experiences (UX) through a longitudinal technology intervention-based mixed-methods approach. *Applied Ergonomics*, *65*, 286–308. https://doi.org/10.1016/j.apergo.2017.06.017

Lee, B., Kwon, O., Lee, I., & Kim, J. (2017). Companionship with smart home devices: The impact of social connectedness and interaction types on perceived social support and companionship in smart homes. *Computers in Human Behavior*, *75*, 922–934. https://doi.org/10.1016/j.chb.2017.06.031

Lee, J. S., Choi, S., & Kwon, O. (2017). Identifying multiuser activity with overlapping acoustic data for mobile decision making in smart home environments. *Expert Systems With Applications*, *81*, 299–308. https://doi.org/10.1016/j.eswa.2017.03.062

Li, G., Xu, X., & Li, Q. (2015). LADP: A lightweight authentication and delegation protocol for RFID tags. *International Conference on Ubiquitous and Future Networks, ICUFN*, *2015–Augus*, 860–865. https://doi.org/10.1109/ICUFN.2015.7182666

Li, J., Yan, Q., & Chang, V. (2018). Internet of Things: Security and privacy in a connected world. *Future Generation Computer Systems*, *78*, 931–932. https://doi.org/10.1016/j.future.2017.09.017

Li, S., Xu, L. Da, & Zhao, S. (2015a). The internet of things: a survey. *Information Systems Frontiers*, *17*(2), 243–

259. https://doi.org/10.1007/s10796-014-9492-7

Li, S., Xu, L. Da, & Zhao, S. (2015b). The internet of things: a survey. *Information Systems Frontiers*, *17*(2), 243–259. https://doi.org/10.1007/s10796-014-9492-7

Li, X., Liu, H., Wei, F., Ma, J., & Yang, W. (2015). A lightweight anonymous authentication protocol using k-pseudonym set in wireless networks. *2015 IEEE Global Communications Conference, GLOBECOM 2015*. https://doi.org/10.1109/GLOCOM.2014.7417584

Li, Y., Wang, Y., Cheng, Y., Li, X., & Xing, G. (2015). QiLoc: A Qi wireless charging based system for robust user-initiated indoor location services. *2015 12th Annual IEEE International Conference on Sensing, Communication, and Networking, SECON 2015*, 480–488. https://doi.org/10.1109/SAHCN.2015.7338349

Lin, S. C., & Wen, C. Y. (2016). Energy-efficient device-based node authentication protocol for the Internet of Things. *2016 IEEE International Conference on Consumer Electronics-Taiwan, ICCE-TW 2016*, (1), 1–2. https://doi.org/10.1109/ICCE-TW.2016.7520962

Lin, Y. W., Lin, Y. B., Hsiao, C. Y., & Wang, Y. Y. (2017). IoTtalk-RC: Sensors As Universal Remote Control for Aftermarket Home Appliances. *IEEE Internet of Things Journal*, *4*(4), 1104–1112. https://doi.org/10.1109/JIOT.2017.2715859

Ling, Z., Luo, J., Xu, Y., Gao, C., Wu, K., & Fu, X. (2017). Security Vulnerabilities of Internet of Things: A Case Study of the Smart Plug System. *IEEE Internet of Things Journal*, *4662*(c), 1–1. https://doi.org/10.1109/JIOT.2017.2707465

Liu, Y., Hu, S., Member, S., Huang, H., Member, S., Ranjan, R., … Member, S. (2017). Game -Theoretic Market-Driven Smart Home Sceduling Considering Energy Balancing. *IEEE Systems Journal*, *11*(2), 910–921.

Liu, Y., Liu, L., Zhou, Y., & Hu, S. (2016). Leveraging carbon nanotube technologies in developing Physically Unclonable Function for cyber-physical system authentication. *Proceedings - IEEE INFOCOM*, *2016–Septe*, 176–180. https://doi.org/10.1109/INFCOMW.2016.7562067

Macal, C. M., & North, M. J. (2008). Agent-based modeling and simulation: ABMS examples. *Proceedings - Winter Simulation Conference*, 101–112. https://doi.org/10.1109/WSC.2008.4736060

Mahalle, P. (2013). Identity Authentication and Capability Based Access Control (IACAC) for the Internet of Things. *Journal of Cyber …*, *1*, 309–348. Retrieved from http://forskningsbasen.deff.dk/Share.external?sp=S72df67ac-3ea5-41da-8cf0-523c6f71bbf2&sp=Saau

Majeed, A. (2017). Internet of Things (IoT): A verification framework. *2017 IEEE 7th Annual Computing and Communication Workshop and Conference, CCWC 2017*, 2–4. https://doi.org/10.1109/CCWC.2017.7868461

Mandyam, G. D. (2017). Tiered Attestation for Internet-of-Things (IoT) Devices. In *2017 9th International Conference on Communication Systems and Networks (COMSNETS)* (pp. 480–483).

Mannion, P. (2015). Optimal Analysis Algorithms are IoT’s Big Opportunity | Electronics360. *Electronics 360*. Retrieved from http://electronics360.globalspec.com/article/4890/optimal-analysis-algorithms-are-iot-s-big-opportunity

Mano, L. Y., Faiçal, B. S., Nakamura, L. H. V., Gomes, P. H., Libralon, G. L., Meneguete, R. I., … Ueyama, J. (2016). Exploiting IoT technologies for enhancing Health Smart Homes through patient identification and emotion recognition. *Computer Communications*, *89–90*, 178–190. https://doi.org/10.1016/j.comcom.2016.03.010

Maple, C. (2017). Security and privacy in the internet of things. *Journal of Cyber Policy*, *2*(2), 155–184. https://doi.org/10.1080/23738871.2017.1366536

March, S. T., & Storey, V. C. (2016). Design Science in the Information Systems Discipline: An Introduction to the

Special Issue on Design Science Research. *MIS Quarterly*, *32*(4), 725–730. Retrieved from url: http://www.jstor.org/stable/25148869

Margulies, J. (2015). Garage Door Openers: An Internet of Things Case Study. *IEEE Security & Privacy*, *13*(4), 80–83. https://doi.org/10.1109/MSP.2015.80

Martina, J. E., dos Santos, E., Carlos, M. C., Price, G., & Custódio, R. F. (2015). An adaptive threat model for security ceremonies. *International Journal of Information Security*. https://doi.org/10.1007/s10207-014-0253-x

Mbarek, B., Meddeb, A., Ben Jaballah, W., & Mosbah, M. (2017). A broadcast authentication scheme in IoT environments. *Proceedings of IEEE/ACS International Conference on Computer Systems and Applications, AICCSA*. https://doi.org/10.1109/AICCSA.2016.7945807

Meana-Llorián, D., González García, C., Pelayo G-Bustelo, B. C., Cueva Lovelle, J. M., & Garcia-Fernandez, N. (2017). IoFClime: The fuzzy logic and the Internet of Things to control indoor temperature regarding the outdoor ambient conditions. *Future Generation Computer Systems*, *76*, 275–284. https://doi.org/10.1016/j.future.2016.11.020

Mohsin, M., Sardar, M. U., Hasan, O., & Anwar, Z. (2017). IoTRiskAnalyzer: A Probabilistic Model Checking Based Framework for Formal Risk Analytics of the Internet of Things. *IEEE Access*, *5*, 5494–5505. https://doi.org/10.1109/ACCESS.2017.2696031

Mokhtari, G., Zhang, Q., Hargrave, C., & Ralston, J. C. (2017). Non-Wearable UWB Sensor for Human Identification in Smart Home. *IEEE Sensors Journal*, *17*(11), 3332–3340. https://doi.org/10.1109/JSEN.2017.2694555

Mokhtari, G., Zhang, Q., Nourbakhsh, G., Ball, S., & Karunanithi, M. (2017). BLUESOUND: A New Resident Identification Sensor - Using Ultrasound Array and BLE Technology for Smart Home Platform. *IEEE Sensors Journal*, *17*(5), 1503–1512. https://doi.org/10.1109/JSEN.2017.2647960

Morsalin, S., Islam, A. M. J., Rahat, G. R., Pidim, S. R. H., Rahman, A., & Siddiqe, M. A. B. (2017). Machine-to-machine communication based smart home security system by NFC, fingerprint, and PIR sensor with mobile android application. *2016 3rd International Conference on Electrical Engineering and Information and Communication Technology, ICEEiCT 2016*. https://doi.org/10.1109/CEEICT.2016.7873048

Moskvitch, K. (2017). Securing IOT: In your smart home and your connected enterprise. *Engineering and Technology*, *12*(3), 40–42. https://doi.org/10.1159/000113927

Nguyen, H. V., & Iacono, L. Lo. (2016). REST-ful CoAP Message Authentication. *Proceedings - 2015 International Workshop on Secure Internet of Things, SIoT 2015*, 35–43. https://doi.org/10.1109/SIOT.2015.8

Nissar, N., Naja, N., & Jamali, A. (2017). Lightweight authentication-based scheme for AODV in ad-hoc networks. In *2017 International Conference on Wireless Technologies, Embedded and Intelligent Systems, WITS 2017*. https://doi.org/10.1109/WITS.2017.7934616

Offermann, P., Levina, O., Schonherr, M., & Bub, U. (2009). Outline of a Design Science Research Process. *Proceedings of the 4th International Conference on Design Science Research in Information Systems and Technology*, *May*, 1–11. https://doi.org/10.1145/1555619.1555629

Orpwood, R. (2012). Smart Homes. *Pathy's Principles and Practice of Geriatric Medicine: Fifth Edition*. John Wiley & Sons, Ltd. https://doi.org/10.1002/9781119952930.ch124

Oyegoke, A. (2011). The constructive research approach in project management research. *International Journal of Managing Projects in Business*, *4*(4), 573–595. https://doi.org/10.1108/17538371111164029

Paek, J. (2015). Fast and Adaptive Mesh Access Control in Low-Power and Lossy Networks. *IEEE Internet of Things Journal*, *2*(5), 435–444. https://doi.org/10.1109/JIOT.2015.2457940

Parikshit N.Mahalle, Bayu Anggorojati, N. R. P. and R. P. (2013). Identity Authentication and Capability Based Access Control (IACAC) for the Internet of Things. *Journal of Cyber …*, *1*, 309–348. Retrieved from http://forskningsbasen.deff.dk/Share.external?sp=S72df67ac-3ea5-41da-8cf0-523c6f71bbf2&sp=Saau

Park, H., Hwang, S., Won, M., & Park, T. (2016). Activity-aware Sensor Cycling for Human Activity Monitoring in Smart Homes. *IEEE Communications Letters*, *7798*(c), 1–1. https://doi.org/10.1109/LCOMM.2016.2619700

Patel, S., Patel, D. R., & Navik, A. P. (2016). Energy efficient integrated authentication and access control mechanisms for Internet of Things. *2016 International Conference on Internet of Things and Applications, IOTA 2016*, 304–309. https://doi.org/10.1109/IOTA.2016.7562742

Pienaar, J. P., Fisher, R. M., & Hancke, G. P. (2015). Smartphone: The key to your connected smart home. *Proceeding - 2015 IEEE International Conference on Industrial Informatics, INDIN 2015*, 999–1004. https://doi.org/10.1109/INDIN.2015.7281871

Pöpper, C., Tippenhauer, N. O., Danev, B., & Capkun, S. (2011). Investigation of signal and message manipulations on the wireless channel. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. https://doi.org/10.1007/978-3-642-23822-2_3

Premnath, S. N., & Haas, Z. J. (2015). Security and privacy in the internet-of-things under time-and-budget-limited adversary model. *IEEE Wireless Communications Letters*, *4*(3), 277–280. https://doi.org/10.1109/LWC.2015.2408609

Rahman, M., Sampangi, R. V., & Sampalli, S. (2015). Lightweight protocol for anonymity and mutual authentication in RFID systems. *2015 12th Annual IEEE Consumer Communications and Networking Conference, CCNC 2015*, 910–915. https://doi.org/10.1109/CCNC.2015.7158097

Rawashdeh, M., Al Zamil, M. G. H., Samarah, S., Hossain, M. S., & Muhammad, G. (2017). A knowledge-driven approach for activity recognition in smart homes based on activity profiling. *Future Generation Computer Systems*. https://doi.org/10.1016/j.future.2017.10.031

Ray, B., Chowdhury, M. U., & Abawajy, J. (2017). A Multi-Protocol Security Framework to Support Internet of Things, *198*(June). https://doi.org/10.1007/978-3-319-59608-2

Ray, B. R., Chowdhury, M. U., & Abawajy, J. H. (2016). Secure Object Tracking Protocol for the Internet of Things. *IEEE Internet of Things Journal*, *3*(4), 544–553. https://doi.org/10.1109/JIOT.2016.2572729

Ray, B. R. R., Abawajy, J., Chowdhury, M., & Alelaiwi, A. (2018). Universal and secure object ownership transfer protocol for the Internet of Things. *Future Generation Computer Systems*, *78*(February), 838–849. https://doi.org/10.1016/j.future.2017.02.020

Ren, H., Song, Y., Yang, S., & Situ, F. (2016). Secure smart home: A voiceprint and internet based authentication system for remote accessing. *ICCSE 2016 - 11th International Conference on Computer Science and Education*, (Iccse), 247–251. https://doi.org/10.1109/ICCSE.2016.7581588

Rigney, C., Willens, S., Rubens, A., & Simpson, W. (2013). RFC 2687 - Remote Authentication Dial In User Service (RADIUS). *Journal of Chemical Information and Modeling*, *53*(9), 1689–1699. https://doi.org/10.1017/CBO9781107415324.004

Rizzardi, A., Sicari, S., Miorandi, D., & Coen-Porisini, A. (2016). AUPS: An Open Source AUthenticated Publish/Subscribe system for the Internet of Things. *Information Systems*, *62*, 29–41. https://doi.org/10.1016/j.is.2016.05.004

Roy, S., Chatterjee, S., Das, A. K., Chattopadhyay, S., Kumari, S., & Jo, M. (2017). Chaotic Map-based Anonymous User Authentication Scheme with User Biometrics and Fuzzy Extractor for Crowdsourcing Internet of Things. *IEEE Internet of Things Journal*, *4662*(c), 1–1. https://doi.org/10.1109/JIOT.2017.2714179

Rwegasira, D., Kondoro, A., Kelati, A., Dhaou, I. B. E. N., Mvungi, N., & Tenhunen, H. (2018). CDE for ICT Innovation Through the IoT Based iGrid Project in Tanzania. In Paul Cunningham and Miriam Cunningham (Eds) (Ed.), *IST-Africa 2018 Conference Proceedings* (pp. 1–9). IIMC International Information Management Corporation.

Saadeh, M., Sleit, A., Qatawneh, M., & Almobaideen, W. (2016). Authentication techniques for the internet of things: A survey. *Proceedings - 2016 Cybersecurity and Cyberforensics Conference, CCC 2016*, 28–34. https://doi.org/10.1109/CCC.2016.22

Saied, Y. Ben, Olivereau, A., Zeghlache, D., & Laurent, M. (2014). Lightweight collaborative key establishment scheme for the Internet of Things. *Computer Networks*, *64*, 273–295. https://doi.org/10.1016/j.comnet.2014.02.001

Savola, R., Abie, H., & Sihvonen, M. (2012). Towards Metrics-Driven Adaptive Security Management in E-Health IoT Applications. *Proceedings of the 7th International Conference on Body Area Networks*, *250241*(SeTTIT), 276–281. https://doi.org/10.4108/icst.bodynets.2012.250241

Saxena, N., Choi, B. J., & Cho, S. (2015). Lightweight privacy-preserving authentication scheme for V2G networks in the smart grid. *Proceedings - 14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2015*, *1*, 604–611. https://doi.org/10.1109/Trustcom.2015.425

Saxena, N., Choi, B. J., & Lu, R. (2016). Authentication and Authorization Scheme for Various User Roles and Devices in Smart Grid. *IEEE Transactions on Information Forensics and Security*, *11*(5), 907–921. https://doi.org/10.1109/TIFS.2015.2512525

Schaumont, P., Moriyama, D., Gulcan, E., & Aysu, A. (2016). Compact and low-power ASIP design for lightweight PUF-based authentication protocols. *IET Information Security*, *10*(5), 232–241. https://doi.org/10.1049/iet-ifs.2015.0401

SDGs. (2017). The Sustainable Development Goals Report, The Unitd Nations. *United Nations*, 1–56. https://doi.org/10.18356/3405d09f-en

Seo, D. W., Kim, H., Kim, J. S., & Lee, J. Y. (2016). Hybrid reality-based user experience and evaluation of a context-aware smart home. *Computers in Industry*, *76*, 11–23. https://doi.org/10.1016/j.compind.2015.11.003

Shahzad, M., Singh, M. P., & Carolina, N. (2017). Continuos Authentication and Authorization for the Internet of Things. *IEEE Internet Computing*, *21*(2), 86–90. https://doi.org/10.1109/MIC.2017.33

Shaju, S., & Panchami, V. (2016). BISC Authentication Algorithm : An Efficient New Authentication Algorithm Using Three Factor Authentication for Mobile Banking. In *2016 Online International Conference on Green Engineering and Technologies (IC-GET) BISC*.

Sharaf-Dabbagh, Y., & Saad, W. (2016). On the authentication of devices in the Internet of things. *WoWMoM 2016 - 17th International Symposium on a World of Wireless, Mobile and Multimedia Networks*, 1–3. https://doi.org/10.1109/WoWMoM.2016.7523532

Sharma, P., Khanna, R. R., & Bhatnagar, V. (2017). Application of TRIZ framework for resolving security issues in IOT. In *Proceeding - IEEE International Conference on Computing, Communication and Automation, ICCCA 2016*. https://doi.org/10.1109/CCAA.2016.7813921

Shen, C., Li, H., Sahin, G., & Choi, H. A. (2016). Low-complexity Scalable Authentication algorithm with Imperfect Shared Keys for Internet of Things. *2016 IEEE International Conference on Communications Workshops, ICC 2016*, 116–121. https://doi.org/10.1109/ICCW.2016.7503774

Shen, J., Liu, D., Chang, S., Shen, J., & He, D. (2016). A Lightweight Mutual Authentication Scheme for User and Server in Cloud. *Proceedings - 2015 1st International Conference on Computational Intelligence Theory, Systems and Applications, CCITSA 2015*, 183–186. https://doi.org/10.1109/CCITSA.2015.47

Shen, J., Tan, H., Chang, S., Ren, Y., & Liu, Q. (2015). A lightweight and practical RFID grouping authentication protocol in multiple-tag arrangements. *International Conference on Advanced Communication Technology, ICACT*, *2015–Augus*, 681–686. https://doi.org/10.1109/ICACT.2015.7224882

Shen, T., & Maode, M. (2016). Security Enhancements on Home Area Networks in Smart Grids. In *IEEE Region 10 Conference (TENCON)* (pp. 2444–2447).

Shin, D., Sharma, V., Kim, J., Kwon, S., & You, I. (2017). Secure and Efficient Protocol for Route Optimization in PMIPv6-based Smart Home IoT Networks. *IEEE Access*, *3536*(c). https://doi.org/10.1109/ACCESS.2017.2710379

Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks*, *76*, 146–164. https://doi.org/10.1016/j.comnet.2014.11.008

Silverajan, B., Luoma, J. P., Vajaranta, M., & Itapuro, R. (2015). Collaborative cloud-based management of home networks. *Proceedings of the 2015 IFIP/IEEE International Symposium on Integrated Network Management, IM 2015*, 786–789. https://doi.org/10.1109/INM.2015.7140376

Sivanathan, A., Sherratt, D., Gharakheili, H. H., Sivaraman, V., & Vishwanath, A. (2017). Low-cost flow-based security solutions for smart-home IoT devices. *2016 IEEE International Conference on Advanced Networks and Telecommunications Systems, ANTS 2016*. https://doi.org/10.1109/ANTS.2016.7947781

Skocir, P., Krivic, P., Tomeljak, M., Kusek, M., & Jezic, G. (2016). Activity Detection in Smart Home Environment. *Procedia Computer Science*, *96*, 672–681. https://doi.org/10.1016/j.procs.2016.08.249

Smirek, L., Zimmermann, G., & Beigl, M. (2016). Just a Smart Home or Your Smart Home - A Framework for Personalized User Interfaces Based on Eclipse Smart Home and Universal Remote Console. *Procedia Computer Science*, *58*(Euspn), 107–116. https://doi.org/10.1016/j.procs.2016.09.018

Song, T., Li, R., Mei, B., Yu, J., Xing, X., & Cheng, X. (2017). A Privacy Preserving Communication Protocol for IoT Applications in Smart Homes. *IEEE Internet of Things Journal*, *4662*(c), 1–1. https://doi.org/10.1109/JIOT.2017.2707489

Stephanie. (2017). Snowball Sampling: Definition, Advantages and Disadvantages. Retrieved January 15, 2018, from http://www.statisticshowto.com/snowball-sampling/

Tankard, C. (2015). The security issues of the Internet of Things. *Computer Fraud & Security*, *2015*(9), 11–14. https://doi.org/10.1016/S1361-3723(15)30084-1

Tao, M., Zuo, J., Liu, Z., Castiglione, A., & Palmieri, F. (2018). Multi-layer cloud architectural model and ontology-based security service framework for IoT-based smart homes. *Future Generation Computer Systems*, *78*, 1040–1051. https://doi.org/10.1016/j.future.2016.11.011

Tobin, G. A., & Begley, C. M. (2004). Methodological Rigour within a Qualittaive Framework. *Journal of Advanced Nursing*, *48*(4), 388–396. https://doi.org/10.1111/j.1365-2648.2004.03207.x

Tran, A. C., Marsland, S., Dietrich, J., Guesgen, H. W., & Lyons, P. (2010). Use cases for abnormal behaviour detection in smart homes. In *Lecture Notes in Computer Science (including subseries Lecture Notes in*

Artificial Intelligence and Lecture Notes in Bioinformatics) (Vol. 6159 LNCS, pp. 144–151). https://doi.org/10.1007/978-3-642-13778-5_18

Vermesan, O., Friess, P., Guillemin, P., Gusmeroli, S., Sundmaeker, H., Bassi, A., … Doody, P. (2016). Internet of Things Strategic Research Roadmap 2.1 Internet of Things Conceptual Framework 2.2 Internet of Things Vision. In *In Proceedings of 2016 International Conference on ICT in Business, Industry, and Government, ICTBIG 2016* (pp. 1–44). Institute of Electrical and Electronics Engineers Inc. https://doi.org/https://doi.org/10.1109/ICTBIG.2016.7892668

Wang, F., Xu, Y., Zhang, H., Zhang, Y., & Zhu, L. (2016). 2FLIP: A two-factor lightweight privacy-preserving authentication scheme for VANET. *IEEE Transactions on Vehicular Technology*, *65*(2), 896–911. https://doi.org/10.1109/TVT.2015.2402166

Weber, R. (2010). Internet of Things - New security and privacy challenges. *Computer Law & Security Review*. https://doi.org/10.1016/j.clsr.2009.11.008

Winter, R. (2008). Design science research in Europe. *European Journal of Information Systems*, *17*(5), 470–475. https://doi.org/10.1057/ejis.2008.44

Witkovski, A., Santin, A., Abreu, V., & Marynowski, J. (2015). An IdM and key-based authentication method for providing single sign-on in IoT. *2015 IEEE Global Communications Conference, GLOBECOM 2015*, (IdM). https://doi.org/10.1109/GLOCOM.2014.7417597

Wu, Q. X., & Li, H. (2013). Secure solution of trusted Internet of things base on TCM. *Journal of China Universities of Posts and Telecommunications*, *20*(SUPPL-2), 47–53. https://doi.org/10.1016/S1005-8885(13)60222-8

Yang, J. H., & Lin, P. Y. (2014). An ID-Based User Authentication Scheme for Cloud Computing. *2014 Tenth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*. https://doi.org/10.1109/IIH-MSP.2014.31

Yang, M. L., Narayanan, A., Parry, D., & Wang, X. (2016). A lightweight authentication scheme for transport system farecards. *2016 IEEE International Conference on RFID Technology and Applications, RFID-TA 2016*, 150–155. https://doi.org/10.1109/RFID-TA.2016.7750746

Yang, Y., Sun, J., & Guo, L. (2016). PersonalA: A Lightweight Implicit Authentication System based on Customized User Behavior Selection. *IEEE Transactions on Dependable and Secure Computing*, *5971*(c), 1–1. https://doi.org/10.1109/TDSC.2016.2645208

Yao, X., Chen, Z., & Tian, Y. (2014). A lightweight attribute-based encryption scheme for the Internet of Things. *Future Generation Computer Systems*, *49*, 104–112. https://doi.org/10.1016/j.future.2014.10.010

Yaqoob, I., Ahmed, E., Rehman, M. H. ur, Ahmed, A. I. A., Al-garadi, M. A., Imran, M., & Guizani, M. (2017). The rise of ransomware and emerging security challenges in the Internet of Things. *Computer Networks*, *129*, 444–458. https://doi.org/10.1016/j.comnet.2017.09.003

Yoon, E.-J., Das, A. K., Yoo, K.-Y., & Goutham Reddy, A. (2016). Lightweight authentication with key-agreement protocol for mobile network environment using smart cards. *IET Information Security*, *10*(5), 272–282. https://doi.org/10.1049/iet-ifs.2015.0390

Yu, M.-D. M., Hiller, M., Delvaux, J., Sowell, R., Devadas, S., & Verbauwhede, I. (2016). A Lockdown Technique to Prevent Machine.pdf. *IEEE Transactions on Multi-Scale Computing Systems*, *2*(3), 146–159. https://doi.org/10.1109/TMSCS.2016.2553027

Zhang, D., Yang, L. T., Chen, M., Zhao, S., Guo, M., & Zhang, Y. (2014). Real-Time Locating Systems Using Active RFID for Internet of Things. *IEEE Systems Journal*, *10*(3), 1–10. https://doi.org/10.1109/JSYST.2014.2346625

Zhang, N., Wu, X., Yang, C., Shen, Y., & Cheng, Y. (2017). A lightweight authentication and authorization solution based on Kerberos. *Proceedings of 2016 IEEE Advanced Information Management, Communicates, Electronic and Automation Control Conference, IMCEC 2016*, 742–746. https://doi.org/10.1109/IMCEC.2016.7867308

Zhang, R. (2017). An enhanced lightweight authentication protocol for low-cost RFID systems. *Proceedings of 2016 IEEE International Conference on Electronic Information and Communication Technology, ICEICT 2016*, (Iceict), 29–33. https://doi.org/10.1109/ICEICT.2016.7879646

Zhang, Y., Xiang, Y., Huang, X., Chen, X., & Alelaiwi, A. (2018). A matrix-based cross-layer key establishment protocol for smart homes. *Information Sciences*, *429*, 390–405. https://doi.org/10.1016/j.ins.2017.11.039

Zhao, K., & Ge, L. (2013). A survey on the internet of things security. In *Proceedings - 9th International Conference on Computational Intelligence and Security, CIS 2013* (pp. 663–667). https://doi.org/10.1109/CIS.2013.145

Zhong, H., Shao, L., & Cui, J. (2016). A Lightweight and Secure Data Authentication Scheme with Privacy Preservation for Wireless Sensor Networks. *2016 International Conference on Networking and Network Applications (NaNA)*, 210–217. https://doi.org/10.1109/NaNA.2016.85

Zhu, Q., Uddin, M. Y. S., Qin, Z., & Venkatasubramanian, N. (2017). Data collection and upload under dynamicity in smart community Internet-of-Things deployments. *Pervasive and Mobile Computing*, *42*, 166–186. https://doi.org/10.1016/j.pmcj.2017.10.003

APPENDICES

Appendix 1: Publication 1

An Impact Review On Internet of Things Attacks.

Attlee M. Gamundani
Computer Science Department: School of Computing & Informatics
Polytechnic of Namibia
Windhoek, Namibia
E-mail: agamundani@polytechnic.edu.na

Abstract—**The heterogeneity of devices that can seamlessly connect to each other and be attached to human beings has given birth to a new computing epitome referred to as the Internet of Things. The connectivity and scalability of such technological waves could be harnessed to improve service delivery in many application areas as revealed by recent studies on the Internet of Things' interoperability. However, for the envisaged benefits to be yielded from Internet of Things there are many security issues to be addressed, which range from application environments security concerns, connection technology inbuilt security issues, scalability and manageability issues. Given the increasing number of objects or "things" that can connect to each other unsupervised, the complexity of such a network is presenting a great concern both for the future Internet's security and reliable operation. The focus of this paper was to review the impact of some of the attacks attributable to Internet of things. A desktop review of work done under this area, using the qualitative methodology was employed. This research may contribute towards a roadmap for security design and future research on Internet of things scalability. The deployment of future applications around Internet of Things may receive valuable insight as the nature of attacks and their perceived impacts will be unveiled and possible solutions could be developed around them.**

Keywords— Attacks, Denial of Service, Internet of Things, Man in the middle, Replay, Security.

I. Introduction

One of the evolving technologies is the Internet of Things (IoT). Despite the various definitions available, the common understanding on IoT revolves around the interconnection capabilities among things, objects and people. As supported by [1] that we are moving towards Internet of things where there is device-to-device communication. Such a heterogeneous network environment is enabled by various connection technologies and protocols available such as RFID, WIFI and Wireless Sensor Networks [1].

An overview of the field of Internet of Things (IoT) will highlight the potential network capabilities and likely fears of such an elastic technology. The envisaged future capabilities of IoT are feared to be under threat of the emerging security concerns since their deployment. Security concerns include Denial of Service (DoS), Replay, and Man in the middle attacks and many common attacks to networked environments [2]. If such security concerns are not addressed to acceptable levels, an out of hand security grip on the technology is feared.

The potential market for the IoT applications will suffer grossly if the security concerns are not solved [6]. As espoused by [6], security is one of the major issues, which reduce the growth of applications such as IoT, and complications with data privacy and data protection continue to plague the market. This affirms the fear of the magnitude; the security threats are likely to be extending to IoT as they propagate to enormous levels across application environments. The need to affirm that solutions are being worked on and will address the perceived threats and attacks is critically important, as service delivery may be halted, yet certain application environments cannot compromise (even to a lesser extent) on safety, like life saver machines in the health sector, such real-time systems have strict compliance requirements, hence their security is of paramount importance.

The projections to 2024 on the number of gadgets per user averaging six (6) or more are quite alarming [1]. This raises great security concerns on privacy and accountability, leaving unanswered questions on whether it will be possible to specifically attribute a particular gadget to a particular individual. This points to yet another critical issue of identity management, which can help localise the threats instead of a plane approach to try and combat any identifiable threat.

The anticipated results from this research points to further research on possible solutions that could be proposed towards alleviating the security challenges, discussed herein.

This paper in organised as follows: Section II outlines the research methodology employed. Section III gives an overview of Internet of things, with a brief explanation on the possible application areas. Building on the application areas, highlighted in section III, section IV, will dwell on the types of attacks that are attributable to Internet of Things. This section discusses the core of this paper, as it hints on the security point of view of different attacks. Section V will summarize the security point of view with a focus on clearly highlighting areas of serious concern for security developers. Section VI will attempt to detail the performance analysis of the identified attacks in section IV. Section VII will pave a road map for future work as it summarizes the key security areas of attention, via a discussion. Section VIII will conclude this paper emphasizing the need to solicit solutions that could be implemented to secure Internet of things applications.

II. Desktop Review and Qualitative Analysis

The methodology employed for this research is justified by the need to gain the preliminary understanding of the work being done in light of the research focus on attacks that are inherent to IoT. The limited existence of practical resources to fully test some of the challenges motivated the need to have a desktop review of the issue in question. A desktop review gives an entry point understanding of a concept to be fully developed into a full-fleshed research with limited resources. A qualitative analysis comes in handy in this context as the information to be analysed is from other sources that have also not had fully published results, hence the need to establish a basic conclusion from such sources.

III. IoT APPLICATIONS OVERVIEW

The horizon of application environments for IoT is growing at an alarming rate. The application areas are no longer confined to communication platforms alone as the applications are stretching even to public safety [2], which among other application domains encompasses fire fighting [3]. Despite the ability to improve and respond to public emergencies in cities [2], IoT applications should be secure and dependable. The application domains are not isolated from some privacy issues which may compromise citizens' safety and the right to confidentiality, as [3] clearly outlines in the context of fire fighting, as an example, the home fire fighting will entail supervision of the protected facilities; this is increasingly weakening the security points to any targeted object, despite the initial plan to ensure safety.

Cloud computing platforms have facilitated the growth of IoT application domains, because of the storage and communication platforms they avail. However the hesitancy around users to participate in active usage of such platforms and such technologies is attributable to the security fears. The need for assurance of whether the user on the other receiving end is exactly the person they are communicating to, and can be identified as such is vital for IoT's survival and thriving. Hence it is important to consider non-repudiation/verification methods.

We now have smart cities; the agricultural sector is also not spared with farmers being able to track their animals, the education and health sectors almost receiving greater impacts in many application environments, as technology pockets continue to open and improve in such areas. There is a diverse hybrid of application capabilities in most of the technology capable environments, such as museums, where the tourism sector has evolved to be more interactive. The import and export industry is also witnessing the impact of improved service delivery as the processing of goods and services at border posts is gradually being automated especially in developing countries, where technology inception could be hampered by the pool of resources such as bandwidth and many indirect resources, that should ensure efficient technology consumption. The heterogeneous nature of applications is thus explained by the various platforms IoT are capable of being implemented and promise to impact.

It can safely be concluded that Internet of things are almost everywhere and continue to expand as technological trends continue to unfold new dimensions and possibilities.

IV. TYPES OF ATTACKS ON IoT

The major challenges inherent to IoT design, implementation and survival as summarised by [1], revolve around technological and security challenges. Among the key security challenges attributable to IoT applications, authentication could assume the toll, as other security loopholes are likely to sprout if the authentication level is weak; hence by addressing authentication requirements, we are creating a cascading solution to the IoT networks. However, there is need to breakdown the sources of threats into various small areas and tackle the challenges from such manageable horizons as the following sections are going to attempt some classifications.

A. Application based

Application environments for IoT are seemingly complicated as there are huge volumes of data to process from different sensor technologies that are supposed to feed their processing activities to the backend databases in some instances. As espoused by [16], some of the challenges could be internal and some external. Considering the application based threats, the application environment could have its own vulnerabilities that are external to the IoT objects or devices, for example, physical insecurity compromising the efficient operation and results generated thereof. As an example, trying to capture the data pertaining to the local activities around a certain object, if there are interferences from people, data read from such an object is obviously biased and wrong information might be captured and decisions made from such data items, are likely to be compromised.

The constrained application environments for some IoT objects contribute to the security threats being stretched. Considering for instance the storage capacity of the application environment being small and not being able to fully store and process all the required security software, will present a susceptible IoT object to various intrusions and attacks. The need for lightweight security application software for such IoT objects is also met with application limitations. The application environment may not be compatible with the inherent security mechanisms of the IoT gadgets, hence extending the vulnerability of the entire application landscape.

The nakedness of the application environments in terms of security capabilities presents a complex security focus, where both the application environment and the IoT enabler object need serious security considerations for reliable functionality to be yielded.

The need for privacy protection for IoT data processing, data hiding methods for high-source heterogeneous data, is quite mandatory. Consider the CCTV cameras in banks, the positioning of such cameras should be strategic to get the maximum coverage of the surface under surveillance. The data that may be of interest to the bank may have to do with protection against thieves, but there is no way to seclude the other bits and details. There is need for a study on the privacy protection methods in the process of mining in the chain of IoT data repositories. The study by [2] on the data processing mechanisms hints also on privacy protection through collaborative algorithms [2], however these still will remain short circuited for whole security packages towards other types of threats, hence the need to expand on this dimension.

The application environments contribute to huge amounts of metadata files that most importantly leave behind trails for attacks to be extended to application environments. A typical scenario could be a phone being tracked by hackers; they are able to connect various places and that in turn compromise security for all such visited areas by the innocent holder of the mobile phone. The biggest challenge being that, IoT are mostly communicating unsupervised.

B. **Connection based**

The existence of data flow paths to an object or an environment that may indirectly be connected to a particular IoT sensor, compromise the very private nature of that object. In trying to gain the holistic representation of the application domain a lot of other hidden components are exposed. A typical example could be a location aware device, which may pave way to dormant non-suspecting and unsecured devices to be attacked, because they are somehow connected to an IoT device broadcasting information to the outside world.

Resource constrained things are connected to the unreliable and untrusted Internet via IPv6 and 6LoWPAN networks [4], explains how connection platforms contribute to the vulnerability of IoT. Internet by its very nature is not secure, added to the insecurity is now an IoT device that is also not fully secured, the end result is a wave of attacks being extended to a whole web of IoT networks.

Considering the work done by [16] on RFID obstacles, if we consider the internal obstacles of integration with legacy systems, there are two sides to such a setup, the legacy systems may be the ones vulnerable or the RFID connections to the legacy system will weaken the existing setup. Either way the connection links established at any point is an option for a different dimension of an attack.

The invisibility nature of networking [5] which is the most prevalent characteristic feature of IoT makes the analysis of potential network attacks even tougher. [5] highlighted capabilities of heterogeneous hardware among IoT, which renders them a complex networking domain to handle, this is so because of security, privacy and trust issues[5] that differ from one hardware manufacturer to the other. As further pointed by [5], such critical issues need to be resolved to get applications of future Internet feasible and accepted by users.

C. Platform based

Platforms vary and as such present specific challenges. Some platforms by their very nature still have security issues that are unsolved to date. As presented by [6], the growth of cloud computing and communications platforms with data privacy and data protection issues continue to plague the market, hence hampering the growth of such platforms. IoT applications have already capitalised on the cloud computing platforms for extensibility and coverage and many other application based reasons. In such a scenario, there is need to first address the platform security loopholes as the inheritance level by applications that utilise such a platform are high and such inheritance cannot be isolated.

WSN has pending issues to be addressed which comprise of applications like communication platforms, security and management [7]. This again points to a serious concern in as far as the platform for communications being employed is concerned. As the growth of IoT connections increase, it implies that, they continue to proliferate the security concerns to be addressed. There is need to establish a secure communication path and improve the security level of the very interactions among the IoT objects themselves as they pass data items from point A to point B.

D. Other forms of attack

The categories mentioned in A to C above might not be an exhaustive analysis of attacks on IoT, hence not a comprehensive representation of the nature of attacks that are attributable to IoT. We may consider such issues as the absence of particular standards and specific laws that support the application development and deployment of IoT. The absence thereof, causes the sustenance and implementation of strict security measures from manufacturing points. We appreciate work underway to have such standards and laws enacted and in some sections being already in practice, however their grip on ensuring security adherence is still an open issue.

A combination of the highlighted sources of threats also breeds another hybrid source of threats and attacks to IoT. Combining application and platform-based threats, gives an intertwined force of challenges that leave the whole security ground weakened, hence proper thriving of IoT applications is endangered. In the same vein, connection based threats combined with application based threats makes the whole application zone susceptible to serious threats. Bringing the entire three in one basket and adding the IoT in the same basket, we have a serious weaker product. This leaves a serious challenge in terms of how IoT will thrive in their various deployment domains.

V. SECURITY POINT OF VIEW

Security in IoT design mainly focuses on the end- to end communication links among the participating nodes. However considering the architectural view of IoT as presented by ITU, the security levels for IoT need to be focused on the middleware level, since this is where the interaction amongst various node connections takes place. This is normally following an assumption that for all participating nodes in the Internet of things to function effectively, they pass through some virtualized middleware. Reality will present a different challenge all together, where connection links created among nodes could so happen on an M2M (Machine to Machine) basis, hence little to no human interaction, under such scenarios. The security designs of the Internet of things are better embedded inside the nodes or things themselves. This is met with physical and technological limitations of the nodes or things. The need to balance among size, memory and storage capacity makes the plan to implement robust security algorithms a futile effort.

The implementations of Intrusion Detection Systems (IDS), as there are no current IDSs that meet the requirements of IPv6 connected IoT, makes the security design for IoT complicated [4]. The available approaches are either customized for wireless sensor networks (WSN) or for the conventional Internet; therefore there are no standardised IDS designs for IoT communication platforms [4].

The SVELTE designed by [4], primarily targets routing attacks. The SVELTE security design is however limited to spoofed or altered information, sinkhole, and selective forwarding, these are not the only attacks IoT experience [4]. To precisely have a solution that address all the security concerns in IoT is still a hard problem to solve.

VI. PERFORMANCE ANALYSIS OF ATTACKS

The attacks on IoT continue to increase in complexity as the number of connections and the possibilities of interaction among different heterogonous platforms increases. This is creating a complex security challenge to deal with, both on the virtual level and physical layer of IoT application platforms. As a result we are now faced with a different calibre of threats to deal with in IoT unlike in networked and confined networked environments; this is mainly amplified by the wireless capabilities coupled with the sensor technology inherent to IoT devices. High processing capabilities that could be harvested from such platforms as cloud computing, quantum computing and all possible ensuing computing technologies are also contributing factors in as far as the possible attack challenges increases are concerned.

“Attacks have to be intercepted, data authenticated, access controlled and the privacy of customers (natural and legal persons) guaranteed” [12]. These requirements seem to be at their infancy in terms of their realisation at a large scale, still presenting an apt ground for threats to continue to grow. Addressing one or two will not ensure the threats are contained, yet to have all addressed at once is a mammoth task.

Issues to deal with confidentiality, authenticity and integrity of data in IoT, should receive attention [13]. These three areas form the pillars of a security package. To realise all three all possible sources of IoT attacks should be identified and addressed to the full. Since it is not easy to have a generic solution that can qualify to embrace all the security requirements and ensure realisation of these security goals, this paper suggests adopting application models that interact via a middleware where such security measures could be enforced and monitored.

If security features are not strengthened, attacks and malfunctions in the IoT will outweigh any of their intended benefits. Protection mechanisms such as lightweight cryptography, secure protocols, and privacy assurance are not adequate to provide security to IoT [14]. This evidently supports the magnitude of the challenge at hand in advancing security to IoT applications.

The proposal by [15] to use digital signatures to address the problem of spamming the IoT is only a one stop gap measure and may not practically apply to a diverse nature of IoT platforms. As a result of the different application domains that may not harness the existence of a solution in one area to cover the next area, still signal the need to have a direct focus on a particular breed of IoT applications and address them in isolation not universally.

VII. Discussion

Secure solution of trusted Internet of things based on TCM [8] is based on cryptographic modules, which have limitations for some of the lightweight IoT objects and hosting platforms. This solution is centred on the trustworthy of Internet of things development and applications, which by nature may be limited in scope, considering the heterogeneous applications environments [9]. “The need to validate how existing security protocols can be adapted to meet the challenge of heterogeneous environments of IoT,” as espoused by [9] is still an open issue.

Authentication and access control mechanisms are crucial components to consider when designing secure communication for Internet of things [1], however the biggest challenge as highlighted by these authors, is provision of a distributed, lightweight and attack resistant solution to ensure comprehensive security for Internet of things. The need to improve on the authentication and access control schemes available will remain a critical research call, as there still remain room for further improvements to the existing protocols.

The proposed solution by [1], was evaluated on the basis of DoS, man-in-the-middle and replay attacks. This cannot conclusively be the list of possible attacks that Internet of Things are susceptible to. As the classifications presented in section IV above, these three attacks can be application based, platform based or connection based, however, there is a new breed of attacks under hybrid based. As the journey towards security solutions design is not an event but a process that is marred with evolving threats, the need to refocus attention and considering endless possibilities to attack sources cannot be overemphasised.

The work done by [10] under the identity management handled some security issues to be focused on, but the effectiveness of security protocols was not handled to the latter. Considering the same work done by [10], the capability levels computationally of IoT devices were not assessed thoroughly. The need to understand the computational capabilities is in light of the need to design implementable solutions that suit the technological build and capabilities of IoT.

Strategically, the need to focus on authentication and access control issues in IoT promises to avail a holistic solution to the technological and security challenges identifiable to IoT environments. Access control will avail a solution for the technological challenges and authentication on one hand will present the security solutions needed to avert the key threats attributable to IoT for the various application platforms especially powered by wireless and sensor connectivity.

VIII. Conclusion

The heterogeneous nature of IoT demands a versatile and unique legal framework that can broadly tackle globosity, verticality, ubiquity and ethnicity of the IoT [12]. In considering security of typical IoT enabled devices and objects the interaction of such objects is not limited among the homogenous interactions, which they can create, but the various modalities that can be possible both horizontally and vertically. As a result of this approach, it can be anticipated that, a holistic approach to security challenges that could be identified for IoT could be uniquely extended to different classes of IoT implementations. A one size fits all strategy will not yield results.

Acknowledgment

For availing a thriving research environment, all gratitude is extended to the Polytechnic of Namibia, which is transforming into Namibia University of Science and Technology. All the input from the research colloquial team that kept the research spirit enduring is highly appreciated.

References

[1] P.N.Mahalle,B.Anggorojati, N.R. Prasad and R.Prasad, “Identity Authentication and capability based access control (IACAC) for the Internet of Things,” Journal of cyber security and Mobility, River Publishers, Vol 1, 2013, pp309-348.

[2] D.C. ZHU Shunbing, “Research on urban public safety emergency management early warning system based on technologes for the Internet of things,” 2012 International symposium on safety science and technology, Procedia Engineering Vol 45, 2012, pp 748-754.

[3] Z. Ying-Cong and Y. Jing, “A study on the fire IOT development strategy,” Procedia Engineering, SciVerse ScienceDirect, Elservier, Vol 52, 2013, pp314-319.

[4] S.Raza, L.Wallgren and T. Voigt, “SVELTE:Real-time intrusion detection in the Internet of Things,” Ad Hoc Networks Vol 11,2013, pp 2661-2674.

[5] P.Jappinen, R. Guarneri and L. M.Correia, “An applications perspective into the future Internet,” Journal of network and computer applications, Elservier, Vol 36, 2013, pp249-254.

[6] S. Subashini and V.Kavitha, “A survey on security issues in service delivery models of cloud computing,” Journal of network and computer applications, Elservier, Vol 34, 2011, pp 1-11.

[7] J.Yick, B. Mukherjee and D.Ghosal, “Wireless sensor network survey,” Computer networks, Vol 52, 2008, pp2292-2330.

[8] Han,W. Qiu-xin and Li, “Secure solution of trusted Internet of Things based on TCM,” The Journal of china universities of Posts and Telecommunications, 2013, pp47-53.

[9] Y.B.Saied,A.Olivereau,D.Zeghlache and M.Laurent,“Lightweight collaborative key establishment scheme for the Internet of Things,” Computer Networks, 2014, pp273-295.

[10] M.P. Narendra, “Identity management framework for Internet of things,”Centre for Telefrastruktur & Aalborg University Denmark, 2013

[11] P. Kassal, I. M. Steinberg and M. D. Steinberg, “Wireless smart tag with potentiometric input for ultra low-power chemical sensing,”Sensors and actuators Vol B 184, 2013,pp 254-259.

[12] R. H.Weber, “Internet of Things-New security and privacy challenges,” Computer law & security review, Vol 26, 2010, pp 23-30.

[13] H. Suo, J. Wan, C. Ou and J. Liu, “Security in the Internet of things: A review,” 2012 International conference on computer science and electronic engineering.IEEE Computer Society, 2012, pp648-651.

[14] R. Roman, P. Najera and J. Lopez, “Securing the Internet of Things,” IEEE computer, Vol 44, No.9 , 2011, pp 51-58.

[15] F.Razzak, “Spamming the Internet of Things: A possibility and its probable solution,” Procedia computer science Vol 10,2012, pp 658-665.

[16] M.Aharan, “Critical success factors and challenges of implementing RFID in supply chain management,” Journal of supply chain and operations management,Vol 10, No.1,2012, pp144-167.

.

Appendix 2: Publication 2

An overview of potential authentication threats and attacks on Internet of Things(IoT): A focus on Smart Home applications.

Attlee M. Gamundani
Namibia University of Science and Technology
Faculty of Computing & Informatics
Computer Science Department
Windhoek, Namibia
e-mail: agamundani@nust.na

Amelia Phillips
Highline College
CIS and Computer Science Departments Cyber Security and Forensics BAS lead
Seattle , USA.
e-mail: aphillips@highline.edu

Hippolyte N. MUYINGI
Namibia University of Science and Technology
Faculty of Computing & Informatics
Windhoek, Namibia
e-mail: hmuyingi@nust.na

***Abstract*—Internet of things (IoT) are finding their wide use in various domains. IoT implementation in the Smart Home domain is one that is complex as the devices that are being used in such platforms are of different sizes and have different computational capacity. The ability to ensure security is enforced on such devices rests on how proper the authentication processes are executed. It is against this background that this paper is formulated, to give a detailed review of the potential authentication threats and attacks on IoT in the Smart Home domain in particular. The main ideas on the potential authentication threats and attacks on IoT in Smart Home applications, presented in this paper are largely informed by the detailed literature review of related work in the domain of IoT.**

Keywords- *Attacks; Authentication; IoT; Smart Home; Security; Threats.*

I. Introduction

IoT security has become a cause for concern as a result of the increased number of resource constrained smart devices which are not architecturally designed to employ robust security techniques on them (Majeed, 2017). As further summed up by (Gu & Liu, 2017) the challenges emanate from existing authentication schemes for IoT devices which include: pre-distributed authentication keys, which are not feasible; manual pairing, which require more user effort especially when dealing with many IoT devices and context-based solutions, which are mostly peer-to-peer instead of being scalable. As clearly summarized by (Khemissa & Tandjaoui, 2016a), IoT's obstacles to their deployment rest on authentication of different interconnected entities, and exchanged data confidentiality are the top concerns that need to be addressed.

Authentication can be viewed as the first line of security by ensuring enforcement of security measures at level 0 (Crossman & Liu, 2016). The process of authenticating the various processes, applications and objects require a handshake that can be done before authorization is granted. The computational limitation(D. Zhang et al., 2014) and overall capacity nature of IoT devices makes it a challenge to apply conventional security techniques (Sharaf-Dabbagh & Saad, 2016). Another key challenge as highlighted by (C. Shen et al., 2016), is that authentication that makes use of the public key system is not pliable under IoT application environments due to some of the reasons cited by (Sharaf-Dabbagh & Saad, 2016).

This main contribution of this paper is the classification of authentication threats based on the key features of IoT devices as they are functionally positioned under various applications scenarios as presented in Table 1, which are Device level; Network level and Application level. These three classifications are based on the 3-layer model for IoT, which correlates to the perception, network and application layers. In the broader sense, such authentication threats, are not confined to one application domain for IoT powered devices, but span almost every domain where IoT devices have their footprints.

To guide the discussion on IoT authentication threats in Smart Homes, this paper has four main key segments. Section I, briefly highlight some of the Smart Home applications, which paints an idea on the nature of IoT application dimensions in a Smart Home setup. Section II, gives an overview of IoT authentication approaches. Section III then builds on Section II by focusing on authentication threats, where a cascading approach is employed by having a more broader approach first, looking into the general then later the specific threats to Smart Homes. As the main core section of this paper, it further populates details on classification of threats in Smart Home applications. Then Section IV concludes and gives a way forward for the broader perspective of this research.

II. Smart Home applications

Smart Home environments as well defined by (Iinatti et al., 2017) can visually be portrayed as an organized and networked collection of heterogeneous components (i.e. be it electronics or appliances) whose defined purpose is to provide smart services seamlessly to the Smart Home owners. The essence of availing convenience is being underscored, yet attached to that functional specification of Smart Home setups is an array of security loopholes that renders them a ripe haven for different possible attacks of varying magnitudes as they interface directly with personal and sensitive data(Shin et al., 2017),(Batool et al., 2017),(Hossain et al., 2017).

The enabling environment for Smart Home as a key towards the fundamental industrial and commercial envisaged test bed for IoT, Smart Grids as well as 5G connectivity (Silverajan et al., 2015) is being fuelled by IoT (Ren et al., 2016). Commercial vendors are introducing health care, home automation and remote monitoring (D. Zhang et al., 2014),(Silverajan et al., 2015). These key facts about a Smart Home, clearly points to the fact that, Smart Homes are a delicate and an underdeveloped domain. Due to the infancy nature of the Smart Home domain, many of the solutions are on trial and not yet fully developed. On the other hand, the future projections into the growth of Smart cities(Saxena et al., 2016),(Paek, 2015)can be honoured if the critical arms to the Smart cities hub are given proper attention; hence Smart Homes are a critical component towards the wider Smart cities project.

Some of the key applications highlighted from literature for Smart Homes are intrusion and detection systems. As clearly presented in (Daramas et al., 2016) where an Android application for monitoring, configuring and notification remotely is demonstrated. Home owners are notified of any unusual events promptly on their mobile devices, equipping them with the ability to advance instant action despite being physically absent from their own premises, thereby increasing security of their homes by the click of a button (Daramas et al., 2016). As a result, traditional usage and connectivity of Internet setups will continue to play a significant role (Silverajan et al., 2015), hence the continual security challenge for Smart Home environments.

Telemedicine is another key application attributable to Smart Homes (Roy et al., 2017), where monitoring of chronic illnesses for homebound patients can be advanced. This offers in home patients monitoring and ubiquitous monitoring as demonstrated by (Hofer et al., 2015) through their personal health system dubbed COMPASS, which empowered by interoperability protocols make use of mobile devices for collection, analysis and subsequent transfer of sensed data to the set observation repository. The architecture of COMPASS is a server-client setting with a publish/ subscribe mechanism, dynamic updates of machine learning models and RESTful services to perform the create, read, update and delete operations (Hofer et al., 2015).

Another key application area for Smart Home solutions is home automation and that range from different aspects in the Smart Home environment. As highlighted by (Pienaar et al., 2015),(Ashibani et al., 2017) home based automation powered by smart phones allows control over home electrical devices (e.g. Geysers, TV, Radio, Lights, etc.) in an embedded environment portrayal. As summed up by (Ashibani et al., 2017) IoT devices are providing a wide range of services for Smart Homes such as surveillance cameras, smart lighting, and door locks. The design thereof is at the backdrop of improving physical security via remote control in a setup that mimics a normal activity based home environment even when the inhabitants are physically absent(Pienaar et al., 2015).

A more precise application is highlighted by (Brenkus et al., 2015) through the smart wall power outlet which enables intelligent home power metering system, capable of measuring power consumption and transferring the data wirelessly through the low energy integrated Bluetooth transmission. Smart plugs are one of the fast emerging IoT devices finding their way in home automation and making remote monitoring and control of Smart Homes easier (Ling et al., 2017). As an example demonstrated by (Ling et al., 2017) one can turn on the heater with their smart phone even before getting home, because of the smart plug capability, however this doesn’t come cheap as there are security challenges to some of the available brands on the market which was the main focus of Ling et al in(Ling et al., 2017).

There are various implementations of Smart Home setups such as Qiloc which enables various Smart Home applications like calendars, instant messaging and email systems to be setup(Y. Li, Wang, Cheng, Li, & Xing, 2015). This diversity positions Smart Home applications at a more vulnerable position as the attack vectors henceforth exponentially grow(Gamundani, 2015). Smart Homes ultimately have these key requirements once established, mobility management, channel security, consistent data rates and handover support as presented by (Shin et al., 2017), which hint towards the need to look at security design and requirements for Smart Home domains with more rigor.

III. IoT Authentication Overview

Authentication is among the top vital aspects for consideration towards the design of secure IoT communication. Authentication can be rendered as the first phase towards access control, and it can be device authentication or user authentication (Shaju & Panchami, 2016), even more. However, the provision of a lightweight, bulletproof and distributed authentication scheme for total security solutions towards IoT applications remains one of the biggest challenge (Mahalle, 2013). Device authentication is critical and a very challenging task for the emerging IoT (D. Chen et al., 2017).

There are three security layers for IoT, which can be summarized as perception layer, network layer and application layer (Zhao & Ge, 2013). These security layers correspondingly correlate with the three security dimensions of the IoT security architecture, which entail information security, physical security and management security (Zhao & Ge, 2013). Authentication should be the initial handshake security level that has to grant access rights to pieces of data around the Smart Home environment. This is corroborated by (Zhao & Ge, 2013), who argues that "IoT should have these characteristics: comprehensive perception, reliable transmission, and intelligent processing (page, 664)."

Detailed review work and the classification of different authentication techniques for IoT was carried out by (Saadeh et al., 2016); building on that work, this section is going to highlight and populate on some of them and highlighting some of the recent schemes as well. As (Saadeh et al., 2016) quoted (Granjal et al., 2015; S. Li et al., 2015b), there is a general agreement that traditional TCP /IP protocols such as HTTP, TCP and IP are not efficient in supporting machine to machine (M2M) communication. This clearly shows that for IoT authentication solutions to work, there has to be specific functional and technical refinement of existing solutions, in a contextual approach as guided by their implementation.

The constrained nature of devices and critical security concerns of IoT applications, sensor-based and wireless systems will demand novel solutions towards system design, network design and data processing procedures (S. C. Lin & Wen, 2016). This is further supported by (Nguyen & Iacono, 2016) in their REST-ful COAP message authentication scheme whose overarching goal through establishment of a message-oriented security layer for COAP, was to address the specific challenges stemming from the architectural style of REST and the resource constrained nature of IoT networks and devices. For proving trustable services, (S. C. Lin & Wen, 2016) explored the possibility of developing a node-based identification protocol by striking a balance between energy consumption versus malicious node detection in a heterogeneous IoT setup.

IV. Authentication threats and attacks

The main security issues in IoT as highlighted by (Sicari et al., 2015) are interdependent on authentication in one way or the other. Access control requires authentication to grant permission to the required resources or services. To ensure a secure middleware, we need to authenticate how access to the middleware is rendered and what rights can be granted, as part of middleware security. Before trust can be extended between communicating parties, these parties need to be authenticated against the set privileges and access rights. The threats therefore are evident when solutions are advanced and are not being effective, when there are gaps still evident after a solution is rendered, certain changes are effected or certain interactions are propagated and there is concern over security.

Also highlighted by (Yao et al., 2014), is the fact that, the increase in the number of sensors available and their ability to interconnect and be linked to user personal information, and the need to control personal data calls for the prioritization of data security. This then justifies why in a Smart Home environment such IoT sensors need to authenticate themselves in their interaction within their locally created ad hoc networks. This has to be ensured before allowing outsiders to have access to the collected and stored inside information, which may be sensitive to the Smart Home owner.

A. Authentication threats and attacks specific to IoT

The motivation behind looking at authentication threats specific to IoT is to prove the fact that, such threats can still be evident as well in Smart Homes. This will give a wider approach, which makes it easier to design solutions that are holistic in nature, as there is no one size fits, all when it comes to security solutions design.

The device-level IoT security vulnerabilities summarized in figure 1, are a clear indication of the varied nature of worries around IoT devices, hence authentication of such devices is already at risk from various angles. There is no doubt that IoT security incidents based on a varied nature of configurations are susceptible to different risk magnitudes (Mohsin et al., 2017). Henceforth the risk level at device level still has a substantial stake towards the overall security worries for IoT applications.

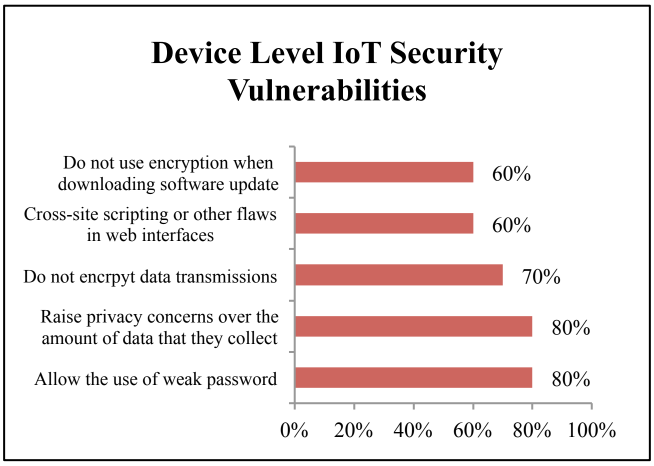


Figure 1: Device-level IoT security vulnerabilities adopted from (Tankard, 2015).

The openness nature of IoT devices positions them to suffer potential security threats as poised by (Ghosh & Mahesh, 2016), when they looked at RFID tags which were noted to suffer the major threats of privacy leakage during the authentication process.

The work of (Ahamed & Rajan, 2016) which looked at IoT application systems and security vulnerabilities and attempted to map the various applications, vulnerabilities and their impacts, was a great initiative. However, we strongly feel there is need to relook at the mapping and appreciate the interconnectedness between the three major application domains of IoT, which are Smart Home, Smart health and Smart city. What affects the Smart health, can directly affect the Smart Home as well as the Smart city. We can therefore represent the Smart health as a subset of the Smart Home and of the Smart city at a bigger scale. Health is part of the individual domain of Personal Area Network (PAN). Considering the vulnerabilities presented by (Ahamed & Rajan, 2016), it will be ideal not to complicate the representation and trying to singularly map each vulnerability towards a specific application domain, for instance, limited AAA cannot explicitly be attributable to Smart Homes alone but across board where IoT devices have been applied. We can have the same IoT device being used across the three platforms that will entail, the inherent vulnerabilities of that device will have to be dealt with for the same challenge though the magnitude of approach may vary due to other surrounding factors at functional level, even if it was used in a smart city or smart health environment. Finally the impacts mentioned henceforth cut across the different application domains. A re-modification of the mapping initially done by (Ahamed & Rajan, 2016), is represented in figure 2.

The authentication solutions proposed by (Wang et al., 2016) was targeting denial-of service (DoS) attacks in both computation and memory, which are believed to be a direct effect of either deliberate invading behaviors or jammed traffic scenes. The 2FLIP scheme(Wang et al., 2016) also aimed at achieving non-repudiation as applied to VANETS, where identification of different drivers of the same vehicle is made possible. The premise presented on the basic security goals for wireless communication by(Wang et al., 2016), as resilience to modification of message and non-repudiation speaks a lot on the key threats that IoT authentication solutions have to embrace.

The work of (X. Li, Liu, Wei, Ma, & Yang, 2015), emphasis the focus on anonymous authentication in wireless networks, pointing to the fact that, privacy protection is key and one of the threats towards authentication solutions. To support the initiative of anonymity (Rahman, Sampangi, & Sampalli, 2015) presented a lightweight anonymity and mutual authentication protocol for RFID systems to achieve the basic security goals of confidentiality, integrity and authentication. On the contrary, (Witkovski, Santin, Abreu, & Marynowski, 2015) proposed an identity management and key based authentication method to provide single sign-on in IoT, pointing to the fact that the biggest threats to IoT are humans, as they are emphasizing the need to authenticate the technicians who intend to access the appliances from the Internet.

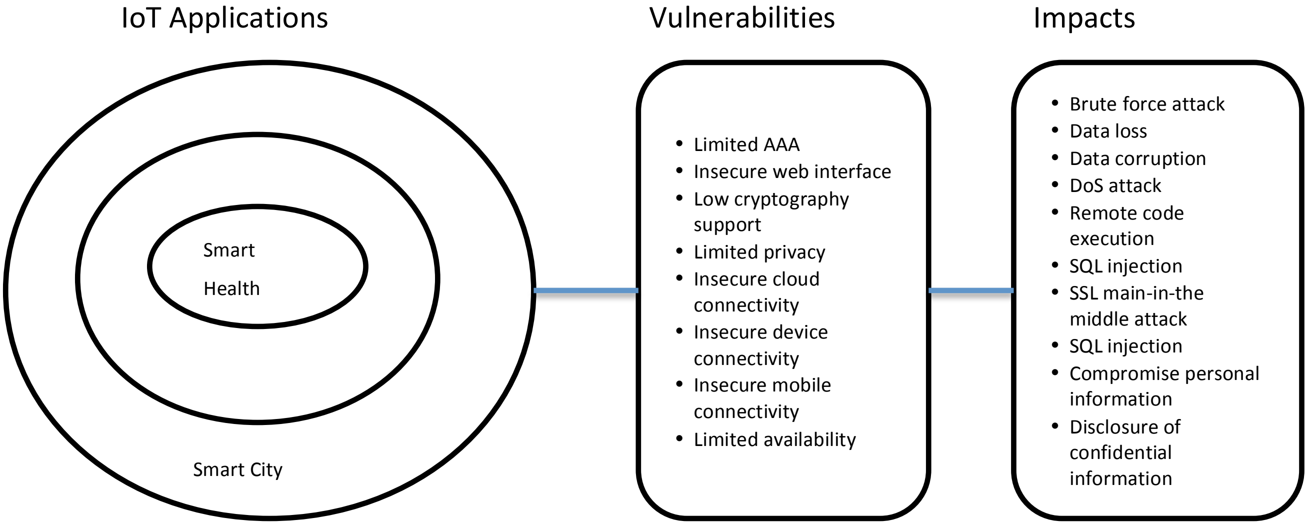


Figure 2: a modification of IoT Application, vulnerabilities and the impacts originally adapted from (Ahamed & Rajan, 2016)

As highlighted by (Cheng et al., 2015), loss of basic privacy, tracking, cloning, eavesdropping, physical attacks and denial of service attacks, are some of the surfacing threats for IoT authentication.

A look at the solution presented by (Jacobsen, Mikkelsen, & Rasmussen, 2015) tells that the scheme was targeting secure bootstrapping of wireless Home Area Network (HAN) devices by capitalizing on identity based cryptography (IBC); the main argument being that attackers may target the system at setup and network operation stages during HAN setup.

The architectural build of some of the networks that enables IoT, are a threat to authentication in themselves as clearly outlined by (Nissar, Naja, & Jamali, 2017) that the vulnerable nature of mobile ad hoc networks (MANETS) makes them prone to an adversary's malicious attacks such as dropping data or sending fake data for example. As a result, their work (Nissar et al., 2017) was on an enhancement design of the Ad hoc On-Demand Distance Vector (AODV) digital signature based authentication aimed at preventing potential routing attacks against their protocol from intruders and malicious nodes.

The key known attacks that were put into consideration by (Nissar et al., 2017) were DoS: Sleep deprivation; routing table overflow; replay attack; black hole; Eavesdropping; Sybil; wormhole; byzantine and main–in-the-middle, which proved to be what the scheme can prevent i.e. potential network layer routing attacks. Some of the unique set of security issues are mobile phishing and smishing for mobile application services as presented by (Baek & Youm, 2015), where a scenario of an attacker being able to overwrite the Near Field Data Exchange Format (NDEF) message can effectively exchange an authentic tag with a hacked tag, which opens doors for mobile malware for the NFC-enabled device.

The work of (Arafin et al., 2017) proves that some of the authentication schemes can be their own threats in their bid to provide authentication solutions. We witness a demonstration of the Voltage Over Scaling (VOS), a technique that operates on the basis of a computation process to produce a two-factor authentication scheme after profiling the error signature and gaining information of the underlying procedures whose variation was then combined with security key based authentication protocols. This approach effectively capitalized on the error by methodically profiling it to gain knowledge of the underlying process variation for computation purposes, hence providing a unique key authentication approach that employs hardware process variations.

A cloud based RFID authentication scheme presented by (Karthi & Harris, 2016) was targeting reader impersonation attack and tag location tracking attack hence was aimed at providing tag location privacy. In a similar research done by (Kaur et al., 2016), it is concluded that identity revelation, information leakage, tracking and spoofing are typical to RFID systems which are defenceless against any varied nature of attacks either active or passive. They suggest that Elliptical Curve Cryptography (ECC) has the ability to establish mutual authentication among the tags and servers, at the same time protecting them against eavesdropping, cloning risks and replay tracking attacks (Kaur et al., 2016).

The work done by (Abdullaziz, Chen, & Wang, 2016) investigated the threats of DoS attacks for Software Based Network (SDN) control channel, which proved that, if an authentication mechanism is missing, controlling resources can easily be drained rendering them incapable of offering the intended services. To counter this setup, (Abdullaziz et al., 2016) proposed a mechanism to hide information of the authentication in a lightweight manner.

Advanced persistent threats are the main driver of the solution design presented by (Juntao Chen & Zhu, 2017), where they looked at cloud enabled (security as a service) Internet of controlled things using a contract design approach.

Vehicle-to Grid (V2G) connections are reported vulnerable against security threats like exposing privacy in authenticating Electric Vehicle (EV) (Abdallah & Shen, 2017). For prevention of various insider and outsider attacks, a mutual authentication and authorization protocol which is efficient and secure is highly recommended on many different devices by (Saxena et al., 2016). The scheme achieves mitigation of insider and outsider threats every instance a device is accessed by the user through implementing a simultaneously authorization and authentication process of the user (Saxena et al., 2016).

Since most IoT devices are likely to be directly connected to the Internet while being battery powered for some, they are particularly vulnerable to DoS attacks specifically aimed at quickly draining battery and severely reducing device lifetime (Gehrmann et al., 2015). The proposed SMACK, offered an early detection mechanism by swiftly picking invalid messages upon reception and validated them against the lightweight message authentication code (Gehrmann et al., 2015), was an initiative to address the DoS threat of this nature.

Light weight mutual authentication alternatives which also are capable of providing data confidentiality are proposed by (Griffin, 2015) which make use of authentication key exchange to defend against phishing and similar attacks. As highlighted by (Mbarek et al., 2017) security vulnerabilities of lightweight authentication mechanisms and their inability to tackle memory DoS attacks, motivated the work on an improved scheme derived from the streamlined µTESLA, referred to as X – µTESLA.

Some of the key highlighted potential attacks on user authentication protocols as tested against the RRAM based lightweight user authentication work of (Arafin & Qu, 2016) are:-

- Password stealing
- Password guessing
- Password collision (false negative) – when different passwords are deemed to be authentic for one user.
- False positive alarm – a case when an authentic password is declined
- Denial of service
- Side channel attack – a group of powerful attacks that targets the vulnerabilities in hardware implementation of the security primitives and protocols

The security attacks identified by (Saxena, Choi, & Cho, 2015), when they looked at Vehicle-to-Grid (V2G) networks for security and privacy challenges in which they noted solutions advanced to such networks were costly and failed to provide resistance to known security attacks are:- (replay, man-in-the-middle, redirection, impersonation and repudiation) attacks.

The careful study by (Yoon, Das, Yoo, & Goutham Reddy, 2016) of a previous proposed enhanced secure authentication scheme for global mobile roaming services based on ECC, proved that it was vulnerable to attacks such as:- (user impersonation, man-in-the-middle, privileged insider, replay, no login phase, denial-of-service and imperfect mutual authentication phase) attacks (Yoon et al., 2016).

B. Authentication threats and attacks specific to IoT in Smart Homes

The reason why we need to zoom further into authentication threats, which are specific to Smart Homes, is the unique nature of the domain of application. Generalizing authentication threats to IoT will not give a clear picture as to which ones are more prevalent under certain domains and not other domains. The picture painted in section I, of a Smart Home, is one that entails the need to contextualize the threats so that they can effectively be handled. As indicated in Section II, a lot of similarities will be picked too under this section, validating our claim.

Control of Smart Homes is being made possible through mobile devices which can access the Internet (Ren et al., 2016), they can easily be compromised if the very devices are not secured properly causing an extension of the attack vector, hence possible threats to authentication thereof.

By reverse engineering a smart plug and advancing unique set of attacks, (Ling et al., 2017) proved that they can effectively and efficiently obtain a victim's authentication credentials. By exploiting the communication protocols, device scans attack, brute force attacks, and spoofing attacks and firmware attacks were performed. As presented by (Ling et al., 2017), where they performed a case study on a smart plug system, a typical gadget in a Smart Home environment, the following vulnerabilities were picked:- insecure communication protocols and lack of device authentication.

The Smart Home scenario is replete with smart devices that have the capability of interconnecting among themselves, making the whole security design in such an environment equally a challenging task. General security solutions cannot directly be advanced towards IoT application domains as a result of the existing unique standards and communication stacks as well as limited computing power (Sicari et al., 2015). To ensure that the refrigerator and the TV can interact as they exist in the same space (Smart Home), the authentication mechanisms needed for these two typical items would not be equivalent to the security measures that can be enforced on two computers.

Malware is a typical threat that can be directed towards personal data in a Smart Home environment if the sensors will present a weak authentication structure. Therefore authentication mechanisms need to be looked at in order to address unauthorized users and devices from accessing data they are not privileged to access (Sicari et al., 2015).

To add on to the list of attacks, (T. Shen & Maode, 2016) highlight the following:- insider attacks, impersonation attacks and man-in-the-middle attacks, reply attacks, unknown key sharing attacks which are presented as some of the prevalent authentication threats that needs serious consideration when designing security solutions. IoT devices are vulnerable to sophisticated security attacks such as man-in-the middle attacks, proffers (Kim et al., 2015) in their work.

In a Smart Home setup, user's privacy information is at risk as a result of low security strength. The magnitude of the risk extend to access of such privacy information by strangers as well as other malicious entities for example eavesdroppers who can gather and aggregate the traffic information to profile a household (Song et al., 2017)

Attacks for rolling-code garage door openers simply synchronize the malicious remote with the existing remote control signals, this requires only a few minutes or simply brute forcing the code or physical attack (Margulies, 2015). The approach by most manufactures of having a centralized authentication, authorization and commands is to reduce the demands of the inevitable tech calls (Margulies, 2015), which eventually becomes a key threat to authentication. The main reason being that, the cloud platform opens new doors to a range of attack vectors, instead of attackers having one target, they end up having mass attacks of the same model and brand at a go (Margulies, 2015) especially during software updates, attackers could gain control of the whole system.

The diversity of the Smart Home devices, causes many security and privacy challenges during their usage (Ren et al., 2016). Authentication based on fingerprint identification is still dangerous when it is defrauded with the fingerprint film (Ren et al., 2016).

V. Classification of IoT Authentication threats and attacks in Smart Homes

Now that this review has allowed us to identify the threats that are specific to IoT in Smart Homes, it will be logical to classify them accordingly into the following key classes, device, network, human and environment.

These classifications are based on the key features of IoT devices as they are functionally positioned under various applications scenarios as presented in Table 1 as Device level; Network level and Application level. These three classifications are based on the 3-layer model for IoT, which correlates to the perception, network and application layers. The threats are presented as sources of potential weakness areas that attackers can capitalize on to gain unauthorized access to data or information that is key to the overall security of IoT device in a Smart Home environment. The classification of attacks is done in two parts, considering data in transit and data at stay, as there is generally an oversight on the different states of data, which can be compromised at varying magnitudes. The examples given for each category on attacks is not an exhaustive list of the various attacks.

Table 1: Classification of Authentication threats and attacks

	Threats	Attacks	
		In transit	*At rest*

Device Level	Limited resources;
	Architecture;
	Interfaces;
	Software.
		Firmware;
		Brute force;
		Defraud;
		DoS;
			Firmware;
			Physical;
			Credentials.

Network Level	Architecture;
	Openness;
	Protocols.
		Eavesdropping;
		Device scan;
		Spoofing;
		Man-in-the middle
		Reply;
		Unknown Key sharing.
			Device Scan;
			Brute force.

Application Level	Interactions;
	Constraints;
	Environment;
	Human.
		Impersonation;
		Malware;
		Insider.	

VI. Conclusion and way forward

This paper gave a detailed summary of the various threats and attacks that can be attributable to Smart Home IoT applications. This initial task of identifying such threats then eventually categorizing them is a great milestone in paving the next task on designing solutions that practically can be implemented to address some of these threats. This work is mainly focused on the lightweight solutions that can be applied to low power, low processing capable objects in Smart Home things.

Acknowledgment

The support from the Digital Forensics and Information Security Research Cluster, the Faculty of Computing and Informatics and the NUST community's support are highly appreciated for the progress of this research work.

References

Abdallah, A., & Shen, X. (2017). Lightweight Authentication and Privacy-Preserving Scheme for V2G Connections. *IEEE Transactions on Vehicular Technology*, *66*(3), 2615–2629. https://doi.org/10.1109/TVT.2016.2577018

Abdullaziz, O. I., Chen, Y. J., & Wang, L. C. (2016). Lightweight authentication mechanism for software defined network using information hiding. *2016 IEEE Global Communications Conference, GLOBECOM 2016 - Proceedings*, 0–5. https://doi.org/10.1109/GLOCOM.2016.7841954

Ahamed, J., & Rajan, A. V. (2016). Internet of Things (IoT): Application Systems and Security Vulnerabilities.

Ahmed, S. H., & Kim, D. (2016). Named data networking-based smart home. *ICT Express*, *2*(3), 130–134. https://doi.org/10.1016/j.icte.2016.08.007

Al-Ali, A. R., Zualkernan, I. A., Rashid, M., Gupta, R., & Alikarar, M. (2017). A smart home energy management system using IoT and big data analytics approach. *IEEE Transactions on Consumer Electronics*, *63*(4), 426–434. https://doi.org/10.1109/TCE.2017.015014

Alaa, M., Zaidan, A. A., Zaidan, B. B., Talal, M., & Kiah, M. L. M. (2017). A review of smart home applications based on Internet of Things. *Journal of Network and Computer Applications*, *97*(February), 48–65. https://doi.org/10.1016/j.jnca.2017.08.017

Amin, R., Islam, S. H., Biswas, G. P., Khan, M. K., Leng, L., & Kumar, N. (2016). Design of an anonymity-preserving three-factor authenticated key exchange protocol for wireless sensor networks. *Computer Networks*, *101*, 42–62. https://doi.org/10.1016/j.comnet.2016.01.006

Amiribesheli, M., Benmansour, A., & Bouchachia, A. (2015). A review of smart homes in healthcare. *Journal of Ambient Intelligence and Humanized Computing*, *6*(4), 495–517. https://doi.org/10.1007/s12652-015-0270-2

Arafin, M. T., Gao, M., & Qu, G. (2017). VOLtA: Voltage over-scaling based lightweight authentication for IoT applications. *Proceedings of the Asia and South Pacific Design Automation Conference, ASP-DAC*, 336–341. https://doi.org/10.1109/ASPDAC.2017.7858345

Arafin, M. T., & Qu, G. (2016). RRAM based lightweight user authentication. *2015 IEEE/ACM International Conference on Computer-Aided Design, ICCAD 2015*, 139–145. https://doi.org/10.1109/ICCAD.2015.7372561

Arasteh, S., Aghili, S. F., & Mala, H. (2016). A new lightweight authentication and key agreement protocol for Internet of Things. *2016 13th International Iranian Society of Cryptology Conference on Information Security and Cryptology (ISCISC)*, 52–59. https://doi.org/10.1109/ISCISC.2016.7736451

Ashibani, Y., Kauling, D., & Mahmoud, Q. H. (2017). A Context-Aware Authentication Framework for Smart Homes. In *2017 IEEE 30th Canadian Conference on Electrical and Computer Engineering (CCECE)*.

Backes, M., Cervesato, I., Jaggard, A. D., Scedrov, A., & Tsay, J. K. (2011). Cryptographically sound security proofs for basic and public-key

Kerberos. *International Journal of Information Security*. https://doi.org/10.1007/s10207-011-0125-6

Baek, J., & Youm, H. Y. (2015). Secure and lightweight authentication protocol for NFC tag based services. *Proceedings - 2015 10th Asia Joint Conference on Information Security, AsiaJCIS 2015*, 63–68. https://doi.org/10.1109/AsiaJCIS.2015.35

Baker, A. (Wind R. (n.d.). Maintaining Data Integrity in Database Applications. Retrieved from http://docs.oracle.com/cd/B28359_01/appdev.111/b28424/adfns_constraints.htm#i1006359

Batool, S., Saqib, N. A., & Khan, M. A. (2017). Internet of Things Data Analytics for User Authentication and Activity Recognition. In *2017 Second International Conference on Fog and Mobile Edge Computing (FMEC)* (pp. 183–187).

Bhati, A., Hansen, M., & Chan, C. M. (2017). Energy conservation through smart homes in a smart city: A lesson for Singapore households. *Energy Policy*, *104*(February), 230–239. https://doi.org/10.1016/j.enpol.2017.01.032

Brandt, J. (2015). 50 billion connected IoT devices by 2020. Retrieved from https://www.privacyrisksadvisors.com/news/a50-billion-connected-iot-devices-by-2020-by-jaclyn-brandt/

Brenkus, J., Stopjakova, V., Zalusky, R., Mihalov, J., & Majer, L. (2015). Power-efficient smart metering plug for intelligent households. *Proceedings of 25th International Conference Radioelektronika, RADIOELEKTRONIKA 2015*, (296131), 110–113. https://doi.org/10.1109/RADIOELEK.2015.7129031

Challa, S., Wazid, M., Das, A. K., Kumar, N., Goutham Reddy, A., Yoon, E. J., & Yoo, K. Y. (2017). Secure Signature-Based Authenticated Key Establishment Scheme for Future IoT Applications. *IEEE Access*, *5*, 3028–3043. https://doi.org/10.1109/ACCESS.2017.2676119

Chen, D., Zhang, N., Qin, Z., Mao, X., Qin, Z., Shen, X., & Li, X. Y. (2017). S2M: A Lightweight Acoustic Fingerprints-Based Wireless Device Authentication Protocol. *IEEE Internet of Things Journal*, *4*(1), 88–100. https://doi.org/10.1109/JIOT.2016.2619679

Chen, J., Ma, J., Zhong, N., Yao, Y., Liu, J., Huang, R., … Cao, J. (2014). WaaS: Wisdom as a service. *IEEE Intelligent Systems*, *29*(6), 40–47. https://doi.org/10.1109/MIS.2014.19

Chen, J., & Zhu, Q. (2017). Security as a Service for Cloud-Enabled Internet of Controlled Things under Advanced Persistent Threats: A Contract Design Approach. *IEEE Transactions on Information Forensics and Security*, *6013*(c). https://doi.org/10.1109/TIFS.2017.2718489

Chen, S., Liu, T., Gao, F., Ji, J., Xu, Z., Qian, B., … Guan, X. (2017). Butler, Not Servant: A Human-Centric Smart Home Energy Management System. *IEEE Communications Magazine*, *55*(2), 27–33. https://doi.org/10.1109/MCOM.2017.1600699CM

Cheng, L., Shenwen, L., Yingbo, L., Na, L., & Xuren, W. (2015). A secure and lightweight authentication protocol for RFID. *ICEIEC 2015 - Proceedings of 2015 IEEE 5th International Conference on Electronics Information and Emergency Communication*, (2012), 317–320. https://doi.org/10.1109/ICEIEC.2015.7284548

Cherry, C., Hopfe, C., MacGillivray, B., & Pidgeon, N. (2017). Homes as machines: Exploring expert and public imaginaries of low carbon housing futures in the United Kingdom. *Energy Research and Social Science*, *23*, 36–45. https://doi.org/10.1016/j.erss.2016.10.011

Chiang, Y. T., Lu, C. H., & Hsu, J. Y. J. (2017). A Feature-Based Knowledge Transfer Framework for Cross-Environment Activity Recognition Toward Smart Home Applications. *IEEE Transactions on Human-Machine Systems*, *47*(3), 310–322. https://doi.org/10.1109/THMS.2016.2641679

Coetzee, L., Oosthuizen, D., & Mkhize, B. (2018). An Analysis of CoAP as Transport in an Internet of Things Environment. In *www.IST-Africa.org/Conference2018* (pp. 1–7).

Cremers, C. (2014). *Scyther User Manual*. Retrieved from http://users.ox.ac.uk/~coml0529/scyther/index.html%0AUsers

Cremers, C. J. F. (2008). Unbounded verification, falsification, and characterization of security protocols by pattern refinement. *Proceedings of the 15th ACM Conference on Computer and Communications Security - CCS '08*, 119. https://doi.org/10.1145/1455770.1455787

Cremers, C. J. F., Lafourcade, P., & Nadeau, P. (2009). Comparing state spaces in automatic security protocol analysis. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *5458 LNCS*, 74–94. https://doi.org/10.1007/978-3-642-02002-5-5

Cross, N. (2007). From a Design Science to a Design Discipline: Understanding Designerly Ways of Knowing and Thinking. *Design Research Now*, (1923), 41–54. https://doi.org/10.1007/978-3-7643-8472-2_3

Crossman, M. A., & Liu, H. (2016). Two-factor authentication through near field communication. In *2016 IEEE Symposium on Technologies for Homeland Security, HST 2016*. https://doi.org/10.1109/THS.2016.7568941

Daramas, A., Pattarakitsophon, S., Eiumtrakul, K., Tantidham, T., &

Tamkittikhun, N. (2016). HIVE: Home Automation System for Intrusion Detection. *Proceedings of the 2016 5th ICT International Student Project Conference, ICT-ISPC 2016*, 101–104. https://doi.org/10.1109/ICT-ISPC.2016.7519246

Denning, T., Kohno, T., & Levy, H. M. (2013). Computer security and the modern home. *Communications of the ACM*, *56*(1), 94. https://doi.org/10.1145/2398356.2398377

Dolev, D., & Yao, a. (1983). On the security of public key protocols. *IEEE Transactions on Information Theory*, *29*(2), 198–208. https://doi.org/10.1109/TIT.1983.1056650

Fabi, V., Spigliantini, G., & Corgnati, S. P. (2017). Insights on Smart Home Concept and Occupants' Interaction with Building Controls. *Energy Procedia*, *111*(September 2016), 759–769. https://doi.org/10.1016/j.egypro.2017.03.238

Fan, X., Qiu, B., Liu, Y., Zhu, H., & Han, B. (2017). Energy Visualization for Smart Home. *Energy Procedia*, *105*, 2545–2548. https://doi.org/10.1016/j.egypro.2017.03.732

Fanti, M. P., Faraut, G., Lesage, J.-J., & Roccotelli, M. (2016). An Integrated Framework for Binary Sensor Placement and Inhabitants Location Tracking. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, *PP*(99), 154–160. https://doi.org/10.1109/TSMC.2016.2597699

Ford, R., Pritoni, M., Sanguinetti, A., & Karlin, B. (2017). Categories and functionality of smart home technology for energy management. *Building and Environment*, *123*, 543–554. https://doi.org/10.1016/j.buildenv.2017.07.020

Gamundani, A. M. (2015). An impact review on internet of things attacks. In *2015 International Conference on Emerging Trends in Networks and Computer Communications (ETNCC)* (pp. 114–118). IEEE. https://doi.org/10.1109/ETNCC.2015.7184819

Gao, Y., Ma, H., Abbott, D., & Al-Sarawi, S. F. (2017). PUF Sensor: Exploiting PUF Unreliability for Secure Wireless Sensing. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 1–12. https://doi.org/10.1109/TCSI.2017.2695228

Ge, M., Hong, J. B., Yusuf, S. E., & Kim, D. S. (2018). Proactive defense mechanisms for the software-defined Internet of Things with non-patchable vulnerabilities. *Future Generation Computer Systems*, *78*, 568–582. https://doi.org/10.1016/j.future.2017.07.008

Gehrmann, C., Tiloca, M., & Hoglund, R. (2015). SMACK: Short message authentication check against battery exhaustion in the Internet of Things. *2015 12th Annual IEEE International Conference on Sensing, Communication, and Networking, SECON 2015*, 274–282. https://doi.org/10.1109/SAHCN.2015.7338326

Ghosh, P., & Mahesh, T. R. (2016). A Privacy Preserving Mutual Authentication Protocol for RFID based Automated Toll Collection System. In *Proceedings of 2016 International Conference on ICT in Business, Industry, and Government, ICTBIG 2016*. Published by Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ICTBIG.2016.7892668

Gioia, D. A., Corley, K. G., & Hamilton, A. L. (2013). Seeking Qualitative Rigor in Inductive Research: Notes on the Gioia Methodology. *Organizational Research Methods*, *16*(1), 15–31. https://doi.org/10.1177/1094428112452151

Gope, P., & Hwang, T. (2016a). Authentication Protocol for Securing Real-Time Application Data Access in Wireless Sensor Networks. *IEEE Transactions on Infdustrial Electronics*, *63*(11), 7124–7132.

Gope, P., & Hwang, T. (2016b). Lightweight and Energy-Efficient Mutual Authentication and Key Agreement Scheme with User Anonymity for Secure Communication in Global Mobility Networks. *IEEE Systems Journal*, *10*(4), 1370–1379. https://doi.org/10.1109/JSYST.2015.2416396

Granjal, J., Monteiro, E., & Sa Silva, J. (2015). Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues. *IEEE Communications Surveys & Tutorials*, *17*(3), 1294–1312. https://doi.org/10.1109/COMST.2015.2388550

Gray, D. E. (2014). *Doing Research in the Real World*.

Griffin, P. H. (2015). Security for ambient assisted living: Multi-factor authentication in the internet of things. *2015 IEEE Globecom Workshops, GC Wkshps 2015 - Proceedings*. https://doi.org/10.1109/GLOCOMW.2015.7413961

Gu, Z. L., & Liu, Y. (2017). Scalable group audio-based authentication scheme for IoT devices. *Proceedings - 12th International Conference on Computational Intelligence and Security, CIS 2016*, 277–281. https://doi.org/10.1109/CIS.2016.69

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, *29*(7), 1645–1660. https://doi.org/10.1016/j.future.2013.01.010

Guesgen, H. W., & Marsland, S. (2016). Using contextual information for recognising human behaviour. *International Journal of Ambient Computing and Intelligence*, *7*(1). https://doi.org/10.4018/IJACI.2016010102

Haller, S. (2013). The Things in the Internet of Things. In *Poster at the (IoT 2010). Tokyo, Japan, November*. https://doi.org/10.1201/b13090

Halpern, J. Y., & Pucella, R. (2012). Modeling adversaries in a logic for security protocol analysis. *Logical Methods in Computer Science*.

https://doi.org/10.2168/LMCS-8(1:21)2012

Han, J. (2016). Chaining the secret: Lightweight authentication for security in pervasive computing. *2016 IEEE International Conference on Pervasive Computing and Communication Workshops, PerCom Workshops 2016*, 0–2. https://doi.org/10.1109/PERCOMW.2016.7457084

Henderson, A. (2015). The CIA Triad: Confidentiality, Integrity, Availability. *Panmore Institute*. Retrieved from http://panmore.com/the-cia-triad-confidentiality-integrity-availability

Hevner, A., & Chatterjee, S. (2010). Design Research in Information Systems. *IntegratedSeries in Information Systems*, *22*, 9–23. https://doi.org/10.1007/978-1-4419-5653-8

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design Science in Information Systems Research. *MIS Quarterly*, *28*(1), 75–105. https://doi.org/10.2307/25148625

Hofer, T., Schumacher, M., & Bromuri, S. (2015). COMPASS: an Interoperable Personal Health System to Monitor and Compress Signals in Chronic Obstructive Pulmonary Disease. *Proceedings of the 9th International Conference on Pervasive Computing Technologies for Healthcare*. https://doi.org/10.4108/icst.pervasivehealth.2015.259186

Hossain, M., Noor, S., & Hasan, R. (2017). HSC-IoT: A Hardware and Software Co-Verification Based Authentication Scheme for Internet of Things. *Proceedings - 5th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering, MobileCloud 2017*, 109–116. https://doi.org/10.1109/MobileCloud.2017.35

Howell, S., Rezgui, Y., & Beach, T. (2017). Integrating building and urban semantics to empower smart water solutions. *Automation in Construction*, *81*, 434–448. https://doi.org/10.1016/j.autcon.2017.02.004

Huang, J.-J., Juang, W.-S., Fan, C.-I., Tseng, Y.-F., & Kikuchi, H. (2016). Lightweight Authentication Scheme with Dynamic Group Members in IoT Environments. In *Proceedings of the 13th International Conference on Mobile and Ubiquitous Systems: Computing Networking and Services - MOBIQUITOUS 2016*. https://doi.org/10.1145/3004010.3004020

Hui, T. K. L., Sherratt, R. S., & Sánchez, D. D. (2017). Major requirements for building Smart Homes in Smart Cities based on Internet of Things technologies. *Future Generation Computer Systems*, *76*, 358–369. https://doi.org/10.1016/j.future.2016.10.026

Iinatti, J., Member, S., & Ha, P. H. (2017). Smart Home Environments. *Ieee Transactions on Information Forensics and Security*, *12*(4), 968–979.

Jacobsen, R. H., Mikkelsen, S. A., & Rasmussen, N. H. (2015). Towards the use of pairing-based cryptography for resource-constrained home area networks. *Proceedings - 18th Euromicro Conference on Digital System Design, DSD 2015*, 233–240. https://doi.org/10.1109/DSD.2015.73

Jacobsson, A., Boldt, M., & Carlsson, B. (2016). A risk analysis of a smart home automation system. *Future Generation Computer Systems*, *56*, 719–733. https://doi.org/10.1016/j.future.2015.09.003

Janbabaei, S., Gharaee, H., & Mohammadzadeh, N. (2017). Lightweight, anonymous and mutual authentication in IoT infrastructure. *2016 8th International Symposium on Telecommunications, IST 2016*, 162–166. https://doi.org/10.1109/ISTEL.2016.7881802

Jen-Ho, Y., Ya-Fen, C., & Chih-Cheng, H. (2013). A user authentication scheme on multi-server environments for cloud computing. *ICICS 2013 - Conference Guide of the 9th International Conference on Information, Communications and Signal Processing*, 1–4. https://doi.org/10.1109/ICICS.2013.6782791

Jha, A., & Sunil, M. C. (2014). *Security considerations for Internet of Things*.

Jiang, Q. I., Zeadally, S., & He, D. (2017). Lightweight Three-Factor Authentication and Key Agreement Protocol for Internet-Integrated Wireless Sensor Networks, *5*. https://doi.org/10.1109/ACCESS.2017.2673239

Joo, I., & Choi, D. (2017). Considering Consumer ' s Electricity Bill Target. *IEEE Transactions on Consumer Electronics*, *1*(63), 19–27.

Kang, K., Pang, Z. B., & Wang, C. (2013). Security and privacy mechanism for health internet of things. *Journal of China Universities of Posts and Telecommunications*, *20*(SUPPL-2), 64–68. https://doi.org/10.1016/S1005-8885(13)60219-8

Kanuparthi, A., Karri, R., & Addepalli, S. (2013). Hardware and embedded security in the context of internet of things. *Proceedings of the 2013 ACM Workshop on Security, Privacy & Dependability for Cyber Vehicles - CyCAR '13*, 61–64. https://doi.org/10.1145/2517968.2517976

Kaplan, B., & Duchon, D. (1988). Combining Qualitative and Quantitative Methods in Information Systems. *MIS Quarterly*, *12*(4), 571–586. Retrieved from http://www.jstor.org

Kara, M., Lamouchi, O., & Ramdane-Cherif, A. (2017). A Quality Model for the Evaluation AAL Systems. *Procedia Computer Science*, *113*, 392–399. https://doi.org/10.1016/j.procs.2017.08.354

Karthi, M., & Harris, P. (2016). A Realistic Lightweight Authentication Protocol for Securing Cloud based RFID System Surekha, 168–171.

https://doi.org/10.1109/CCEM.2016.38

Kaur, K., Kumar, N., Singh, M., & Obaidat, M. S. (2016). Lightweight authentication protocol for RFID-enabled systems based on ECC. *2016 IEEE Global Communications Conference, GLOBECOM 2016 - Proceedings*, (Id). https://doi.org/10.1109/GLOCOM.2016.7841955

Khemissa, H., & Tandjaoui, D. (2016a). A Lightweight Authentication Scheme for E-Health Applications in the Context of Internet of Things. *Proceedings - NGMAST 2015: The 9th International Conference on Next Generation Mobile Applications, Services and Technologies*, 90–95. https://doi.org/10.1109/NGMAST.2015.31

Khemissa, H., & Tandjaoui, D. (2016b). A Novel Lightweight Authentication Scheme for heterogeneous Wireless Sensor Networks in the context of Internet of Things. *2016 Wireless Telecommunications Symposium (WTS)}*, 1–6.

Kim, Y. P., Yoo, S., & Yoo, C. (2015). DAoT: Dynamic and energy-aware authentication for smart home appliances in Internet of Things. In *2015 IEEE International Conference on Consumer Electronics, ICCE 2015*. https://doi.org/10.1109/ICCE.2015.7066378

Kishimoto, H., Yanai, N., & Okamura, S. (2017). An anonymous authentication protocol for smart grid. *Proceedings - 31st IEEE International Conference on Advanced Information Networking and Applications Workshops, WAINA 2017*, 62–67. https://doi.org/10.1109/WAINA.2017.41

Kothmayr, T., Schmitt, C., Hu, W., Brünig, M., & Carle, G. (2013). DTLS based security and two-way authentication for the Internet of Things. *Ad Hoc Networks*, *11*(8), 2710–2723. https://doi.org/10.1016/j.adhoc.2013.05.003

Kruusimagi, M., Sharples, S., & Robinson, D. (2017). Living with an autonomous spatiotemporal home heating system: Exploration of the user experiences (UX) through a longitudinal technology intervention-based mixed-methods approach. *Applied Ergonomics*, *65*, 286–308. https://doi.org/10.1016/j.apergo.2017.06.017

Lee, B., Kwon, O., Lee, I., & Kim, J. (2017). Companionship with smart home devices: The impact of social connectedness and interaction types on perceived social support and companionship in smart homes. *Computers in Human Behavior*, *75*, 922–934. https://doi.org/10.1016/j.chb.2017.06.031

Lee, J. S., Choi, S., & Kwon, O. (2017). Identifying multiuser activity with overlapping acoustic data for mobile decision making in smart home environments. *Expert Systems With Applications*, *81*, 299–308. https://doi.org/10.1016/j.eswa.2017.03.062

Li, G., Xu, X., & Li, Q. (2015). LADP: A lightweight authentication and delegation protocol for RFID tags. *International Conference on Ubiquitous and Future Networks, ICUFN*, *2015–Augus*, 860–865. https://doi.org/10.1109/ICUFN.2015.7182666

Li, J., Yan, Q., & Chang, V. (2018). Internet of Things: Security and privacy in a connected world. *Future Generation Computer Systems*, *78*, 931–932. https://doi.org/10.1016/j.future.2017.09.017

Li, S., Xu, L. Da, & Zhao, S. (2015a). The internet of things: a survey. *Information Systems Frontiers*, *17*(2), 243–259. https://doi.org/10.1007/s10796-014-9492-7

Li, S., Xu, L. Da, & Zhao, S. (2015b). The internet of things: a survey. *Information Systems Frontiers*, *17*(2), 243–259. https://doi.org/10.1007/s10796-014-9492-7

Li, X., Liu, H., Wei, F., Ma, J., & Yang, W. (2015). A lightweight anonymous authentication protocol using k-pseudonym set in wireless networks. *2015 IEEE Global Communications Conference, GLOBECOM 2015*. https://doi.org/10.1109/GLOCOM.2014.7417584

Li, Y., Wang, Y., Cheng, Y., Li, X., & Xing, G. (2015). QiLoc: A Qi wireless charging based system for robust user-initiated indoor location services. *2015 12th Annual IEEE International Conference on Sensing, Communication, and Networking, SECON 2015*, 480–488. https://doi.org/10.1109/SAHCN.2015.7338349

Lin, S. C., & Wen, C. Y. (2016). Energy-efficient device-based node authentication protocol for the Internet of Things. *2016 IEEE International Conference on Consumer Electronics-Taiwan, ICCE-TW 2016*, (1), 1–2. https://doi.org/10.1109/ICCE-TW.2016.7520962

Lin, Y. W., Lin, Y. B., Hsiao, C. Y., & Wang, Y. Y. (2017). IoTtalk-RC: Sensors As Universal Remote Control for Aftermarket Home Appliances. *IEEE Internet of Things Journal*, *4*(4), 1104–1112. https://doi.org/10.1109/JIOT.2017.2715859

Ling, Z., Luo, J., Xu, Y., Gao, C., Wu, K., & Fu, X. (2017). Security Vulnerabilities of Internet of Things: A Case Study of the Smart Plug System. *IEEE Internet of Things Journal*, *4662*(c), 1–1. https://doi.org/10.1109/JIOT.2017.2707465

Liu, Y., Hu, S., Member, S., Huang, H., Member, S., Ranjan, R., … Member, S. (2017). Game -Theoretic Market-Driven Smart Home Sceduling Considering Energy Balancing. *IEEE Systems Journal*, *11*(2), 910–921.

Liu, Y., Liu, L., Zhou, Y., & Hu, S. (2016). Leveraging carbon nanotube technologies in developing Physically Unclonable Function for cyber-physical system authentication. *Proceedings - IEEE INFOCOM*, *2016–Septe*, 176–180. https://doi.org/10.1109/INFCOMW.2016.7562067

Macal, C. M., & North, M. J. (2008). Agent-based modeling and simulation:

ABMS examples. *Proceedings - Winter Simulation Conference*, 101–112. https://doi.org/10.1109/WSC.2008.4736060

Mahalle, P. (2013). Identity Authentication and Capability Based Access Control (IACAC) for the Internet of Things. *Journal of Cyber …*, *1*, 309–348. Retrieved from http://forskningsbasen.deff.dk/Share.external?sp=S72df67ac-3ea5-41da-8cf0-523c6f71bbf2&sp=Saau

Majeed, A. (2017). Internet of Things (IoT): A verification framework. *2017 IEEE 7th Annual Computing and Communication Workshop and Conference, CCWC 2017*, 2–4. https://doi.org/10.1109/CCWC.2017.7868461

Mandyam, G. D. (2017). Tiered Attestation for Internet-of-Things (IoT) Devices. In *2017 9th International Conference on Communication Systems and Networks (COMSNETS)* (pp. 480–483).

Mannion, P. (2015). Optimal Analysis Algorithms are IoT's Big Opportunity | Electronics360. *Electronics 360*. Retrieved from http://electronics360.globalspec.com/article/4890/optimal-analysis-algorithms-are-iot-s-big-opportunity

Mano, L. Y., Faiçal, B. S., Nakamura, L. H. V., Gomes, P. H., Libralon, G. L., Meneguete, R. I., … Ueyama, J. (2016). Exploiting IoT technologies for enhancing Health Smart Homes through patient identification and emotion recognition. *Computer Communications*, *89–90*, 178–190. https://doi.org/10.1016/j.comcom.2016.03.010

Maple, C. (2017). Security and privacy in the internet of things. *Journal of Cyber Policy*, *2*(2), 155–184. https://doi.org/10.1080/23738871.2017.1366536

March, S. T., & Storey, V. C. (2016). Design Science in the Information Systems Discipline: An Introduction to the Special Issue on Design Science Research. *MIS Quarterly*, *32*(4), 725–730. Retrieved from url: http://www.jstor.org/stable/25148869

Margulies, J. (2015). Garage Door Openers: An Internet of Things Case Study. *IEEE Security & Privacy*, *13*(4), 80–83. https://doi.org/10.1109/MSP.2015.80

Martina, J. E., dos Santos, E., Carlos, M. C., Price, G., & Custódio, R. F. (2015). An adaptive threat model for security ceremonies. *International Journal of Information Security*. https://doi.org/10.1007/s10207-014-0253-x

Mbarek, B., Meddeb, A., Ben Jaballah, W., & Mosbah, M. (2017). A broadcast authentication scheme in IoT environments. *Proceedings of IEEE/ACS International Conference on Computer Systems and Applications, AICCSA*. https://doi.org/10.1109/AICCSA.2016.7945807

Meana-Llorián, D., González García, C., Pelayo G-Bustelo, B. C., Cueva Lovelle, J. M., & Garcia-Fernandez, N. (2017). IoFClime: The fuzzy logic and the Internet of Things to control indoor temperature regarding the outdoor ambient conditions. *Future Generation Computer Systems*, *76*, 275–284. https://doi.org/10.1016/j.future.2016.11.020

Mohsin, M., Sardar, M. U., Hasan, O., & Anwar, Z. (2017). IoTRiskAnalyzer: A Probabilistic Model Checking Based Framework for Formal Risk Analytics of the Internet of Things. *IEEE Access*, *5*, 5494–5505. https://doi.org/10.1109/ACCESS.2017.2696031

Mokhtari, G., Zhang, Q., Hargrave, C., & Ralston, J. C. (2017). Non-Wearable UWB Sensor for Human Identification in Smart Home. *IEEE Sensors Journal*, *17*(11), 3332–3340. https://doi.org/10.1109/JSEN.2017.2694555

Mokhtari, G., Zhang, Q., Nourbakhsh, G., Ball, S., & Karunanithi, M. (2017). BLUESOUND: A New Resident Identification Sensor - Using Ultrasound Array and BLE Technology for Smart Home Platform. *IEEE Sensors Journal*, *17*(5), 1503–1512. https://doi.org/10.1109/JSEN.2017.2647960

Morsalin, S., Islam, A. M. J., Rahat, G. R., Pidim, S. R. H., Rahman, A., & Siddiqe, M. A. B. (2017). Machine-to-machine communication based smart home security system by NFC, fingerprint, and PIR sensor with mobile android application. *2016 3rd International Conference on Electrical Engineering and Information and Communication Technology, ICEEiCT 2016*. https://doi.org/10.1109/CEEICT.2016.7873048

Moskvitch, K. (2017). Securing IOT: In your smart home and your connected enterprise. *Engineering and Technology*, *12*(3), 40–42. https://doi.org/10.1159/000113927

Nguyen, H. V., & Iacono, L. Lo. (2016). REST-ful CoAP Message Authentication. *Proceedings - 2015 International Workshop on Secure Internet of Things, SIoT 2015*, 35–43. https://doi.org/10.1109/SIOT.2015.8

Nissar, N., Naja, N., & Jamali, A. (2017). Lightweight authentication-based scheme for AODV in ad-hoc networks. In *2017 International Conference on Wireless Technologies, Embedded and Intelligent Systems, WITS 2017*. https://doi.org/10.1109/WITS.2017.7934616

Offermann, P., Levina, O., Schonherr, M., & Bub, U. (2009). Outline of a Design Science Research Process. *Proceedings of the 4th International Conference on Design Science Research in Information Systems and Technology, May*, 1–11. https://doi.org/10.1145/1555619.1555629

Orpwood, R. (2012). Smart Homes. *Pathy's Principles and Practice of Geriatric Medicine: Fifth Edition*. John Wiley & Sons, Ltd. https://doi.org/10.1002/9781119952930.ch124

Oyegoke, A. (2011). The constructive research approach in project management research. *International Journal of Managing Projects in Business*, *4*(4), 573–595. https://doi.org/10.1108/17538371111164029

Paek, J. (2015). Fast and Adaptive Mesh Access Control in Low-Power and Lossy Networks. *IEEE Internet of Things Journal*, *2*(5), 435–444. https://doi.org/10.1109/JIOT.2015.2457940

Parikshit N.Mahalle, Bayu Anggorojati, N. R. P. and R. P. (2013). Identity Authentication and Capability Based Access Control (IACAC) for the Internet of Things. *Journal of Cyber …*, *1*, 309–348. Retrieved from http://forskningsbasen.deff.dk/Share.external?sp=S72df67ac-3ea5-41da-8cf0-523c6f71bbf2&sp=Saau

Park, H., Hwang, S., Won, M., & Park, T. (2016). Activity-aware Sensor Cycling for Human Activity Monitoring in Smart Homes. *IEEE Communications Letters*, *7798*(c), 1–1. https://doi.org/10.1109/LCOMM.2016.2619700

Patel, S., Patel, D. R., & Navik, A. P. (2016). Energy efficient integrated authentication and access control mechanisms for Internet of Things. *2016 International Conference on Internet of Things and Applications, IOTA 2016*, 304–309. https://doi.org/10.1109/IOTA.2016.7562742

Pienaar, J. P., Fisher, R. M., & Hancke, G. P. (2015). Smartphone: The key to your connected smart home. *Proceeding - 2015 IEEE International Conference on Industrial Informatics, INDIN 2015*, 999–1004. https://doi.org/10.1109/INDIN.2015.7281871

Pöpper, C., Tippenhauer, N. O., Danev, B., & Capkun, S. (2011). Investigation of signal and message manipulations on the wireless channel. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. https://doi.org/10.1007/978-3-642-23822-2_3

Premnath, S. N., & Haas, Z. J. (2015). Security and privacy in the internet-of-things under time-and-budget-limited adversary model. *IEEE Wireless Communications Letters*, *4*(3), 277–280. https://doi.org/10.1109/LWC.2015.2408609

Rahman, M., Sampangi, R. V., & Sampalli, S. (2015). Lightweight protocol for anonymity and mutual authentication in RFID systems. *2015 12th Annual IEEE Consumer Communications and Networking Conference, CCNC 2015*, 910–915. https://doi.org/10.1109/CCNC.2015.7158097

Rawashdeh, M., Al Zamil, M. G. H., Samarah, S., Hossain, M. S., & Muhammad, G. (2017). A knowledge-driven approach for activity recognition in smart homes based on activity profiling. *Future Generation Computer Systems*. https://doi.org/10.1016/j.future.2017.10.031

Ray, B., Chowdhury, M. U., & Abawajy, J. (2017). A Multi-Protocol Security Framework to Support Internet of Things, *198*(June). https://doi.org/10.1007/978-3-319-59608-2

Ray, B. R., Chowdhury, M. U., & Abawajy, J. H. (2016). Secure Object Tracking Protocol for the Internet of Things. *IEEE Internet of Things Journal*, *3*(4), 544–553. https://doi.org/10.1109/JIOT.2016.2572729

Ray, B. R. R., Abawajy, J., Chowdhury, M., & Alelaiwi, A. (2018). Universal and secure object ownership transfer protocol for the Internet of Things. *Future Generation Computer Systems*, *78*(February), 838–849. https://doi.org/10.1016/j.future.2017.02.020

Ren, H., Song, Y., Yang, S., & Situ, F. (2016). Secure smart home: A voiceprint and internet based authentication system for remote accessing. *ICCSE 2016 - 11th International Conference on Computer Science and Education*, (Iccse), 247–251. https://doi.org/10.1109/ICCSE.2016.7581588

Rigney, C., Willens, S., Rubens, A., & Simpson, W. (2013). RFC 2687 - Remote Authentication Dial In User Service (RADIUS). *Journal of Chemical Information and Modeling*, *53*(9), 1689–1699. https://doi.org/10.1017/CBO9781107415324.004

Rizzardi, A., Sicari, S., Miorandi, D., & Coen-Porisini, A. (2016). AUPS: An Open Source AUthenticated Publish/Subscribe system for the Internet of Things. *Information Systems*, *62*, 29–41. https://doi.org/10.1016/j.is.2016.05.004

Roy, S., Chatterjee, S., Das, A. K., Chattopadhyay, S., Kumari, S., & Jo, M. (2017). Chaotic Map-based Anonymous User Authentication Scheme with User Biometrics and Fuzzy Extractor for Crowdsourcing Internet of Things. *IEEE Internet of Things Journal*, *4662*(c), 1–1. https://doi.org/10.1109/JIOT.2017.2714179

Rwegasira, D., Kondoro, A., Kelati, A., Dhaou, I. B. E. N., Mvungi, N., & Tenhunen, H. (2018). CDE for ICT Innovation Through the IoT Based iGrid Project in Tanzania. In Paul Cunningham and Miriam Cunningham (Eds) (Ed.), *IST-Africa 2018 Conference Proceedings* (pp. 1–9). IIMC International Information Management Corporation.

Saadeh, M., Sleit, A., Qatawneh, M., & Almobaideen, W. (2016). Authentication techniques for the internet of things: A survey. *Proceedings - 2016 Cybersecurity and Cyberforensics Conference, CCC 2016*, 28–34. https://doi.org/10.1109/CCC.2016.22

Saied, Y. Ben, Olivereau, A., Zeghlache, D., & Laurent, M. (2014). Lightweight collaborative key establishment scheme for the Internet of Things. *Computer Networks*, *64*, 273–295. https://doi.org/10.1016/j.comnet.2014.02.001

Savola, R., Abie, H., & Sihvonen, M. (2012). Towards Metrics-Driven Adaptive Security Management in E-Health IoT Applications. *Proceedings of the 7th International Conference on Body Area Networks*, *250241*(SeTTIT), 276–281. https://doi.org/10.4108/icst.bodynets.2012.250241

Saxena, N., Choi, B. J., & Cho, S. (2015). Lightweight privacy-preserving authentication scheme for V2G networks in the smart grid. *Proceedings - 14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2015*, *1*, 604–611. https://doi.org/10.1109/Trustcom.2015.425

Saxena, N., Choi, B. J., & Lu, R. (2016). Authentication and Authorization Scheme for Various User Roles and Devices in Smart Grid. *IEEE Transactions on Information Forensics and Security*, *11*(5), 907–921. https://doi.org/10.1109/TIFS.2015.2512525

Schaumont, P., Moriyama, D., Gulcan, E., & Aysu, A. (2016). Compact and low-power ASIP design for lightweight PUF-based authentication protocols. *IET Information Security*, *10*(5), 232–241. https://doi.org/10.1049/iet-ifs.2015.0401

SDGs. (2017). The Sustainable Development Goals Report, The Unitd Nations. *United Nations*, 1–56. https://doi.org/10.18356/3405d09f-en

Seo, D. W., Kim, H., Kim, J. S., & Lee, J. Y. (2016). Hybrid reality-based user experience and evaluation of a context-aware smart home. *Computers in Industry*, *76*, 11–23. https://doi.org/10.1016/j.compind.2015.11.003

Shahzad, M., Singh, M. P., & Carolina, N. (2017). Continuos Authentication and Authorization for the Internet of Things. *IEEE Internet Computing*, *21*(2), 86–90. https://doi.org/10.1109/MIC.2017.33

Shaju, S., & Panchami, V. (2016). BISC Authentication Algorithm : An Efficient New Authentication Algorithm Using Three Factor Authentication for Mobile Banking. In *2016 Online International Conference on Green Engineering and Technologies (IC-GET) BISC*.

Sharaf-Dabbagh, Y., & Saad, W. (2016). On the authentication of devices in the Internet of things. *WoWMoM 2016 - 17th International Symposium on a World of Wireless, Mobile and Multimedia Networks*, 1–3. https://doi.org/10.1109/WoWMoM.2016.7523532

Sharma, P., Khanna, R. R., & Bhatnagar, V. (2017). Application of TRIZ framework for resolving security issues in IOT. In *Proceeding - IEEE International Conference on Computing, Communication and Automation, ICCCA 2016*. https://doi.org/10.1109/CCAA.2016.7813921

Shen, C., Li, H., Sahin, G., & Choi, H. A. (2016). Low-complexity Scalable Authentication algorithm with Imperfect Shared Keys for Internet of Things. *2016 IEEE International Conference on Communications Workshops, ICC 2016*, 116–121. https://doi.org/10.1109/ICCW.2016.7503774

Shen, J., Liu, D., Chang, S., Shen, J., & He, D. (2016). A Lightweight Mutual Authentication Scheme for User and Server in Cloud. *Proceedings - 2015 1st International Conference on Computational Intelligence Theory, Systems and Applications, CCITSA 2015*, 183–186. https://doi.org/10.1109/CCITSA.2015.47

Shen, J., Tan, H., Chang, S., Ren, Y., & Liu, Q. (2015). A lightweight and practical RFID grouping authentication protocol in multiple-tag arrangements. *International Conference on Advanced Communication Technology, ICACT*, *2015–Augus*, 681–686. https://doi.org/10.1109/ICACT.2015.7224882

Shen, T., & Maode, M. (2016). Security Enhancements on Home Area Networks in Smart Grids. In *IEEE Region 10 Conference (TENCON)* (pp. 2444–2447).

Shin, D., Sharma, V., Kim, J., Kwon, S., & You, I. (2017). Secure and Efficient Protocol for Route Optimization in PMIPv6-based Smart Home IoT Networks. *IEEE Access*, *3536*(c). https://doi.org/10.1109/ACCESS.2017.2710379

Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks*, *76*, 146–164. https://doi.org/10.1016/j.comnet.2014.11.008

Silverajan, B., Luoma, J. P., Vajaranta, M., & Itapuro, R. (2015). Collaborative cloud-based management of home networks. *Proceedings of the 2015 IFIP/IEEE International Symposium on Integrated Network Management, IM 2015*, 786–789. https://doi.org/10.1109/INM.2015.7140376

Sivanathan, A., Sherratt, D., Gharakheili, H. H., Sivaraman, V., & Vishwanath, A. (2017). Low-cost flow-based security solutions for smart-home IoT devices. *2016 IEEE International Conference on Advanced Networks and Telecommunications Systems, ANTS 2016*. https://doi.org/10.1109/ANTS.2016.7947781

Skocir, P., Krivic, P., Tomeljak, M., Kusek, M., & Jezic, G. (2016). Activity Detection in Smart Home Environment. *Procedia Computer Science*, *96*, 672–681. https://doi.org/10.1016/j.procs.2016.08.249

Smirek, L., Zimmermann, G., & Beigl, M. (2016). Just a Smart Home or Your Smart Home - A Framework for Personalized User Interfaces Based on Eclipse Smart Home and Universal Remote Console. *Procedia Computer Science*, *58*(Euspn), 107–116. https://doi.org/10.1016/j.procs.2016.09.018

Song, T., Li, R., Mei, B., Yu, J., Xing, X., & Cheng, X. (2017). A Privacy Preserving Communication Protocol for IoT Applications in Smart Homes. *IEEE Internet of Things Journal*, *4662*(c), 1–1. https://doi.org/10.1109/JIOT.2017.2707489

Stephanie. (2017). Snowball Sampling: Definition, Advantages and Disadvantages. Retrieved January 15, 2018, from http://www.statisticshowto.com/snowball-sampling/

Tankard, C. (2015). The security issues of the Internet of Things. *Computer Fraud & Security*, *2015*(9), 11–14. https://doi.org/10.1016/S1361-3723(15)30084-1

Tao, M., Zuo, J., Liu, Z., Castiglione, A., & Palmieri, F. (2018). Multi-layer cloud architectural model and ontology-based security service framework for IoT-based smart homes. *Future Generation Computer Systems*, *78*, 1040–1051. https://doi.org/10.1016/j.future.2016.11.011

Tobin, G. A., & Begley, C. M. (2004). Methodological Rigour within a Qualittaive Framework. *Journal of Advanced Nursing*, *48*(4), 388–396. https://doi.org/10.1111/j.1365-2648.2004.03207.x

Tran, A. C., Marsland, S., Dietrich, J., Guesgen, H. W., & Lyons, P. (2010). Use cases for abnormal behaviour detection in smart homes. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* (Vol. 6159 LNCS, pp. 144–151). https://doi.org/10.1007/978-3-642-13778-5_18

Vermesan, O., Friess, P., Guillemin, P., Gusmeroli, S., Sundmaeker, H., Bassi, A., … Doody, P. (2016). Internet of Things Strategic Research Roadmap 2.1 Internet of Things Conceptual Framework 2.2 Internet of Things Vision. In *In Proceedings of 2016 International Conference on ICT in Business, Industry, and Government, ICTBIG 2016* (pp. 1–44). Institute of Electrical and Electronics Engineers Inc. https://doi.org/https://doi.org/10.1109/ICTBIG.2016.7892668

Wang, F., Xu, Y., Zhang, H., Zhang, Y., & Zhu, L. (2016). 2FLIP: A two-factor lightweight privacy-preserving authentication scheme for VANET. *IEEE Transactions on Vehicular Technology*, *65*(2), 896–911. https://doi.org/10.1109/TVT.2015.2402166

Weber, R. (2010). Internet of Things - New security and privacy challenges. *Computer Law & Security Review*. https://doi.org/10.1016/j.clsr.2009.11.008

Winter, R. (2008). Design science research in Europe. *European Journal of Information Systems*, *17*(5), 470–475. https://doi.org/10.1057/ejis.2008.44

Witkovski, A., Santin, A., Abreu, V., & Marynowski, J. (2015). An IdM and key-based authentication method for providing single sign-on in IoT. *2015 IEEE Global Communications Conference, GLOBECOM 2015*, (IdM). https://doi.org/10.1109/GLOCOM.2014.7417597

Wu, Q. X., & Li, H. (2013). Secure solution of trusted Internet of things base on TCM. *Journal of China Universities of Posts and Telecommunications*, *20*(SUPPL-2), 47–53. https://doi.org/10.1016/S1005-8885(13)60222-8

Yang, J. H., & Lin, P. Y. (2014). An ID-Based User Authentication Scheme for Cloud Computing. *2014 Tenth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*. https://doi.org/10.1109/IIH-MSP.2014.31

Yang, M. L., Narayanan, A., Parry, D., & Wang, X. (2016). A lightweight authentication scheme for transport system farecards. *2016 IEEE International Conference on RFID Technology and Applications, RFID-TA 2016*, 150–155. https://doi.org/10.1109/RFID-TA.2016.7750746

Yang, Y., Sun, J., & Guo, L. (2016). PersonaIA: A Lightweight Implicit Authentication System based on Customized User Behavior Selection. *IEEE Transactions on Dependable and Secure Computing*, *5971*(c), 1–1. https://doi.org/10.1109/TDSC.2016.2645208

Yao, X., Chen, Z., & Tian, Y. (2014). A lightweight attribute-based encryption scheme for the Internet of Things. *Future Generation Computer Systems*, *49*, 104–112. https://doi.org/10.1016/j.future.2014.10.010

Yaqoob, I., Ahmed, E., Rehman, M. H. ur, Ahmed, A. I. A., Al-garadi, M. A., Imran, M., & Guizani, M. (2017). The rise of ransomware and emerging security challenges in the Internet of Things. *Computer Networks*, *129*, 444–458. https://doi.org/10.1016/j.comnet.2017.09.003

Yoon, E.-J., Das, A. K., Yoo, K.-Y., & Goutham Reddy, A. (2016). Lightweight authentication with key-agreement protocol for mobile network environment using smart cards. *IET Information Security*, *10*(5), 272–282. https://doi.org/10.1049/iet-ifs.2015.0390

Yu, M.-D. M., Hiller, M., Delvaux, J., Sowell, R., Devadas, S., & Verbauwhede, I. (2016). A Lockdown Technique to Prevent Machine.pdf. *IEEE Transactions on Multi-Scale Computing Systems*, *2*(3), 146–159. https://doi.org/10.1109/TMSCS.2016.2553027

Zhang, D., Yang, L. T., Chen, M., Zhao, S., Guo, M., & Zhang, Y. (2014). Real-Time Locating Systems Using Active RFID for Internet of Things.

IEEE Systems Journal, *10*(3), 1–10. https://doi.org/10.1109/JSYST.2014.2346625

Zhang, N., Wu, X., Yang, C., Shen, Y., & Cheng, Y. (2017). A lightweight authentication and authorization solution based on Kerberos. *Proceedings of 2016 IEEE Advanced Information Management, Communicates, Electronic and Automation Control Conference, IMCEC 2016*, 742–746. https://doi.org/10.1109/IMCEC.2016.7867308

Zhang, R. (2017). An enhanced lightweight authentication protocol for low-cost RFID systems. *Proceedings of 2016 IEEE International Conference on Electronic Information and Communication Technology, ICEICT 2016*, (Iceict), 29–33. https://doi.org/10.1109/ICEICT.2016.7879646

Zhang, Y., Xiang, Y., Huang, X., Chen, X., & Alelaiwi, A. (2018). A matrix-based cross-layer key establishment protocol for smart homes. *Information Sciences*, *429*, 390–405. https://doi.org/10.1016/j.ins.2017.11.039

Zhao, K., & Ge, L. (2013). A survey on the internet of things security. In *Proceedings - 9th International Conference on Computational Intelligence and Security, CIS 2013* (pp. 663–667). https://doi.org/10.1109/CIS.2013.145

Zhong, H., Shao, L., & Cui, J. (2016). A Lightweight and Secure Data Authentication Scheme with Privacy Preservation for Wireless Sensor Networks. *2016 International Conference on Networking and Network Applications (NaNA)*, 210–217. https://doi.org/10.1109/NaNA.2016.85

Zhu, Q., Uddin, M. Y. S., Qin, Z., & Venkatasubramanian, N. (2017). Data collection and upload under dynamicity in smart community Internet-of-Things deployments. *Pervasive and Mobile Computing*, *42*, 166–186. https://doi.org/10.1016/j.pmcj.2017.10.003

Appendix 3: Publication 3

A Review and Costing of Lightweight Authentication Schemes for Internet of Things(IoT): *Towards design of an authentication architecture for Smart Home applications*.

Attlee M. Gamundani[1], Amelia Phillips[2], Hippolyte N. MUYINGI[3]

[1,3]Namibia University of Science and Technology, Faculty of Computing & Informatics, Computer Science Department, Windhoek, Namibia.
[2]Highline College, CIS and Computer Science, Departments Cyber Security and Forensics BAS Lead, Seattle, USA.
[1]agamundani@nust.na,[2]aphillips@highline.edu, [3]hmuyingi@nust.na

Abstract. Internet of Things (IoT) authentication for resource-constrained devices thrives under lightweight solutions. The requirements of the lightweight solutions are that, they have to meet the processing, storage and limited resource base of the resource-constrained devices. There are a number of lightweight solutions advanced for IoT under different domains. To provide feasible authentication solutions for Smart Home security calls for focus on key attributes that suit the domain in question. This paper is positioned to give a review of some existing lightweight authentication schemes, guide the selection and design of best possible solutions that can be applied to Smart Home environments. From the costing of randomly selected lightweight authentication techniques, the least costly solution is recommended for adoption.

Keywords. Authentication, Architecture, Cost, Lightweight, IoT, Smart Home.

1. Introduction

The strength and weakness of many security solutions is anchored on authentication as it grants access to various components of any system. The varied nature of the appliances in a Smart Home setup presents a huge challenge towards IoT authentication especially considering a setup where remote access is enabled (Witkovski et al., 2015). To further support the challenge of incorporating security protocols in IoT components (Arafin et al., 2017) highlights that, it is a challenge due to their extreme constrained resources.

Coming up with the best authentication scheme for resource-constrained devices is one of the biggest challenges. Existing solutions applied under similar constrained environments sometimes do not meet the strictly constrained device resource capabilities in terms of computational power and storage facility. The need therefore to evaluate existing lightweight solutions advanced even outside the Smart Home domain, will inform the design of lightweight solutions that suits strictly constrained devices.

Contribution: This paper gives a costing on a comparison basis of various IoT authentication architectures. The costing is done on the basis of the hash algorithm used, the intensity of string concatenation and exclusive or operations. These parameters were selected, without loss of generality, on the basis that, they may affect the performance of resource-constrained devices.

The best authentication approach for Smart Home applications is proposed based on the comparison results from the randomly selected lightweight authentication protocols without focus on their domain of application as depicted in Table 12.

The paper gives a quick overview of several lightweight authentication architectures. From the pool of identified lightweight authentication architectures the ones closely linked to the architectural setup of a Smart Home environment were selected.

The key observation presented in this paper is that, the lightweight stature of authentication schemes may differ based on the domain of application but the principal design goals are the same. It is therefore safe to consider one solution from a different domain and customise it for another domain. We maintain that, if the principal design goals of the scheme to be adopted are maintained, the functional specifications should be returned. Furthermore, the original security design goals of the protocol should be preserved. If that condition cannot be met, then customisation should be discarded thereof.

Organisation: Section 2 is a summary of the threat landscape for Smart Home applications. Section 3 gives an overview of IoT security with the motivation of placing authentication in light of security design. Section 4 takes a detailed look at IoT authentication by first highlighting some of the existing lightweight IoT authentication schemes then zooming into lightweight authentication schemes that have been applied to Smart Home applications. Guided by the observations from section 4, section 5 gives comparisons of lightweight solutions based on the costing of the algorithms. Section 6 finally presents some recommendations for Smart Home security solution designs. The conclusion is aptly packed in section 7.

2. Threat landscape for Smart Home applications

In general, the threats inherent to IoT devices anywhere else are typically the same threats one would find in a Smart Home setup. The Smart Home domain may have setbacks of not having formal security design setups and that mainly depend on the expertise level of the inhabitants. If at manufacturer level, certain devices don't have robust security solutions embedded in them, that will contribute to the vulnerabilities a Smart Home domain is likely to suffer.

For consideration of a threat landscape for the purposes of this paper, the Dolev-Yao attack model(Dolev & Yao, 1983) is considered. The possible attacks such as eavesdropping, message injects, replay, spoofing, insider and outside attacks are all deemed possible actions by the attacker. These attacks may be perpetrated with the motive to gain access to sensitive data, gain unauthorised control of Smart Home devices and propagate denial of service and service degradation.

3. IoT Security

The general approach to IoT security is one that carefully pays attention to the resource-constrained attributes of the various applications and devices/things. Third party platforms are sometimes used to design security solutions due to computational and storage limitations for robust solutions. The need for end-to-end security therefore becomes of paramount importance.

A typical IoT environment and implementation may involve various communication and networking protocols and designs. This is further supported by the work of (B. Ray, Chowdhury, & Abawajy, 2017), on multi-protocol security framework. For example we can consider wireless network connectivity and the Radio Frequency Identification (RFID) tags being applied for the same platform. As part of the fundamental security requirements for wireless communications, resilience towards message forgery and non-repudiation are key(Wang et al., 2016). RFID systems as poised by (R. Zhang, 2017) may cause security and privacy risks. Advancing security to RFID may call for cloud-based security solutions, hence remote authentication. An argument for proposing RFID cloud based authentication may be under the supposition that, the backend server is dependable as supported by (Karthi & Harris, 2016) when they looked at a solution which was meant for secure cloud based RFID systems.

Home area networks as mainly enabled by wireless sensors and actuators which are generally resource constrained and depend on open standard protocols(Jacobsen et al., 2015). This setup alone deems IoT security design a complex task to execute for effective results. Clearly, when it comes to IoT security, authentication as the first line of defence demands attention like any other key security activities. Many if not all of the security solutions will depend on how properly the authentication part is crafted.

4. IoT Authentication

As summarized by (Kim et al., 2015), the key operations for authentication as observed from (Denning et al., 2013; Kothmayr et al., 2013; Saied et al., 2014) are key establishment , message authentication code and handshake. It can therefore be highlighted that these are the three vital ingredients for effective authentication.

A close look at various solutions presented and applied for IoT authentication platforms, signals the varied nature of such solutions. Common among the various solutions as will be covered in this section, despite the domain of application is their lightweight nature, which of course has varying degrees depending on areas of implementation.

The first selection on lightweight IoT authentication schemes in general have been randomly on the following key categories: - two-factor authentication based, use of pseudonyms, hardware and bio based, network based, Physically Unclonable function (PUF) based, three-factor authentication based and cloud computing application focused. These were general trends observed from recent work on lightweight authentication schemes. The second selection on lightweight IoT authentication for Smart Home applications were mainly populated based on a random selection which satisfied the condition, A = {IoT, Lightweight, Authentication, Smart Home}.

4.1 Lightweight IoT Authentication Schemes in General

This section will give an overview of selected authentication schemes in groups of the classifications already highlighted above. For the scheme selected from any classification for further comparisons in section 5, a costing of the scheme will be done. The main focus will be on the authentication function, without focusing on the key establishment phase and any other procedures before or after authentication.

A. Two- factor authentication schemes

Two-factor authentication (2FLIP) solutions as applied in Vehicular Ad Hoc Network (VANET) communication presented by (Wang et al., 2016) focused on privacy-preserving. The presented 2FLIP operates by employing a certificate authority that is decentralized making use of two-factor authentication which is biologically password protected (Wang et al., 2016). For message signing, a number of very lightweight hashing processes coupled with fast message authentication-code were applied (Wang et al., 2016).

B. Pseudonym technique based schemes

Pseudonyms are another popular technique employed for lightweight solutions as can be observed from the following three examples: -
(a) The proposed *k*-pseudonym by (X. Li et al., 2015) presents an anonymous authentication protocol that functions on the premise of a shared secret key where *k*-pseudonym set, are send by the user including an open real identity as well as other *k*-1 pseudonyms. After the authentication server exchanges shared keys with each of the users in the set and verifies the authentication information, it can determine the real user and complete the authentication(X. Li et al., 2015). **(b)** A lightweight mutual authentication protocol also preserving anonymity, through use of a unique selection of pseudorandom numbers towards attaining fundamental security objectives was proposed by (Rahman et al., 2015), for RFID setups which encompassed a tag, readers and a backend server(B. R. R. Ray, Abawajy, Chowdhury, & Alelaiwi, 2018). Readers and tags realize mutual authentication as proposed by (Rahman et al., 2015) through a combination of a pseudorandom number generator as well as an XOR computation. **(c)** A similar authentication scheme that made use of pseudonym identities is presented by (Abdallah & Shen, 2017) where the scheme, provided security by discharging sessions through lightweight

overhead. Diminishing the count for exchanged messages, helped significantly reduce the cumulative computation load and the communication for Vehicle to Grid (V2G) connection, particularly for Electric Vehicles (EVs).

Considering the resource constraints for low-cost RFID tags, and as presented by (R. Zhang, 2017) that several researchers focused more on proposing protocols that are based on hash functions and pseudo-random number generators. The enhanced lightweight authentication protocol henceforth proposed by (R. Zhang, 2017) was aiming at meeting the security demands of low-cost RFID systems and improve computational cost and search efficiency at the backend database(B. R. R. Ray et al., 2018). This was an attempt to counter some of the general approach limitations. The cost analysis of the presented solution as summarised in Table 1 is relatively reasonable in terms of the lightweight features employed.

Table 1: Cost analysis of Zhang's protocol (R. Zhang, 2017)

	Device (Tag)	***Database***
Hash (x)	*3*	*3*
XOR(y)	*3*	*3*
|| (z)	*2*	*2*
Total cost	*3x+3y+2z*	*3x+3y+2z*

C. Network based schemes

An interesting trend among the authentication schemes is their ability to authenticate among the communicating things. Typical to that functionality is the lightweight authentication protocol between sensors in stationary and mobile node proposed by (Janbabaei et al., 2017) which is suitable for constrained entities. The proposed protocol by (Janbabaei et al., 2017) can ensure some security and privacy features such as anonymity, untraceability etc. The performance analysis based on costing of the protocol as depicted in Table 2 is relatively reasonable, but will require some adjustments at device level if applied to seriously constrained devices that may have little to no computational capacity.

Table 2: Cost analysis of Janbabaei et al's protocol(Janbabaei et al., 2017)

	Device	***Server***
Hash (x)	*4*	*5*
XOR(y)	*5*	*7*
|| (z)	*8*	*9*
Total cost	*4x+5y+8z*	*5x + 7y + 9z*

Central to some of the solutions is their pursuit to observe anonymity, which closely relate towards addressing the privacy concerns. An authentication scheme such as a realistic authentication scheme advanced for WSN, promising key security attributes such as user privacy, unreachability, forward/backward confidentiality and perfect forward confidentiality, which was proposed by (Gope & Hwang, 2016a) in their work aimed at real-time application security for data access in WSN which is closely related to setups typical to IoT environments. Table 3 details the performance analysis based on the costing of the protocol.

Table 3: Cost analysis of Gope et al's protocol (Gope & Hwang, 2016a)

	Device (Smart card)	***Server***
Hash (x)	*12*	*10*
XOR(y)	*6*	*5*
|| (z)	*13*	*19*
Total cost	*12x+6y+13z*	*10x + 5y +19z*

The authentication scheme for information hiding towards prevention of DoS attacks in software defined network control channel is presented by (Abdullaziz et al., 2016), which is an architecture that offloads overall network control from the end nodes to a central controller. Yet for group authentication as well as group session, (Huang et al., 2016) proposes on the client side , a key generation that is lightweight authenticated via a dynamic group as enabled by the various members in the IoT environments. Table 4, gives a summary of the costing analysis, the analysis is based on equivalent operations for hashing and XOR where encryption/decryption and nonce are used respectively.

Table 4:Costing analysis of Huang et al's protocol (Huang et al., 2016)

	Device (node i)	***Proxy Server***
Encryption (x)	*3*	*6*
nonce(y)	*1*	*-*
|| (z)	*3*	*5*
Total cost	*3x + y+3z*	*6x +5z*

D. Hardware and Bio based schemes

In the work by (C. Shen et al., 2016), an authentication framework that is scalable and less complex was proposed for low-power IoT applications and environments. The applications under consideration were those capable of using physical layer information gained from previous verified communications as part of shared secrecy between two parties. The assumption that each terminal individually made use of half-duplex radio and independent noises to generate a key meant that the extracted bit sequences were ultimately non-identical after a quantification process (C. Shen et al., 2016). As argued by (C. Shen et al., 2016) proper authentication was attained as a result of bit mismatches which required certain key properties to be applied for their handling. Similarly, (M. L. Yang, Narayanan, Parry, & Wang, 2016) proposed an authentication scheme based on the ability of the card and reader to generate identical pairwise keys, not their shared secret keys. The identical pairwise keys were generated using their own private key methods gotten from the same source.

Nevertheless, the same capabilities of authenticating among the things in IoT is apparent in an object authentication framework proposed by (Sharaf-Dabbagh & Saad, 2016) which utilize specific device information referred to here as fingerprints, for authenticating the objects in the IoT environment. The authentication is attained by effectively tracking the environmental effects towards the object's fingerprints, which can be detected through the distinction between supposed attacks and identifiable fingerprint changes (Sharaf-Dabbagh & Saad, 2016). On the other hand, the authentication scheme presented by (Khemissa & Tandjaoui, 2016b) enabled the sensor and the remote server to authenticate mutually thereby achieving communication security. While, (N. Zhang et al., 2017) proposed an authentication protocol based on Kerberos for both authentication and authorization, whose performance analysis mainly based on the costing being used for other schemes so far, is presented in Table 5. From the costing in Table 5, it is clear that optimisation was done on the gateway level as compared with the device level.

Table 5: Cost analysis of Khemissa et al's protocol(Khemissa & Tandjaoui, 2016b)

	Sensor node	*Remote user*	*Gateway*
Hash (x)	*2*	*2*	*1*
XOR(y)	*3*	*4*	*1*
|| (z)	*1*	*1*	*0*
Total cost	*2x+3y+z*	*2x +4y+ z*	*x+y*

On the other hand (Han, 2016), proposed a Pre-Shared Key (PSK) chaining system functioning on the basis of a lightweight pre-shared key enabling and offering defence against key attacks at minimal cost. Through generation of a series of arbitrary PSKs and not utilizing secret exchanges the system provides new PSK from the series of the envisaged secure session.

E. Physically Unclonable Function (PUF) based schemes

Challenge-response authentication schemes enabled through Physically Unclonable Function are another popular approach towards lightweight authentication. The work by (Liu, Liu, Zhou, & Hu, 2016) proposed a PUF that operate on carbon nanotube technologies. A hardware and software co-verification authentication scheme, a resource–efficient PUF-based security protocol is presented by (Hossain et al., 2017), and is based on elliptic curve cryptography. The cost analysis of the protocol reveals that, the protocol is expensive on the device level as compared with the provider side, hence will require optimisation if adopted for use on strictly constrained devices. In the work of (B. R. Ray, Chowdhury, & Abawajy, 2016) PUF is recommended to prevent fake injection into the chain, which is quite an important aspect to consider if overall security is to be advanced in IoT applications.

Table 6:Cost analysis of Hossain et al's protocol(Hossain et al., 2017)

	IoT	*IoT Identity Provider (IIP)*
Hash (x)	*7*	*5*
XOR (y)	*2*	*4*
|| (z)	*5*	*6*
Total cost	*7x+2y+5z*	*5x + 4y +6z*

Another work on PUF is demonstrated by (Gao, Ma, Abbott, & Al-Sarawi, 2017), where an authenticated sensing procedure is presented to identify man-in-the middle attacks and robust against eavesdropping. The scheme presented by (Yu et al., 2016) uses a server-managed challenge/response pair lockdown protocol which was an improvement of previous similar approaches.

A close analysis of PUF-based authentication done by (Schaumont, Moriyama, Gulcan, & Aysu, 2016), points to a key viewpoint that many PUF-based authentication solutions proposed, though equipped with unique features and astounding functioning assertions, there is need for practical implementation and a measure of even simple performance figures. On the contrary, PUF has been proposed in PUF-enabled tag to prevent tag cloning(G. Li, Xu, & Li, 2015)

F. Cloud computing application based schemes

A unique approach on RFID authentication is proposed by (Karthi & Harris, 2016), where a cloud based RFID authentication scheme aimed at providing tag location privacy is proposed. A performance analysis of (R. Zhang, 2017) and (Karthi & Harris, 2016), clearly show that Zhang's protocol scales way better on the device level, which is one of the focus for lightweight solutions, to reduce as much computation as necessary on the device level. Since there was a proposal to use a cloud server, we strongly feel that could have been maximally be used to reduce the computation cost at the device level on (Karthi & Harris, 2016)'s protocol.

Table 7: Cost analysis of Karthi et al's protocol (Karthi & Harris, 2016)

	Device (Tag)	*Tag reader*	*Cloud Server*
Hash (x)	*2*	*3*	*0*
XOR(y)	*6*	*6*	*0*
|| (z)	*16*	*22*	*4*
Total cost	*2x+6y+16z*	*3x +6y+22z*	*4z*

Three interrelated lightweight authentication schemes are Shen et al(J. Shen et al., 2016) , Yang et al's (J. H. Yang & Lin, 2014) ID-based user authentication scheme for cloud computing and Yang et al's (Jen-Ho et al., 2013) user authentication scheme on multi-server environments for cloud computing. These schemes are related in that Shen et al(J. Shen et al., 2016)'s protocol is an improvement of Yang et al (Jen-Ho et al., 2013; J. H. Yang & Lin, 2014)'s protocols and they are all applied in the cloud environment setup.

Table 8: Cost analysis of Yang et al(J. H. Yang & Lin, 2014), Yang et al(Jen-Ho et al., 2013) and Shen et al(J. Shen et al., 2016) ' protocols

Key:- **A**- user side **B**- server side

	Yang et al(J. H. Yang & Lin, 2014)		***Yang et al***(Jen-Ho et al., 2013)		***Shen et al***(J. Shen et al., 2016)	
	A	*B*	*A*	*B*	*A*	*B*
Hash (x)	*4*	*4*	*2*	*2*	*1*	*1*
XOR(y)	*6*	*6*	*4*	*4*	*1*	*1*
|| (z)	*4*	*4*	*6*	*6*	*1*	*1*
Total cost	*4x+6y+4z*	*4x+6y+4z*	*2x+4y+6z*	*2x+4y+6z*	*x+y+z*	*x+y+z*

G. Three-factor authentication schemes

To wrap up this section, now focus on three-factor authentication schemes. The BISC authentication algorithm uses three-factor authentication when performing identity confirming credentials from three varying authentication factors – (knowledge, possession and inherent) categories (Shaju & Panchami, 2016). In the sense of BISC the three- factor authentication combines biometrics information with colour and smart card to provide security-enhanced user authentication(Shaju & Panchami, 2016). The three-factor authenticated scheme proposed by Amin et al (Amin et al., 2016), for IoT networks was further improved by (Arasteh et al., 2016) and (Jiang et al., 2017) addressing some of the identified weaknesses such as 'smart card loss attack' user identity and password guessing attacks. Our costing analysis of the three protocols as reflected in Table 9, indicate varying improvements on the overall protocol costs.

Table 9: Cost analysis of Amin et al (A)(Amin et al., 2016), Arasteh et al (B)(Arasteh et al., 2016) and Jiang et al (C)(Jiang et al., 2017) protocols

	Ui (user)			***Gateway (GWN)***			***Sensor node (Si)***		
	A	*B*	*C*	*A*	*B*	*C*	*A*	*B*	*C*
Hash (x)	*12*	*5*	*8*	*15*	*8*	*12*	*5*	*5*	*5*
XOR(y)	*8*	*5*	*6*	*7*	*7*	*5*	*3*	*2*	*3*
|| (z)	*20*	*13*	*17*	*31*	*20*	*29*	*14*	*4*	*16*
Total cost	*12x+8y+20z*	*5x+5y+13z*	*8x+6y+17z*	*15x+7y+31z*	*8x+7y+20z*	*12x+5y+29z*	*5x+3y+14z*	*5x+2y+4z*	*5x+3y+16z*

4.2 Lightweight IoT Authentication for Smart Home Applications

With homes becoming smarter and more complex as well as technologically dependent, the call for robust and less to no human mediation reliant security solutions, are now critical as summed up by(Iinatti et al., 2017). The use of two-phase authentication is popular among many Smart Home solutions for security designs (Silverajan et al., 2015),(Margulies, 2015),(Daramas et al., 2016). A context-aware authentication framework for Smart Homes, that utilize contextual information such as the user's location, profile, calendar, request time and access behaviour patterns to enable access to home devices is presented by (Ashibani et al., 2017), which does not require additional user intervention. Pairing-based cryptography was advanced by (Jacobsen et al., 2015) for ensuring bootstrapping security for Home Area Networks (HAN) wireless devices based on IBC. We performed a costing of (Iinatti et al., 2017), as summarised in Table 10, and there is an indication of the need for more optimisation to cater for seriously constrained devices in the Smart Home.

Table 10: Performance analysis of Iinatti et al's protocol(Iinatti et al., 2017)

	Device	***Home Gateway (HG)***
Hash (x)	*8*	*11*
XOR(y)	*7*	*8*
|| (z)	*12*	*13*
Total cost	*8x+7y+12z*	*11x + 8y +13z*

Enhanced Secure Device Authentication (ESDA) scheme for HAN in smart grids is also presented by (T. Shen & Maode, 2016). The Secure Intuitive and Low Cost Device Authentication (SILDA) mechanism for HANs was resilient against insider incidents, man-in-the-middle and impersonation attacks (T. Shen & Maode, 2016). The SILDA has its problems surfacing in the management of symmetric keys to make the authentication procedure complex as during the process of establishing a secure communication channel, there is room to launch some malicious attacks by the attacker such as replay and unknown key sharing attacks(T. Shen & Maode, 2016).

'Near Field Communication (NFC) tag, secured password system and fingerprint authentication' are some of the highlighted options for authentication as proposed by (Morsalin et al., 2017), a six layered Smart Home Security System (HSS). A secure lightweight authentication scheme was proposed by (Baek & Youm, 2015), aimed at tag based services in NFC, effectively prevented such attacks as DoS, phishing, spoofing and data modification.

In the proposed solution by (Silverajan et al., 2015), an Authentication, Access Control , Assurance (AAA) - based mechanism which uses the RADIUS protocol(Rigney, Willens, Rubens, & Simpson, 2013), is presented. The focus of (Silverajan et al., 2015)'s solution was on the isolation of such functions as management, forwarding , control and routing away from the actual operations for example, access points and routers. As a solution, the REST-based scheme which was externally hosted on the cloud platform ran a resource graph as a replica of the home network, is presented by (Silverajan et al., 2015). For authentication purposes, contained in each home is the RADIUS server whose sole responsibility is to authenticate local users against given identifications for example passwords for having access to home networks (Silverajan et al., 2015). Other key attributes taken into account by the architecture are roles and time to ensure adequate authentication validation (Silverajan et al., 2015).

As observed by (Sivanathan, Sherratt, Gharakheili, Sivaraman, & Vishwanath, 2017), the use of network-level solutions has been supported by many researchers, on the premise that, they can be key in detecting possible attacks which subsequently help in the prevention of possible attacks towards IoT devices in Smart Home setups. In their proposed solution, (Sivanathan et al., 2017) did a comparison of flow-based versus packet based towards an analysis of techniques for network-level monitoring solutions in IoT. They found out that flow-based monitoring has the potential to offer more security benefits especially towards packet-based monitoring, but at relatively low processing costs.

As suggested by (Kim et al., 2015) DAoT functions by utilizing feedback control scheme as a way of dynamically selecting an energy-efficient authentication policy. With DAoT, focus is on the device identification for accessing the network, hence more efficient and cost-effective (Kim et al., 2015). The authentication of IoT devices as presented in this scheme, is possible through device ID verification by the target device, which is considered to be secure (Kim et al., 2015).

In the work of (Gope & Hwang, 2016b), they looked at a lightweight solution to secure and preserve user anonymity through roaming services in global mobility networking environments. To ensure that their solution best suit mobile devices, which were battery powered, cryptographic primitives, one-way hash functions and XOR operations were made use of. Table 11 is the summary of the costing for the protocol.

Table 11: Performance analysis of Gope et al's protocol(Gope & Hwang, 2016b)

	Device (Smart Card)	***Server (Home Agent***
Hash (x)	*9*	*11*
XOR(y)	*8*	*9*
|| (z)	*15*	*17*
Total cost	*9x+8y+15z*	*11x +9y +17z*

An android application requiring two factor authentication is presented by (Pienaar et al., 2015), which makes use of biometric security features such as facial recognition and a personalized five digit pin code, gives control of access to the application. This clearly shows some of the similarities as already discussed under section A.

5. Comparison of IoT authentication schemes based on costing.

In this section, the various selected lightweight solutions are compared on the basic architectural attributes of hash functions (x), XOR (y) and concatenation (z). Based on the comparison given in Table 12, our recommendation is that, the possible authentication techniques to adopt for Smart Home applications are those that do not have high cost but at the same time, they need to satisfy the fundamental security solution requirements. The basis for choosing a typical scheme to apply in a Smart Home environment will be the consideration of the device features and the computational capabilities. Most of the IoT devices and sensors finding themselves in Smart Home environments are typically constrained in terms of storage space, computational capacity and memory size.

The costing comparison represented in Table 12, was mainly done considering the device level authentication phase. The reason for considering the device level was mainly on the basis that, it is the constrained element in the whole IoT setup for Smart Home applications.

Table 12: Device level costing comparison of various protocols

Hash (x)	*3*	*2*	*4*	*2*	*3*	*12*	*7*	*5*	*5*	*5*	*8*	*9*	*2*	*1*	*4*
XoR(y)	*3*	*6*	*5*	*3*	*1*	*6*	*2*	*2*	*3*	*3*	*7*	*8*	*4*	*1*	*6*
||(z)	*2*	*16*	*8*	*1*	*3*	*13*	*5*	*4*	*14*	*16*	*12*	*15*	*6*	*1*	*4*
Protocols	*Zhang et al*	*Karthi et*	*Janbabaei et al*	*Khemissa et al*	*Huang et al*	*Gope et al*	*Hossain et al*	*Arasteh et al*	*Amin et al*	*Jiang et al*	*Linatti et al*	*Gope et al*	*Yang et al*	*Shen et al*	*Yang et al*

What is out of the scope of this paper, but also critical to consider when looking at comparison of authentication architectures, which we strongly believe will bring an in-depth dimension to the classification of the various authentication techniques is what was covered by (Saadeh et al., 2016). The classification done by (Saadeh et al., 2016) depicts two distinct approaches, firstly according to how the authentication process is performed, which they classified into centralized and distributed, which was tallied against hierarchical and flat based. Secondly, they performed a classification according to the characteristics of the authentication process and the attributes employed. The comparisons of the selected authentication techniques by (Saadeh et al., 2016) based on the evaluation model and their resistance to some identified security attacks, brings a comprehensive approach towards evaluation and subsequently selecting the best features to incorporate when designing an authentication architecture.

6. Recommendations for Smart Home solutions

To guide the choice of solutions, for Smart Homes, from the comparisons done in Table 12, it will be ideal to consider all the dimensions of the authentication protocol to be advanced from functional specifications to their resilience towards some known attacks as well as their resource requirements.

It will be important to consider the identity of the objects for a holistic authentication solution. Uniquely identifying the objects or things in IoT will help, but this aspect is out of the scope of this paper. We strongly believe digital signatures will play an important role in this regard and introducing agent based trusted solutions would enhance the authentication solutions to be advanced to IoT platforms especially in Smart Homes.

From the comparison done in Table 12, we picked Huang et al(Huang et al., 2016), Khemissa et al(Khemissa & Tandjaoui, 2016b) and Shen et al(J. Shen et al., 2016)'s protocols as probable best options based on their costing values. We did further comparisons as depicted in Table 13, of the three based on the threats they address. This comparison was focused on the threat landscape highlighted in section 2.

Table 13: Device level costing comparison of various protocols

Khemissa et al	✔	✔	✔	✔	✔	✔	
Huang et al	✔	✔	✔	✔			
Shen et al	✔	✔	✔	✔	✔		✔
Threats addressed	*Dictionary attack*	*Man-in-the middle attack*	*Replay attack*	*Modification attack*	*Impersonation attack*	*DoS attack*	*Forward security*

It is imperative to note that addressing all the threats using one solution may not be practical, especially with the backdrop of lightweight requirements. We may conclude based on this analysis that shen et al(J. Shen et al., 2016) can suitably be adopted for solutions in Smart Home applications.

7. Conclusion

Outlined in this paper was coverage of the different authentication architectures that can be found in the IoT domain, this is by no way an exhaustive list of the various approaches being developed and implemented as this area is receiving wide attention from various angles. A relook at existing authentication protocols will help in improving on newer designs and addressing some of the shortfalls of similar and previous versions. As security remains an evolving discipline, rigid approaches and standardizations for measuring some of the solutions on the ground may not be feasible, henceforth, it will be ideal to have an outline of fundamental features to be incorporated in typical solutions.

As the focus of the paper was to identify the best lightweight authentication approaches for Smart Homes, it will be ideal to consider a number of key aspects when selecting a solution to advance towards design of authentication techniques for Smart Homes. There are crosscutting dynamics in the various authentication approaches already in use and borrowing the best features from one solution and combining with the other will surely give a recipe for a secure solution.

This paper employed costing of probable authentication architectures for consideration hence helping in the decision of selecting a less cost effective solution to propose for lightweight applications.

Acknowledgments.

The support from the Digital Forensics and Information security research cluster, the Faculty of Computing and Informatics and the NUST community's support are highly appreciated for the progress of this research work.

References.

Abdallah, A., & Shen, X. (2017). Lightweight Authentication and Privacy-Preserving Scheme for V2G Connections. *IEEE Transactions on Vehicular Technology*, *66*(3), 2615–2629. https://doi.org/10.1109/TVT.2016.2577018

Abdullaziz, O. I., Chen, Y. J., & Wang, L. C. (2016). Lightweight authentication mechanism for software defined network using information hiding. *2016 IEEE Global Communications Conference, GLOBECOM 2016 - Proceedings*, 0–5. https://doi.org/10.1109/GLOCOM.2016.7841954

Ahamed, J., & Rajan, A. V. (2016). Internet of Things (IoT): Application Systems and Security Vulnerabilities.

Ahmed, S. H., & Kim, D. (2016). Named data networking-based smart home. *ICT Express*, *2*(3), 130–134. https://doi.org/10.1016/j.icte.2016.08.007

Al-Ali, A. R., Zualkernan, I. A., Rashid, M., Gupta, R., & Alikarar, M. (2017). A smart home energy management system using IoT and big data analytics approach. *IEEE Transactions on Consumer Electronics*, *63*(4), 426–434. https://doi.org/10.1109/TCE.2017.015014

Alaa, M., Zaidan, A. A., Zaidan, B. B., Talal, M., & Kiah, M. L. M. (2017). A review of smart home applications based on Internet of Things. *Journal of Network and Computer Applications*, *97*(February), 48–65. https://doi.org/10.1016/j.jnca.2017.08.017

Amin, R., Islam, S. H., Biswas, G. P., Khan, M. K., Leng, L., & Kumar, N. (2016). Design of an anonymity-preserving three-factor authenticated key exchange protocol for wireless sensor networks. *Computer Networks*, *101*, 42–62. https://doi.org/10.1016/j.comnet.2016.01.006

Amiribesheli, M., Benmansour, A., & Bouchachia, A. (2015). A review of smart homes in healthcare. *Journal of Ambient Intelligence and Humanized Computing*, *6*(4), 495–517. https://doi.org/10.1007/s12652-015-0270-2

Arafin, M. T., Gao, M., & Qu, G. (2017). VOLtA: Voltage over-scaling based lightweight authentication for IoT applications. *Proceedings of the Asia and South Pacific Design Automation Conference, ASP-DAC*, 336–341. https://doi.org/10.1109/ASPDAC.2017.7858345

Arafin, M. T., & Qu, G. (2016). RRAM based lightweight user authentication. *2015 IEEE/ACM International Conference on Computer-Aided Design, ICCAD 2015*, 139–145. https://doi.org/10.1109/ICCAD.2015.7372561

Arasteh, S., Aghili, S. F., & Mala, H. (2016). A new lightweight authentication and key agreement protocol for Internet of Things. *2016 13th International Iranian Society of Cryptology Conference on Information Security and Cryptology (ISCISC)*, 52–59. https://doi.org/10.1109/ISCISC.2016.7736451

Ashibani, Y., Kauling, D., & Mahmoud, Q. H. (2017). A Context-Aware Authentication Framework for Smart Homes. In *2017 IEEE 30th Canadian Conference on Electrical and Computer Engineering (CCECE)*.

Backes, M., Cervesato, I., Jaggard, A. D., Scedrov, A., & Tsay, J. K. (2011). Cryptographically sound security proofs for basic and public-key Kerberos. *International Journal of Information Security*. https://doi.org/10.1007/s10207-011-0125-6

Baek, J., & Youm, H. Y. (2015). Secure and lightweight authentication protocol for NFC tag based services. *Proceedings - 2015 10th Asia Joint Conference on Information Security, AsiaJCIS 2015*, 63–68. https://doi.org/10.1109/AsiaJCIS.2015.35

Baker, A. (Wind R. (n.d.). Maintaining Data Integrity in Database Applications. Retrieved from http://docs.oracle.com/cd/B28359_01/appdev.111/b28424/adfns_constraints.htm#i1006359

Batool, S., Saqib, N. A., & Khan, M. A. (2017). Internet of Things Data Analytics for User Authentication and Activity Recognition. In *2017 Second International Conference on Fog and Mobile Edge Computing (FMEC)* (pp. 183–187).

Bhati, A., Hansen, M., & Chan, C. M. (2017). Energy conservation through smart homes in a smart city: A lesson for Singapore households. *Energy Policy*, *104*(February), 230–239. https://doi.org/10.1016/j.enpol.2017.01.032

Brandt, J. (2015). 50 billion connected IoT devices by 2020. Retrieved from https://www.privacyrisksadvisors.com/news/a50-billion-connected-iot-devices-by-2020-by-jaclyn-brandt/

Brenkus, J., Stopjakova, V., Zalusky, R., Mihalov, J., & Majer, L. (2015). Power-efficient smart metering plug for intelligent households. *Proceedings of 25th International Conference Radioelektronika, RADIOELEKTRONIKA 2015*, (296131), 110–113. https://doi.org/10.1109/RADIOELEK.2015.7129031

Challa, S., Wazid, M., Das, A. K., Kumar, N., Goutham Reddy, A., Yoon, E. J., & Yoo, K. Y. (2017). Secure Signature-Based Authenticated Key Establishment Scheme for Future IoT Applications. *IEEE Access*, *5*, 3028–3043. https://doi.org/10.1109/ACCESS.2017.2676119

Chen, D., Zhang, N., Qin, Z., Mao, X., Qin, Z., Shen, X., & Li, X. Y. (2017). S2M: A Lightweight Acoustic Fingerprints-Based Wireless Device Authentication Protocol. *IEEE Internet of Things Journal*, *4*(1), 88–100. https://doi.org/10.1109/JIOT.2016.2619679

Chen, J., Ma, J., Zhong, N., Yao, Y., Liu, J., Huang, R., … Cao, J. (2014). WaaS: Wisdom as a service. *IEEE Intelligent Systems*, *29*(6), 40–47. https://doi.org/10.1109/MIS.2014.19

Chen, J., & Zhu, Q. (2017). Security as a Service for Cloud-Enabled Internet of Controlled Things under Advanced Persistent Threats: A Contract Design Approach. *IEEE Transactions on Information Forensics and Security*, *6013*(c). https://doi.org/10.1109/TIFS.2017.2718489

Chen, S., Liu, T., Gao, F., Ji, J., Xu, Z., Qian, B., … Guan, X. (2017). Butler, Not Servant: A Human-Centric Smart Home Energy Management System. *IEEE Communications Magazine*, *55*(2), 27–33. https://doi.org/10.1109/MCOM.2017.1600699CM

Cheng, L., Shenwen, L., Yingbo, L., Na, L., & Xuren, W. (2015). A secure and lightweight authentication protocol for RFID. *ICEIEC 2015 - Proceedings of 2015 IEEE 5th International Conference on Electronics Information and Emergency Communication*, (2012), 317–320. https://doi.org/10.1109/ICEIEC.2015.7284548

Cherry, C., Hopfe, C., MacGillivray, B., & Pidgeon, N. (2017). Homes as machines: Exploring expert and public imaginaries of low carbon housing futures in the United Kingdom. *Energy Research and Social Science*, *23*, 36–45. https://doi.org/10.1016/j.erss.2016.10.011

Chiang, Y. T., Lu, C. H., & Hsu, J. Y. J. (2017). A Feature-Based Knowledge Transfer Framework for Cross-Environment Activity Recognition Toward Smart Home Applications. *IEEE Transactions on Human-Machine Systems*, *47*(3), 310–322. https://doi.org/10.1109/THMS.2016.2641679

Coetzee, L., Oosthuizen, D., & Mkhize, B. (2018). An Analysis of CoAP as Transport in an Internet of Things Environment. In *www.IST-Africa.org/Conference2018* (pp. 1–7).

Cremers, C. (2014). *Scyther User Manual*. Retrieved from http://users.ox.ac.uk/~coml0529/scyther/index.html%0AUsers

Cremers, C. J. F. (2008). Unbounded verification, falsification, and characterization of security protocols by pattern refinement. *Proceedings of the 15th ACM Conference on Computer and Communications Security - CCS '08*, 119. https://doi.org/10.1145/1455770.1455787

Cremers, C. J. F., Lafourcade, P., & Nadeau, P. (2009). Comparing state spaces in automatic security protocol analysis. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *5458 LNCS*, 74–94. https://doi.org/10.1007/978-3-642-02002-5-5

Cross, N. (2007). From a Design Science to a Design Discipline: Understanding Designerly Ways of Knowing and Thinking. *Design Research Now*, (1923), 41–54. https://doi.org/10.1007/978-3-7643-8472-2_3

Crossman, M. A., & Liu, H. (2016). Two-factor authentication through near field communication. In *2016 IEEE Symposium on Technologies for Homeland Security, HST 2016*. https://doi.org/10.1109/THS.2016.7568941

Daramas, A., Pattarakitsophon, S., Eiumtrakul, K., Tantidham, T., & Tamkittikhun, N. (2016). HIVE: Home Automation System for Intrusion Detection. *Proceedings of the 2016 5th ICT International Student Project Conference, ICT-ISPC 2016*, 101–104. https://doi.org/10.1109/ICT-ISPC.2016.7519246

Denning, T., Kohno, T., & Levy, H. M. (2013). Computer security and the modern home. *Communications of the ACM*, *56*(1), 94. https://doi.org/10.1145/2398356.2398377

Dolev, D., & Yao, a. (1983). On the security of public key protocols. *IEEE Transactions on Information Theory*, *29*(2), 198–208. https://doi.org/10.1109/TIT.1983.1056650

Fabi, V., Spigliantini, G., & Corgnati, S. P. (2017). Insights on Smart Home Concept and Occupants' Interaction with Building Controls. *Energy Procedia*, *111*(September 2016), 759–769. https://doi.org/10.1016/j.egypro.2017.03.238

Fan, X., Qiu, B., Liu, Y., Zhu, H., & Han, B. (2017). Energy Visualization for Smart Home. *Energy Procedia*, *105*, 2545–2548. https://doi.org/10.1016/j.egypro.2017.03.732

Fanti, M. P., Faraut, G., Lesage, J.-J., & Roccotelli, M. (2016). An Integrated Framework for Binary Sensor Placement and Inhabitants Location Tracking. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, *PP*(99), 154–160. https://doi.org/10.1109/TSMC.2016.2597699

Ford, R., Pritoni, M., Sanguinetti, A., & Karlin, B. (2017). Categories and functionality of smart home technology for energy management. *Building and Environment*, *123*, 543–554. https://doi.org/10.1016/j.buildenv.2017.07.020

Gamundani, A. M. (2015). An impact review on internet of things attacks. In *2015 International Conference on Emerging Trends in Networks and Computer Communications (ETNCC)* (pp. 114–118). IEEE. https://doi.org/10.1109/ETNCC.2015.7184819

Gao, Y., Ma, H., Abbott, D., & Al-Sarawi, S. F. (2017). PUF Sensor: Exploiting PUF Unreliability for Secure Wireless Sensing. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 1–12. https://doi.org/10.1109/TCSI.2017.2695228

Ge, M., Hong, J. B., Yusuf, S. E., & Kim, D. S. (2018). Proactive defense mechanisms for the software-defined Internet of Things with non-patchable vulnerabilities. *Future Generation Computer Systems*, *78*, 568–582. https://doi.org/10.1016/j.future.2017.07.008

Gehrmann, C., Tiloca, M., & Hoglund, R. (2015). SMACK: Short message authentication check against battery exhaustion in the Internet of Things. *2015 12th Annual IEEE International Conference on Sensing, Communication, and Networking, SECON 2015*, 274–282. https://doi.org/10.1109/SAHCN.2015.7338326

Ghosh, P., & Mahesh, T. R. (2016). A Privacy Preserving Mutual Authentication Protocol for RFID based Automated Toll Collection System. In *Proceedings of 2016 International Conference on ICT in Business, Industry, and Government, ICTBIG 2016*. Published by Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ICTBIG.2016.7892668

Gioia, D. A., Corley, K. G., & Hamilton, A. L. (2013). Seeking Qualitative Rigor in Inductive Research: Notes on the Gioia Methodology. *Organizational Research Methods*, *16*(1), 15–31. https://doi.org/10.1177/1094428112452151

Gope, P., & Hwang, T. (2016a). Authentication Protocol for Securing Real-Time Application Data Access in Wireless Sensor Networks. *IEEE Transactions on Infdustrial Electronics*, *63*(11), 7124–7132.

Gope, P., & Hwang, T. (2016b). Lightweight and Energy-Efficient Mutual Authentication and Key Agreement Scheme with User Anonymity for Secure Communication in Global Mobility Networks. *IEEE Systems Journal*, *10*(4), 1370–1379. https://doi.org/10.1109/JSYST.2015.2416396

Granjal, J., Monteiro, E., & Sa Silva, J. (2015). Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues. *IEEE Communications Surveys & Tutorials*, *17*(3), 1294–1312. https://doi.org/10.1109/COMST.2015.2388550

Gray, D. E. (2014). *Doing Research in the Real World*.

Griffin, P. H. (2015). Security for ambient assisted living: Multi-factor authentication in the internet of things. *2015 IEEE Globecom Workshops, GC Wkshps 2015 - Proceedings*. https://doi.org/10.1109/GLOCOMW.2015.7413961

Gu, Z. L., & Liu, Y. (2017). Scalable group audio-based authentication scheme for IoT devices. *Proceedings - 12th International Conference on Computational Intelligence and Security, CIS 2016*, 277–281. https://doi.org/10.1109/CIS.2016.69

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, *29*(7), 1645–1660. https://doi.org/10.1016/j.future.2013.01.010

Guesgen, H. W., & Marsland, S. (2016). Using contextual information for recognising human behaviour. *International Journal of Ambient Computing and Intelligence*, *7*(1). https://doi.org/10.4018/IJACI.2016010102

Haller, S. (2013). The Things in the Internet of Things. In *Poster at the (IoT 2010). Tokyo, Japan, November*. https://doi.org/10.1201/b13090

Halpern, J. Y., & Pucella, R. (2012). Modeling adversaries in a logic for security protocol analysis. *Logical Methods in Computer Science*. https://doi.org/10.2168/LMCS-8(1:21)2012

Han, J. (2016). Chaining the secret: Lightweight authentication for security in pervasive computing. *2016 IEEE International Conference on Pervasive Computing and Communication Workshops, PerCom Workshops 2016*, 0–2. https://doi.org/10.1109/PERCOMW.2016.7457084

Henderson, A. (2015). The CIA Triad: Confidentiality, Integrity, Availability. *Panmore Institute*. Retrieved from http://panmore.com/the-cia-triad-confidentiality-integrity-availability

Hevner, A., & Chatterjee, S. (2010). Design Research in Information Systems. *IntegratedSeries in Information Systems*, *22*, 9–23. https://doi.org/10.1007/978-1-4419-5653-8

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design Science in Information Systems Research. *MIS Quarterly*, *28*(1), 75–105. https://doi.org/10.2307/25148625

Hofer, T., Schumacher, M., & Bromuri, S. (2015). COMPASS: an Interoperable Personal Health System to Monitor and Compress Signals in Chronic Obstructive Pulmonary Disease. *Proceedings of the 9th International Conference on Pervasive Computing Technologies for Healthcare*. https://doi.org/10.4108/icst.pervasivehealth.2015.259186

Hossain, M., Noor, S., & Hasan, R. (2017). HSC-IoT: A Hardware and Software Co-Verification Based Authentication Scheme for Internet of Things.

Proceedings - 5th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering, MobileCloud 2017, 109–116. https://doi.org/10.1109/MobileCloud.2017.35

Howell, S., Rezgui, Y., & Beach, T. (2017). Integrating building and urban semantics to empower smart water solutions. *Automation in Construction*, *81*, 434–448. https://doi.org/10.1016/j.autcon.2017.02.004

Huang, J.-J., Juang, W.-S., Fan, C.-I., Tseng, Y.-F., & Kikuchi, H. (2016). Lightweight Authentication Scheme with Dynamic Group Members in IoT Environments. In *Proceedings of the 13th International Conference on Mobile and Ubiquitous Systems: Computing Networking and Services - MOBIQUITOUS 2016*. https://doi.org/10.1145/3004010.3004020

Hui, T. K. L., Sherratt, R. S., & Sánchez, D. D. (2017). Major requirements for building Smart Homes in Smart Cities based on Internet of Things technologies. *Future Generation Computer Systems*, *76*, 358–369. https://doi.org/10.1016/j.future.2016.10.026

Iinatti, J., Member, S., & Ha, P. H. (2017). Smart Home Environments. *Ieee Transactions on Information Forensics and Security*, *12*(4), 968–979.

Jacobsen, R. H., Mikkelsen, S. A., & Rasmussen, N. H. (2015). Towards the use of pairing-based cryptography for resource-constrained home area networks. *Proceedings - 18th Euromicro Conference on Digital System Design, DSD 2015*, 233–240. https://doi.org/10.1109/DSD.2015.73

Jacobsson, A., Boldt, M., & Carlsson, B. (2016). A risk analysis of a smart home automation system. *Future Generation Computer Systems*, *56*, 719–733. https://doi.org/10.1016/j.future.2015.09.003

Janbabaei, S., Gharaee, H., & Mohammadzadeh, N. (2017). Lightweight, anonymous and mutual authentication in IoT infrastructure. *2016 8th International Symposium on Telecommunications, IST 2016*, 162–166. https://doi.org/10.1109/ISTEL.2016.7881802

Jen-Ho, Y., Ya-Fen, C., & Chih-Cheng, H. (2013). A user authentication scheme on multi-server environments for cloud computing. *ICICS 2013 - Conference Guide of the 9th International Conference on Information, Communications and Signal Processing*, 1–4. https://doi.org/10.1109/ICICS.2013.6782791

Jha, A., & Sunil, M. C. (2014). *Security considerations for Internet of Things*.

Jiang, Q. I., Zeadally, S., & He, D. (2017). Lightweight Three-Factor Authentication and Key Agreement Protocol for Internet-Integrated Wireless Sensor Networks, *5*. https://doi.org/10.1109/ACCESS.2017.2673239

Joo, I., & Choi, D. (2017). Considering Consumer ' s Electricity Bill Target. *IEEE Transactions on Consumer Electronics*, *1*(63), 19–27.

Kang, K., Pang, Z. B., & Wang, C. (2013). Security and privacy mechanism for health internet of things. *Journal of China Universities of Posts and Telecommunications*, *20*(SUPPL-2), 64–68. https://doi.org/10.1016/S1005-8885(13)60219-8

Kanuparthi, A., Karri, R., & Addepalli, S. (2013). Hardware and embedded security in the context of internet of things. *Proceedings of the 2013 ACM Workshop on Security, Privacy & Dependability for Cyber Vehicles - CyCAR '13*, 61–64. https://doi.org/10.1145/2517968.2517976

Kaplan, B., & Duchon, D. (1988). Combining Qualitative and Quantitative Methods in lnformation Systems. *MIS Quarterly*, *12*(4), 571–586. Retrieved from http://www.jstor.org

Kara, M., Lamouchi, O., & Ramdane-Cherif, A. (2017). A Quality Model for the Evaluation AAL Systems. *Procedia Computer Science*, *113*, 392–399. https://doi.org/10.1016/j.procs.2017.08.354

Karthi, M., & Harris, P. (2016). A Realistic Lightweight Authentication Protocol for Securing Cloud based RFID System Surekha, 168–171. https://doi.org/10.1109/CCEM.2016.38

Kaur, K., Kumar, N., Singh, M., & Obaidat, M. S. (2016). Lightweight authentication protocol for RFID-enabled systems based on ECC. *2016 IEEE Global Communications Conference, GLOBECOM 2016 - Proceedings*, (Id). https://doi.org/10.1109/GLOCOM.2016.7841955

Khemissa, H., & Tandjaoui, D. (2016a). A Lightweight Authentication Scheme for E-Health Applications in the Context of Internet of Things. *Proceedings - NGMAST 2015: The 9th International Conference on Next Generation Mobile Applications, Services and Technologies*, 90–95. https://doi.org/10.1109/NGMAST.2015.31

Khemissa, H., & Tandjaoui, D. (2016b). A Novel Lightweight Authentication Scheme for heterogeneous Wireless Sensor Networks in the context of Internet of Things. *2016 Wireless Telecommunications Symposium (WTS)}*, 1–6.

Kim, Y. P., Yoo, S., & Yoo, C. (2015). DAoT: Dynamic and energy-aware authentication for smart home appliances in Internet of Things. In *2015 IEEE International Conference on Consumer Electronics, ICCE 2015*. https://doi.org/10.1109/ICCE.2015.7066378

Kishimoto, H., Yanai, N., & Okamura, S. (2017). An anonymous authentication protocol for smart grid. *Proceedings - 31st IEEE International Conference on*

Advanced Information Networking and Applications Workshops, WAINA 2017, 62–67. https://doi.org/10.1109/WAINA.2017.41

Kothmayr, T., Schmitt, C., Hu, W., Brünig, M., & Carle, G. (2013). DTLS based security and two-way authentication for the Internet of Things. *Ad Hoc Networks*, *11*(8), 2710–2723. https://doi.org/10.1016/j.adhoc.2013.05.003

Kruusimagi, M., Sharples, S., & Robinson, D. (2017). Living with an autonomous spatiotemporal home heating system: Exploration of the user experiences (UX) through a longitudinal technology intervention-based mixed-methods approach. *Applied Ergonomics*, *65*, 286–308. https://doi.org/10.1016/j.apergo.2017.06.017

Lee, B., Kwon, O., Lee, I., & Kim, J. (2017). Companionship with smart home devices: The impact of social connectedness and interaction types on perceived social support and companionship in smart homes. *Computers in Human Behavior*, *75*, 922–934. https://doi.org/10.1016/j.chb.2017.06.031

Lee, J. S., Choi, S., & Kwon, O. (2017). Identifying multiuser activity with overlapping acoustic data for mobile decision making in smart home environments. *Expert Systems With Applications*, *81*, 299–308. https://doi.org/10.1016/j.eswa.2017.03.062

Li, G., Xu, X., & Li, Q. (2015). LADP: A lightweight authentication and delegation protocol for RFID tags. *International Conference on Ubiquitous and Future Networks, ICUFN*, *2015–Augus*, 860–865. https://doi.org/10.1109/ICUFN.2015.7182666

Li, J., Yan, Q., & Chang, V. (2018). Internet of Things: Security and privacy in a connected world. *Future Generation Computer Systems*, *78*, 931–932. https://doi.org/10.1016/j.future.2017.09.017

Li, S., Xu, L. Da, & Zhao, S. (2015a). The internet of things: a survey. *Information Systems Frontiers*, *17*(2), 243–259. https://doi.org/10.1007/s10796-014-9492-7

Li, S., Xu, L. Da, & Zhao, S. (2015b). The internet of things: a survey. *Information Systems Frontiers*, *17*(2), 243–259. https://doi.org/10.1007/s10796-014-9492-7

Li, X., Liu, H., Wei, F., Ma, J., & Yang, W. (2015). A lightweight anonymous authentication protocol using k-pseudonym set in wireless networks. *2015 IEEE Global Communications Conference, GLOBECOM 2015*. https://doi.org/10.1109/GLOCOM.2014.7417584

Li, Y., Wang, Y., Cheng, Y., Li, X., & Xing, G. (2015). QiLoc: A Qi wireless charging based system for robust user-initiated indoor location services. *2015 12th Annual IEEE International Conference on Sensing, Communication, and Networking, SECON 2015*, 480–488. https://doi.org/10.1109/SAHCN.2015.7338349

Lin, S. C., & Wen, C. Y. (2016). Energy-efficient device-based node authentication protocol for the Internet of Things. *2016 IEEE International Conference on Consumer Electronics-Taiwan, ICCE-TW 2016*, (1), 1–2. https://doi.org/10.1109/ICCE-TW.2016.7520962

Lin, Y. W., Lin, Y. B., Hsiao, C. Y., & Wang, Y. Y. (2017). IoTtalk-RC: Sensors As Universal Remote Control for Aftermarket Home Appliances. *IEEE Internet of Things Journal*, *4*(4), 1104–1112. https://doi.org/10.1109/JIOT.2017.2715859

Ling, Z., Luo, J., Xu, Y., Gao, C., Wu, K., & Fu, X. (2017). Security Vulnerabilities of Internet of Things: A Case Study of the Smart Plug System. *IEEE Internet of Things Journal*, *4662*(c), 1–1. https://doi.org/10.1109/JIOT.2017.2707465

Liu, Y., Hu, S., Member, S., Huang, H., Member, S., Ranjan, R., … Member, S. (2017). Game -Theoretic Market-Driven Smart Home Sceduling Considering Energy Balancing. *IEEE Systems Journal*, *11*(2), 910–921.

Liu, Y., Liu, L., Zhou, Y., & Hu, S. (2016). Leveraging carbon nanotube technologies in developing Physically Unclonable Function for cyber-physical system authentication. *Proceedings - IEEE INFOCOM*, *2016–Septe*, 176–180. https://doi.org/10.1109/INFCOMW.2016.7562067

Macal, C. M., & North, M. J. (2008). Agent-based modeling and simulation: ABMS examples. *Proceedings - Winter Simulation Conference*, 101–112. https://doi.org/10.1109/WSC.2008.4736060

Mahalle, P. (2013). Identity Authentication and Capability Based Access Control (IACAC) for the Internet of Things. *Journal of Cyber …*, *1*, 309–348. Retrieved from http://forskningsbasen.deff.dk/Share.external?sp=S72df67ac-3ea5-41da-8cf0-523c6f71bbf2&sp=Saau

Majeed, A. (2017). Internet of Things (IoT): A verification framework. *2017 IEEE 7th Annual Computing and Communication Workshop and Conference, CCWC 2017*, 2–4. https://doi.org/10.1109/CCWC.2017.7868461

Mandyam, G. D. (2017). Tiered Attestation for Internet-of-Things (IoT) Devices. In *2017 9th International Conference on Communication Systems and Networks (COMSNETS)* (pp. 480–483).

Mannion, P. (2015). Optimal Analysis Algorithms are IoT's Big Opportunity | Electronics360. *Electronics 360*. Retrieved from http://electronics360.globalspec.com/article/4890/optimal-analysis-algorithms-are-iot-s-big-opportunity

Mano, L. Y., Faiçal, B. S., Nakamura, L. H. V., Gomes, P. H., Libralon, G. L., Meneguete, R. I., … Ueyama, J. (2016). Exploiting IoT technologies for enhancing Health Smart Homes through patient identification and emotion recognition. *Computer Communications*, *89–90*, 178–190. https://doi.org/10.1016/j.comcom.2016.03.010

Maple, C. (2017). Security and privacy in the internet of things. *Journal of Cyber Policy*, *2*(2), 155–184. https://doi.org/10.1080/23738871.2017.1366536

March, S. T., & Storey, V. C. (2016). Design Science in the Information Systems Discipline: An Introduction to the Special Issue on Design Science Research. *MIS Quarterly*, *32*(4), 725–730. Retrieved from url: http://www.jstor.org/stable/25148869

Margulies, J. (2015). Garage Door Openers: An Internet of Things Case Study. *IEEE Security & Privacy*, *13*(4), 80–83. https://doi.org/10.1109/MSP.2015.80

Martina, J. E., dos Santos, E., Carlos, M. C., Price, G., & Custódio, R. F. (2015). An adaptive threat model for security ceremonies. *International Journal of Information Security*. https://doi.org/10.1007/s10207-014-0253-x

Mbarek, B., Meddeb, A., Ben Jaballah, W., & Mosbah, M. (2017). A broadcast authentication scheme in IoT environments. *Proceedings of IEEE/ACS International Conference on Computer Systems and Applications, AICCSA*. https://doi.org/10.1109/AICCSA.2016.7945807

Meana-Llorián, D., González García, C., Pelayo G-Bustelo, B. C., Cueva Lovelle, J. M., & Garcia-Fernandez, N. (2017). IoFClime: The fuzzy logic and the Internet of Things to control indoor temperature regarding the outdoor ambient conditions. *Future Generation Computer Systems*, *76*, 275–284. https://doi.org/10.1016/j.future.2016.11.020

Mohsin, M., Sardar, M. U., Hasan, O., & Anwar, Z. (2017). IoTRiskAnalyzer: A Probabilistic Model Checking Based Framework for Formal Risk Analytics of the Internet of Things. *IEEE Access*, *5*, 5494–5505. https://doi.org/10.1109/ACCESS.2017.2696031

Mokhtari, G., Zhang, Q., Hargrave, C., & Ralston, J. C. (2017). Non-Wearable UWB Sensor for Human Identification in Smart Home. *IEEE Sensors Journal*, *17*(11), 3332–3340. https://doi.org/10.1109/JSEN.2017.2694555

Mokhtari, G., Zhang, Q., Nourbakhsh, G., Ball, S., & Karunanithi, M. (2017). BLUESOUND: A New Resident Identification Sensor - Using Ultrasound Array and BLE Technology for Smart Home Platform. *IEEE Sensors Journal*, *17*(5), 1503–1512. https://doi.org/10.1109/JSEN.2017.2647960

Morsalin, S., Islam, A. M. J., Rahat, G. R., Pidim, S. R. H., Rahman, A., & Siddiqe, M. A. B. (2017). Machine-to-machine communication based smart home security system by NFC, fingerprint, and PIR sensor with mobile android application. *2016 3rd International Conference on Electrical Engineering and Information and Communication Technology, ICEEiCT 2016*. https://doi.org/10.1109/CEEICT.2016.7873048

Moskvitch, K. (2017). Securing IOT: In your smart home and your connected enterprise. *Engineering and Technology*, *12*(3), 40–42. https://doi.org/10.1159/000113927

Nguyen, H. V., & Iacono, L. Lo. (2016). REST-ful CoAP Message Authentication. *Proceedings - 2015 International Workshop on Secure Internet of Things, SIoT 2015*, 35–43. https://doi.org/10.1109/SIOT.2015.8

Nissar, N., Naja, N., & Jamali, A. (2017). Lightweight authentication-based scheme for AODV in ad-hoc networks. In *2017 International Conference on Wireless Technologies, Embedded and Intelligent Systems, WITS 2017*. https://doi.org/10.1109/WITS.2017.7934616

Offermann, P., Levina, O., Schonherr, M., & Bub, U. (2009). Outline of a Design Science Research Process. *Proceedings of the 4th International Conference on Design Science Research in Information Systems and Technology*, *May*, 1–11. https://doi.org/10.1145/1555619.1555629

Orpwood, R. (2012). Smart Homes. *Pathy's Principles and Practice of Geriatric Medicine: Fifth Edition*. John Wiley & Sons, Ltd. https://doi.org/10.1002/9781119952930.ch124

Oyegoke, A. (2011). The constructive research approach in project management research. *International Journal of Managing Projects in Business*, *4*(4), 573–595. https://doi.org/10.1108/17538371111164029

Paek, J. (2015). Fast and Adaptive Mesh Access Control in Low-Power and Lossy Networks. *IEEE Internet of Things Journal*, *2*(5), 435–444. https://doi.org/10.1109/JIOT.2015.2457940

Parikshit N.Mahalle, Bayu Anggorojati, N. R. P. and R. P. (2013). Identity Authentication and Capability Based Access Control (IACAC) for the Internet of Things. *Journal of Cyber …*, *1*, 309–348. Retrieved from http://forskningsbasen.deff.dk/Share.external?sp=S72df67ac-3ea5-41da-8cf0-523c6f71bbf2&sp=Saau

Park, H., Hwang, S., Won, M., & Park, T. (2016). Activity-aware Sensor Cycling for Human Activity Monitoring in Smart Homes. *IEEE Communications Letters*, *7798*(c), 1–1. https://doi.org/10.1109/LCOMM.2016.2619700

Patel, S., Patel, D. R., & Navik, A. P. (2016). Energy efficient integrated authentication and access control mechanisms for Internet of Things. *2016 International Conference on Internet of Things and Applications, IOTA 2016*, 304–309. https://doi.org/10.1109/IOTA.2016.7562742

Pienaar, J. P., Fisher, R. M., & Hancke, G. P. (2015). Smartphone: The key to your connected smart home. *Proceeding - 2015 IEEE International Conference on Industrial Informatics, INDIN 2015*, 999–1004. https://doi.org/10.1109/INDIN.2015.7281871

Pöpper, C., Tippenhauer, N. O., Danev, B., & Capkun, S. (2011). Investigation of signal and message manipulations on the wireless channel. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. https://doi.org/10.1007/978-3-642-23822-2_3

Premnath, S. N., & Haas, Z. J. (2015). Security and privacy in the internet-of-things under time-and-budget-limited adversary model. *IEEE Wireless Communications Letters*, *4*(3), 277–280. https://doi.org/10.1109/LWC.2015.2408609

Rahman, M., Sampangi, R. V., & Sampalli, S. (2015). Lightweight protocol for anonymity and mutual authentication in RFID systems. *2015 12th Annual IEEE Consumer Communications and Networking Conference, CCNC 2015*, 910–915. https://doi.org/10.1109/CCNC.2015.7158097

Rawashdeh, M., Al Zamil, M. G. H., Samarah, S., Hossain, M. S., & Muhammad, G. (2017). A knowledge-driven approach for activity recognition in smart homes based on activity profiling. *Future Generation Computer Systems*. https://doi.org/10.1016/j.future.2017.10.031

Ray, B., Chowdhury, M. U., & Abawajy, J. (2017). A Multi-Protocol Security Framework to Support Internet of Things, *198*(June). https://doi.org/10.1007/978-3-319-59608-2

Ray, B. R., Chowdhury, M. U., & Abawajy, J. H. (2016). Secure Object Tracking Protocol for the Internet of Things. *IEEE Internet of Things Journal*, *3*(4), 544–553. https://doi.org/10.1109/JIOT.2016.2572729

Ray, B. R. R., Abawajy, J., Chowdhury, M., & Alelaiwi, A. (2018). Universal and secure object ownership transfer protocol for the Internet of Things. *Future Generation Computer Systems*, *78*(February), 838–849. https://doi.org/10.1016/j.future.2017.02.020

Ren, H., Song, Y., Yang, S., & Situ, F. (2016). Secure smart home: A voiceprint and internet based authentication system for remote accessing. *ICCSE 2016 - 11th International Conference on Computer Science and Education*, (Iccse), 247–251. https://doi.org/10.1109/ICCSE.2016.7581588

Rigney, C., Willens, S., Rubens, A., & Simpson, W. (2013). RFC 2687 - Remote Authentication Dial In User Service (RADIUS). *Journal of Chemical Information and Modeling*, *53*(9), 1689–1699. https://doi.org/10.1017/CBO9781107415324.004

Rizzardi, A., Sicari, S., Miorandi, D., & Coen-Porisini, A. (2016). AUPS: An Open Source AUthenticated Publish/Subscribe system for the Internet of Things. *Information Systems*, *62*, 29–41. https://doi.org/10.1016/j.is.2016.05.004

Roy, S., Chatterjee, S., Das, A. K., Chattopadhyay, S., Kumari, S., & Jo, M. (2017). Chaotic Map-based Anonymous User Authentication Scheme with User Biometrics and Fuzzy Extractor for Crowdsourcing Internet of Things. *IEEE Internet of Things Journal*, *4662*(c), 1–1. https://doi.org/10.1109/JIOT.2017.2714179

Rwegasira, D., Kondoro, A., Kelati, A., Dhaou, I. B. E. N., Mvungi, N., & Tenhunen, H. (2018). CDE for ICT Innovation Through the IoT Based iGrid Project in Tanzania. In Paul Cunningham and Miriam Cunningham (Eds) (Ed.), *IST-Africa 2018 Conference Proceedings* (pp. 1–9). IIMC International Information Management Corporation.

Saadeh, M., Sleit, A., Qatawneh, M., & Almobaideen, W. (2016). Authentication techniques for the internet of things: A survey. *Proceedings - 2016 Cybersecurity and Cyberforensics Conference, CCC 2016*, 28–34. https://doi.org/10.1109/CCC.2016.22

Saied, Y. Ben, Olivereau, A., Zeghlache, D., & Laurent, M. (2014). Lightweight collaborative key establishment scheme for the Internet of Things. *Computer Networks*, *64*, 273–295. https://doi.org/10.1016/j.comnet.2014.02.001

Savola, R., Abie, H., & Sihvonen, M. (2012). Towards Metrics-Driven Adaptive Security Management in E-Health IoT Applications. *Proceedings of the 7th International Conference on Body Area Networks*, *250241*(SeTTIT), 276–281. https://doi.org/10.4108/icst.bodynets.2012.250241

Saxena, N., Choi, B. J., & Cho, S. (2015). Lightweight privacy-preserving authentication scheme for V2G networks in the smart grid. *Proceedings - 14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2015*, *1*, 604–611. https://doi.org/10.1109/Trustcom.2015.425

Saxena, N., Choi, B. J., & Lu, R. (2016). Authentication and Authorization Scheme for Various User Roles and Devices in Smart Grid. *IEEE Transactions on Information Forensics and Security*, *11*(5), 907–921. https://doi.org/10.1109/TIFS.2015.2512525

Schaumont, P., Moriyama, D., Gulcan, E., & Aysu, A. (2016). Compact and low-power ASIP design for lightweight PUF-based authentication protocols. *IET Information Security*, *10*(5), 232–241. https://doi.org/10.1049/iet-ifs.2015.0401

SDGs. (2017). The Sustainable Development Goals Report, The Unitd Nations. *United Nations*, 1–56. https://doi.org/10.18356/3405d09f-en

Seo, D. W., Kim, H., Kim, J. S., & Lee, J. Y. (2016). Hybrid reality-based user experience and evaluation of a context-aware smart home. *Computers in Industry*, *76*, 11–23. https://doi.org/10.1016/j.compind.2015.11.003

Shahzad, M., Singh, M. P., & Carolina, N. (2017). Continuos Authentication and Authorization for the Internet of Things. *IEEE Internet Computing*, *21*(2), 86–90. https://doi.org/10.1109/MIC.2017.33

Shaju, S., & Panchami, V. (2016). BISC Authentication Algorithm : An Efficient New Authentication Algorithm Using Three Factor Authentication for Mobile Banking. In *2016 Online International Conference on Green Engineering and Technologies (IC-GET) BISC*.

Sharaf-Dabbagh, Y., & Saad, W. (2016). On the authentication of devices in the Internet of things. *WoWMoM 2016 - 17th International Symposium on a World of Wireless, Mobile and Multimedia Networks*, 1–3. https://doi.org/10.1109/WoWMoM.2016.7523532

Sharma, P., Khanna, R. R., & Bhatnagar, V. (2017). Application of TRIZ framework for resolving security issues in IOT. In *Proceeding - IEEE International Conference on Computing, Communication and Automation, ICCCA 2016*. https://doi.org/10.1109/CCAA.2016.7813921

Shen, C., Li, H., Sahin, G., & Choi, H. A. (2016). Low-complexity Scalable Authentication algorithm with Imperfect Shared Keys for Internet of Things. *2016 IEEE International Conference on Communications Workshops, ICC 2016*, 116–121. https://doi.org/10.1109/ICCW.2016.7503774

Shen, J., Liu, D., Chang, S., Shen, J., & He, D. (2016). A Lightweight Mutual Authentication Scheme for User and Server in Cloud. *Proceedings - 2015 1st International Conference on Computational Intelligence Theory, Systems and Applications, CCITSA 2015*, 183–186. https://doi.org/10.1109/CCITSA.2015.47

Shen, J., Tan, H., Chang, S., Ren, Y., & Liu, Q. (2015). A lightweight and practical RFID grouping authentication protocol in multiple-tag arrangements. *International Conference on Advanced Communication Technology, ICACT*, *2015–Augus*, 681–686. https://doi.org/10.1109/ICACT.2015.7224882

Shen, T., & Maode, M. (2016). Security Enhancements on Home Area Networks in Smart Grids. In *IEEE Region 10 Conference (TENCON)* (pp. 2444–2447).

Shin, D., Sharma, V., Kim, J., Kwon, S., & You, I. (2017). Secure and Efficient Protocol for Route Optimization in PMIPv6-based Smart Home IoT Networks. *IEEE Access*, *3536*(c). https://doi.org/10.1109/ACCESS.2017.2710379

Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks*, *76*, 146–164. https://doi.org/10.1016/j.comnet.2014.11.008

Silverajan, B., Luoma, J. P., Vajaranta, M., & Itapuro, R. (2015). Collaborative cloud-based management of home networks. *Proceedings of the 2015 IFIP/IEEE International Symposium on Integrated Network Management, IM 2015*, 786–789. https://doi.org/10.1109/INM.2015.7140376

Sivanathan, A., Sherratt, D., Gharakheili, H. H., Sivaraman, V., & Vishwanath, A. (2017). Low-cost flow-based security solutions for smart-home IoT devices. *2016 IEEE International Conference on Advanced Networks and Telecommunications Systems, ANTS 2016*. https://doi.org/10.1109/ANTS.2016.7947781

Skocir, P., Krivic, P., Tomeljak, M., Kusek, M., & Jezic, G. (2016). Activity Detection in Smart Home Environment. *Procedia Computer Science*, *96*, 672–681. https://doi.org/10.1016/j.procs.2016.08.249

Smirek, L., Zimmermann, G., & Beigl, M. (2016). Just a Smart Home or Your Smart Home - A Framework for Personalized User Interfaces Based on Eclipse Smart Home and Universal Remote Console. *Procedia Computer Science*, *58*(Euspn), 107–116. https://doi.org/10.1016/j.procs.2016.09.018

Song, T., Li, R., Mei, B., Yu, J., Xing, X., & Cheng, X. (2017). A Privacy Preserving Communication Protocol for IoT Applications in Smart Homes. *IEEE Internet of Things Journal*, *4662*(c), 1–1. https://doi.org/10.1109/JIOT.2017.2707489

Stephanie. (2017). Snowball Sampling: Definition, Advantages and Disadvantages. Retrieved January 15, 2018, from http://www.statisticshowto.com/snowball-sampling/

Tankard, C. (2015). The security issues of the Internet of Things. *Computer Fraud & Security*, *2015*(9), 11–14. https://doi.org/10.1016/S1361-3723(15)30084-1

Tao, M., Zuo, J., Liu, Z., Castiglione, A., & Palmieri, F. (2018). Multi-layer cloud architectural model and ontology-based security service framework for IoT-based smart homes. *Future Generation Computer Systems*, *78*, 1040–1051. https://doi.org/10.1016/j.future.2016.11.011

Tobin, G. A., & Begley, C. M. (2004). Methodological Rigour within a Qualittaive Framework. *Journal of Advanced Nursing*, *48*(4), 388–396. https://doi.org/10.1111/j.1365-2648.2004.03207.x

Tran, A. C., Marsland, S., Dietrich, J., Guesgen, H. W., & Lyons, P. (2010). Use cases for abnormal behaviour detection in smart homes. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* (Vol. 6159 LNCS, pp. 144–151). https://doi.org/10.1007/978-3-642-13778-5_18

Vermesan, O., Friess, P., Guillemin, P., Gusmeroli, S., Sundmaeker, H., Bassi, A., … Doody, P. (2016). Internet of Things Strategic Research Roadmap 2.1 Internet of Things Conceptual Framework 2.2 Internet of Things Vision. In *In Proceedings of 2016 International Conference on ICT in Business, Industry, and Government, ICTBIG 2016* (pp. 1–44). Institute of Electrical and Electronics Engineers Inc.

https://doi.org/https://doi.org/10.1109/ICTBIG.2016.7892668

Wang, F., Xu, Y., Zhang, H., Zhang, Y., & Zhu, L. (2016). 2FLIP: A two-factor lightweight privacy-preserving authentication scheme for VANET. *IEEE Transactions on Vehicular Technology*, *65*(2), 896–911. https://doi.org/10.1109/TVT.2015.2402166

Weber, R. (2010). Internet of Things - New security and privacy challenges. *Computer Law & Security Review*. https://doi.org/10.1016/j.clsr.2009.11.008

Winter, R. (2008). Design science research in Europe. *European Journal of Information Systems*, *17*(5), 470–475. https://doi.org/10.1057/ejis.2008.44

Witkovski, A., Santin, A., Abreu, V., & Marynowski, J. (2015). An IdM and key-based authentication method for providing single sign-on in IoT. *2015 IEEE Global Communications Conference, GLOBECOM 2015*, (IdM). https://doi.org/10.1109/GLOCOM.2014.7417597

Wu, Q. X., & Li, H. (2013). Secure solution of trusted Internet of things base on TCM. *Journal of China Universities of Posts and Telecommunications*, *20*(SUPPL-2), 47–53. https://doi.org/10.1016/S1005-8885(13)60222-8

Yang, J. H., & Lin, P. Y. (2014). An ID-Based User Authentication Scheme for Cloud Computing. *2014 Tenth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*. https://doi.org/10.1109/IIH-MSP.2014.31

Yang, M. L., Narayanan, A., Parry, D., & Wang, X. (2016). A lightweight authentication scheme for transport system farecards. *2016 IEEE International Conference on RFID Technology and Applications, RFID-TA 2016*, 150–155. https://doi.org/10.1109/RFID-TA.2016.7750746

Yang, Y., Sun, J., & Guo, L. (2016). PersonalA: A Lightweight Implicit Authentication System based on Customized User Behavior Selection. *IEEE Transactions on Dependable and Secure Computing*, *5971*(c), 1–1. https://doi.org/10.1109/TDSC.2016.2645208

Yao, X., Chen, Z., & Tian, Y. (2014). A lightweight attribute-based encryption scheme for the Internet of Things. *Future Generation Computer Systems*, *49*, 104–112. https://doi.org/10.1016/j.future.2014.10.010

Yaqoob, I., Ahmed, E., Rehman, M. H. ur, Ahmed, A. I. A., Al-garadi, M. A., Imran, M., & Guizani, M. (2017). The rise of ransomware and emerging security challenges in the Internet of Things. *Computer Networks*, *129*, 444–458. https://doi.org/10.1016/j.comnet.2017.09.003

Yoon, E.-J., Das, A. K., Yoo, K.-Y., & Goutham Reddy, A. (2016). Lightweight authentication with key-agreement protocol for mobile network environment using smart cards. *IET Information Security*, *10*(5), 272–282. https://doi.org/10.1049/iet-ifs.2015.0390

Yu, M.-D. M., Hiller, M., Delvaux, J., Sowell, R., Devadas, S., & Verbauwhede, I. (2016). A Lockdown Technique to Prevent Machine.pdf. *IEEE Transactions on Multi-Scale Computing Systems*, *2*(3), 146–159. https://doi.org/10.1109/TMSCS.2016.2553027

Zhang, D., Yang, L. T., Chen, M., Zhao, S., Guo, M., & Zhang, Y. (2014). Real-Time Locating Systems Using Active RFID for Internet of Things. *IEEE Systems Journal*, *10*(3), 1–10. https://doi.org/10.1109/JSYST.2014.2346625

Zhang, N., Wu, X., Yang, C., Shen, Y., & Cheng, Y. (2017). A lightweight authentication and authorization solution based on Kerberos. *Proceedings of 2016 IEEE Advanced Information Management, Communicates, Electronic and Automation Control Conference, IMCEC 2016*, 742–746. https://doi.org/10.1109/IMCEC.2016.7867308

Zhang, R. (2017). An enhanced lightweight authentication protocol for low-cost RFID systems. *Proceedings of 2016 IEEE International Conference on Electronic Information and Communication Technology, ICEICT 2016*, (Iceict), 29–33. https://doi.org/10.1109/ICEICT.2016.7879646

Zhang, Y., Xiang, Y., Huang, X., Chen, X., & Alelaiwi, A. (2018). A matrix-based cross-layer key establishment protocol for smart homes. *Information Sciences*, *429*, 390–405. https://doi.org/10.1016/j.ins.2017.11.039

Zhao, K., & Ge, L. (2013). A survey on the internet of things security. In *Proceedings - 9th International Conference on Computational Intelligence and Security, CIS 2013* (pp. 663–667). https://doi.org/10.1109/CIS.2013.145

Zhong, H., Shao, L., & Cui, J. (2016). A Lightweight and Secure Data Authentication Scheme with Privacy Preservation for Wireless Sensor Networks. *2016 International Conference on Networking and Network Applications (NaNA)*, 210–217. https://doi.org/10.1109/NaNA.2016.85

Zhu, Q., Uddin, M. Y. S., Qin, Z., & Venkatasubramanian, N. (2017). Data collection and upload under dynamicity in smart community Internet-of-Things deployments. *Pervasive and Mobile Computing*, *42*, 166–186. https://doi.org/10.1016/j.pmcj.2017.10.003

Appendix 4: Publication 4

Security and Privacy Preservation Authentication Schemes for IoT: Relationship proposition.

Attlee M. Gamundani
Namibia University of Science and Technology
Faculty of Computing & Informatics
Computer Science Department
Windhoek, Namibia
e-mail: agamundani@nust.na

Amelia Phillips
Highline College
CIS and Computer Science
Departments Cyber Security and Forensics BAS lead
Seattle , USA.
e-mail: aphillips@highline.edu

Hippolyte N. MUYINGI
Namibia University of Science and Technology
Faculty of Computing & Informatics
Windhoek, Namibia
e-mail: hmuyingi@nust.na

***Abstract*— IoT authentication demands a complex approach to ensure all facets of security are taken care of. Security in IoT is not complete without looking at privacy protection. Privacy of user credentials is critically important as that holds pieces of data that can compromise the whole security system. The need to emphasize on privacy preserving for authentication is on the basis that, we need to complete the security puzzle unequivocally. One of the security worries in IoT is user data privacy as a result of the unsupervised nature of IoT device's interaction. Focusing on Smart Home environments and personal area networks to a large extent, this paper gives an overview on some of the existing solutions that employs privacy preserving attributes towards providing IoT authentication security solutions in the quest to try and provide the relationship between privacy and security.**

***Keywords*—** Authentication, Data, Internet of Things, Privacy & Security.

I. INTRODUCTION

IoT Security boarders around many aspects, most of the aspects are far from being solved, as this is an evolving discipline. Privacy preservation is among the key issues that are topical in the circles of IoT security. Among the irregularities to be addressed to attain privacy preservation during authentication process is the notion of security by obscurity. How can we ensure we are authenticating with the authentic devices in the IoT platform if their identity is concealed? How do we troubleshoot any authentication problem that goes wrong if the players to the process are anonymous? These may be some of the questions that can be presented for consideration when tabling the privacy preservation requirement as a key input towards IoT authentication.

As said by(Gamundani, 2015), Maintaining privacy at the expense of other security variables demands more than just looking at the *why?* But also the *how*? Beyond that, there is need to consider the subsequent consequences of elevating the privacy index versus other security indexes which must be almost at par with privacy. For example if we consider such security variables as integrity, availability and non-repudiation. Of course, there is a close relationship between privacy and many of the security variables. For instance, we can't ensure integrity without being concerned about the privacy of the data we are protecting.

This paper is presented with the main focus on giving an assumed relationship between privacy and security. We are motivated by the hypothesis that, there is no clear-cut relationship between security and privacy

II. Why Privacy?

A Smart Home setup presents an environment that calls for privacy especially to user's information such as their banking credentials or even their personal data as any compromise on such data has serious repercussions. To support this reasoning on the need for privacy, (Song et al., 2017) emphasis on the need to protect Smart Homes as any piece of information gathered from the Smart Home setup can be used by intruders to profile users. Hence can eventually be used to steal their personal details, which can be linked for example to their credit card details and the list goes on.

Among the security threats that IoT devices suffer from, privacy is one of them. As supported by (Abdallah & Shen, 2017), when they looked at authentication of electrical vehicles in smart grids. Once the privacy of the object is effectively protected, such threats as physical attacks on the objects is minimized if not eliminated. This implies context-ware authentication schemes such as the framework proposed by (Ashibani et al., 2017) becomes a threat towards privacy preservation, despite their functional objective of providing security to IoT devices.

The fact that IoT devices senses and transmit sensitive data based on their deployed environments, demands that the security solutions designed for such devices maintain the privacy of the communication interactions of such devices to ensure the data and the interactions are protected. As presented by (Batool et al., 2017) IoT devices generates enormous quantities of data, the need to ensure that every activity around that data is tightly protected, is a direct call for security that advances privacy preservation.

The extended visibility of IoT around people calls for privacy, as clearly outlined by (Shahzad, Singh, & Carolina, 2017) that computing has been brought to our bodies and our daily surroundings as a result of it's pervasive and ubiquitous nature. As further supported by (Patel, Patel, & Navik, 2016) the heterogeneous nature of IoT presents concerns for security as such privacy need to be considered during the design phase of IoT.

Clearly privacy is needed as it makes security solutions complete. Without privacy consideration, the other window to security threats is as good as left open without any due consideration.

A. Privacy and Security Requirements

It will be ideal to consider privacy and security requirements when advancing privacy preserving security solutions as they can open doors to anonymous attacks. The other reason will be to ensure that, no complication to the overall system layout is made such that troubleshooting becomes easier. The source of the problem should not be concealed, in a bid to preserve privacy. As such privacy should be considered as an enhancement to security not a hindrance of security.

It is noted in (Ghosh & Mahesh, 2016) that privacy leakage could pause a serious challenge during the authentication process, as they looked at Radio Frequency Identification (RFID) tags. Henceforth, an overlook on the privacy component for IoT security is a recipe for ill-structured solutions unless the application domains do not require such considerations, which may be rare.

B. Existing Privacy Preservation Schemes

Anonymous authentication is seemingly a precursor to privacy preservation in some of the authentication schemes being advanced in wireless sensor networks as supported by (X. Li et al., 2015). One of the major worries highlighted on some of these solutions is their reliance on asymmetric keys, which makes them heavy and unsuitable for resource constrained IoT environments (X. Li et al., 2015). Being able to separate the real identity of the authenticating parties is one of the key approach that is being proposed by (X. Li et al., 2015), at the same time achieving efficiency of the authentication process. Henceforth, the scheme presented by (Song et al., 2017) uses a chaotic system that employs symmetric encryption and secret keys as well as message authentication codes to protect data transmissions inside the Smart Home. Also in (Roy et al., 2017) chaotic systems are combined with smart cards, biometrics and passwords offering a three-factor user authentication for an e-healthcare setup.

In similar work presented by (Janbabaei et al., 2017), anonymity is also being emphasized which equally speaks to the need for privacy during the authentication process as highlighted in (Roy et al., 2017). To further highlight the need for privacy an underscore on untraceability is done by (Janbabaei et al., 2017). The use of pseudonyms is common on schemes that endeavour to offer privacy preserving schemes for authentication as witnessed in the work of (Abdallah & Shen, 2017). It clearly points to the fact that, real identities need to be protected to realize the privacy protection requirement.

In some of the solutions that attempt to realize the privacy protection in authentication, advancement of a layered approach is implemented as can be witnessed in the approach proposed by (Mandyam, 2017). The argument for not recommending this approach in some scenarios could be on the basis of computation latencies, which may be costly as compared to consequences likely to be incurred for not having valued the privacy component for authentication enough.

Another trend observed from literature is the use of group signatures instead of individual signatures for authenticating IoT devices. The approach proposed by (Kishimoto, Yanai, & Okamura, 2017) promotes the use of group signatures for anonymous authentication for smart grids with the proposition to use tokens to link the group signatures. Almost similar to group signatures is what (Gu & Liu, 2017) advanced, which is the use of group audio based authentication aimed at providing privacy of user data in IoT devices and networks. Furthermore, (J. Shen, Tan, Chang, Ren, & Liu, 2015) proposed a multiple-tag approach to authentication, where a single object to be authenticated is attached to a group of RFID tags. A further improvement to the group dynamic approach is introduced by (Cheng et al., 2015) where they introduced two new parameters to Tan's work on RFID tag authentication, which are brand secret and series secret, which managed to prevent loss of basic privacy and other security benefits envisaged thereof.

Salted hash functions are among the techniques employed for privacy preservation, as evident in the work of (Ghosh & Mahesh, 2016), where they proposed an authentication protocol for use by RFID tags. To maintain the privacy, the tag receives random responses, which do not disclose the identity information as they are being sent from the protocol. The key here was to disguise the target recipients of the send responses from the protocol, as it was not obvious which of the randomized responses are targeted at what requests.

The work of (Zhong, Shao, & Cui, 2016), presents an authentication scheme that avails privacy preservation, through the use encryption schemes, message authentication code and pseudonym technology. The approach was used for wireless sensor networks, which are highly vulnerable yet they collect large amounts of data, which may be used by adversaries to profile their targets.

C. Privacy Preserving Security Challenges

Maintaining privacy at the same time having the goal of achieving a watertight security solution are two competing paradigms that may be difficult to balance yet are equally important. There are scenarios where authenticating parties have to be validated henceforth violating the privacy preservation call, especially considering where anonymity is being proposed for security solutions.

Common among the privacy preservation schemes is the extension of the already existing security attributes to incorporate the privacy component. Three factor-authentication solutions are evidence of privacy preserving authentication aware schemes. Anonymity is among the key attributes also noted for privacy preserving schemes. All these attributes may present challenges towards designing efficient and effective security solutions as IoT devices are resource constrained by nature.

D. Privacy Preservation in the Smart Home Context

Given the Smart Home context, it will be ideal to map the security solutions advanced at any level of the IoT architecture for Smart Home security design. We envisage a complete security as one that incorporates privacy to all the security levels as depicted in Figure 2. Missing the privacy component in the security design for Smart Home security solutions entails an inadequate solution package.

The idea of presenting privacy as the middle piece of the puzzle is to depict the essence of it as a vital ingredient in the whole security recipe. Henceforth, whatever security solutions are designed for the application layer in order for them to be well balanced they need to incorporate the privacy preservation component. The same applies to security solutions at the network layer and at the perception layer.

IoT devices being constrained on storage capacity may not be storing the data on-board that they will be collecting but have to rely on third party setups like cloud computing or a backend server. The interaction that has to take place between these devices and the respective repositories of data needs to be secured as well as being privacy protected. Considering this scenario, we already experience all the three levels of security invoked.

The same window in a Smart Home used for giving access to view beautiful scenery from the inside can be an intruder's door into the very house. This is how visually security and privacy inter-relate. Securing the window entails mounting bulgur bars but privacy entails tinting the window and applying curtains. This hypothetical representation explains what privacy preservation means in relation to security.

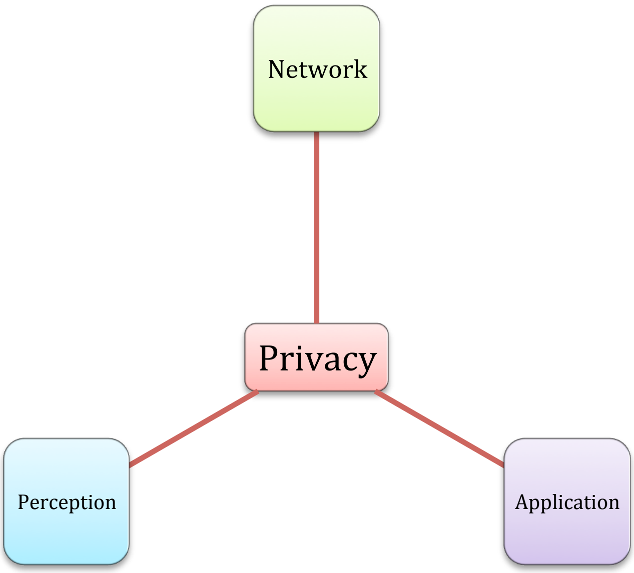


Figure 1. Smart IoT Security Design

Privacy in the Smart Home context has to be holistic as any device interaction in a Smart Home has access to personal data that needs protection at any level of the security architecture designed for the Smart Home setup.

E. Way forward on Privacy Preservation

Privacy preservation needs to be considered in light of the security protocols being advanced. Functionally the proposed privacy preservation techniques should not make the security solution heavy in terms of IoT resource requirements. There is need to balance the computational cost and the processing demands of the privacy preservation solutions being merged with the applied security solution.

Logically privacy should not be an after thought when designing security solutions for IoT devices or deployment in IoT environments.

III. Our proposed relationship

The heterogeneous and dynamic nature of IoT presents a wide range of security threats and privacy issues as argued by (Challa et al., 2017). This points to an interesting trend noticeable in literature that privacy is treated as a separate component of security. As would be noticed in the work of (Premnath & Haas, 2015), privacy cannot be separated from security. Henceforth, our proposed relationship is that privacy should be treated as an added requirement to security as there is no way one can implement a successful privacy preservation solution without a security solution. We can summarize this relationship between security and privacy as in Figure 2.

A security solution can be implemented without taking into consideration the privacy protection component for example an authentication scheme can grant access to IoT systems without protecting the user information. On the hand, a privacy preservation solution can be implemented without focusing on security features. In either of these situations, we cannot say the solutions advanced did not meet the standard requirements. It is a matter of striking a balance between the two where needed. This is why we are proposing a decision table in Figure 3 to be used effectively when considering the decisions between security and privacy.

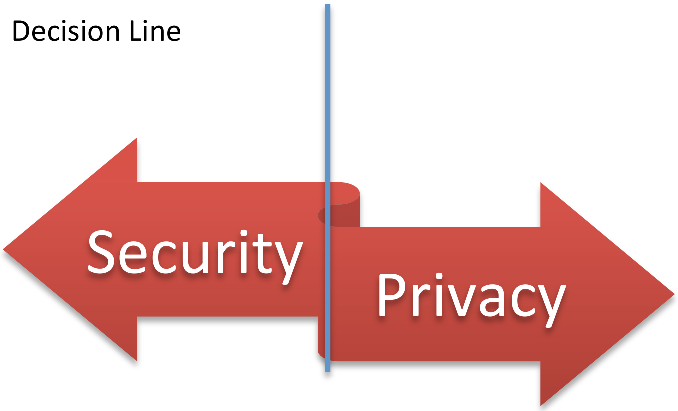


Figure 2. Privacy and Security Relationship

Our proposition is that, security is one end of the spectrum and privacy in another end of the spectrum. It is only at the decision line point that we either chose to stretch the band towards security to a certain extend or towards privacy to a defined extent. For a holistic approach where feasible, consideration can be made to stretch the bank both ends to render end-to-end, privacy preservation and secure solutions.

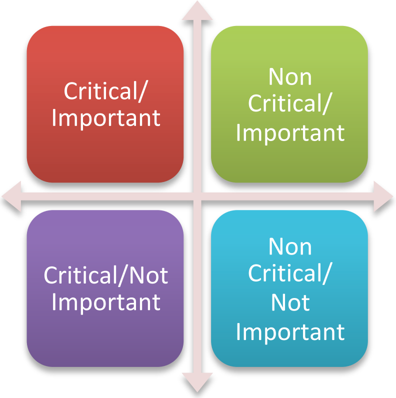


Figure 3. Decision line between Privacy and Security

IV. Conclusion

IoT security solutions for Smart Home environments are incomplete without privacy consideration. As outlined in this paper, relationship between security and privacy for a complete security package should be inseparable hence demands equal attention. As also hinted in this paper, from the onset at design stage, privacy need to be considered for a complete package for smart devices especially those that find themselves in the Smart Home environment.

Appreciating the nature of data found in the Smart Home environment, the need for privacy couldn't be overemphasized, henceforth where technically possible every layer of the security design for IoT devices in the Smart Home should consider privacy as depicted in Figure 2.

References

Abdallah, A., & Shen, X. (2017). Lightweight Authentication and Privacy-Preserving Scheme for V2G Connections. *IEEE Transactions on Vehicular Technology*, *66*(3), 2615–2629. https://doi.org/10.1109/TVT.2016.2577018

Abdullaziz, O. I., Chen, Y. J., & Wang, L. C. (2016). Lightweight authentication mechanism for software defined network using information hiding. *2016 IEEE Global Communications Conference, GLOBECOM 2016 - Proceedings*, 0–5. https://doi.org/10.1109/GLOCOM.2016.7841954

Ahamed, J., & Rajan, A. V. (2016). Internet of Things (IoT): Application Systems and Security Vulnerabilities.

Ahmed, S. H., & Kim, D. (2016). Named data networking-based smart home. *ICT Express*, *2*(3), 130–134. https://doi.org/10.1016/j.icte.2016.08.007

Al-Ali, A. R., Zualkernan, I. A., Rashid, M., Gupta, R., & Alikarar, M. (2017). A smart home energy management system using IoT and big data analytics approach. *IEEE Transactions on Consumer Electronics*, *63*(4), 426–434. https://doi.org/10.1109/TCE.2017.015014

Alaa, M., Zaidan, A. A., Zaidan, B. B., Talal, M., & Kiah, M. L. M. (2017). A review of smart home applications based on Internet of Things. *Journal of Network and Computer Applications*, *97*(February), 48–65. https://doi.org/10.1016/j.jnca.2017.08.017

Amin, R., Islam, S. H., Biswas, G. P., Khan, M. K., Leng, L., & Kumar, N. (2016). Design of an anonymity-preserving three-factor authenticated key exchange protocol for wireless sensor networks. *Computer Networks*, *101*, 42–62. https://doi.org/10.1016/j.comnet.2016.01.006

Amiribesheli, M., Benmansour, A., & Bouchachia, A. (2015). A review of smart homes in healthcare. *Journal of Ambient Intelligence and Humanized Computing*, *6*(4), 495–517. https://doi.org/10.1007/s12652-015-0270-2

Arafin, M. T., Gao, M., & Qu, G. (2017). VOLtA: Voltage over-scaling based lightweight authentication for IoT applications. *Proceedings of the Asia and South Pacific Design Automation Conference, ASP-DAC*, 336–341. https://doi.org/10.1109/ASPDAC.2017.7858345

Arafin, M. T., & Qu, G. (2016). RRAM based lightweight user authentication. *2015 IEEE/ACM International Conference on Computer-Aided Design, ICCAD 2015*, 139–145. https://doi.org/10.1109/ICCAD.2015.7372561

Arasteh, S., Aghili, S. F., & Mala, H. (2016). A new lightweight authentication and key agreement protocol for Internet of Things. *2016 13th International Iranian Society of Cryptology Conference on Information Security and Cryptology (ISCISC)*, 52–59. https://doi.org/10.1109/ISCISC.2016.7736451

Ashibani, Y., Kauling, D., & Mahmoud, Q. H. (2017). A Context-Aware Authentication Framework for Smart Homes. In *2017 IEEE 30th Canadian Conference on Electrical and Computer Engineering (CCECE)*.

Backes, M., Cervesato, I., Jaggard, A. D., Scedrov, A., & Tsay, J. K. (2011). Cryptographically sound security proofs for basic and public-key Kerberos. *International Journal of Information Security*. https://doi.org/10.1007/s10207-011-0125-6

Baek, J., & Youm, H. Y. (2015). Secure and lightweight authentication protocol for NFC tag based services. *Proceedings - 2015 10th Asia Joint Conference on Information Security, AsiaJCIS 2015*, 63–68. https://doi.org/10.1109/AsiaJCIS.2015.35

Baker, A. (Wind R. (n.d.). Maintaining Data Integrity in Database Applications. Retrieved from http://docs.oracle.com/cd/B28359_01/appdev.111/b28424/adfns_constraints.htm#i1006359

Batool, S., Saqib, N. A., & Khan, M. A. (2017). Internet of Things Data Analytics for User Authentication and Activity Recognition. In *2017 Second International Conference on Fog and Mobile Edge Computing (FMEC)* (pp. 183–187).

Bhati, A., Hansen, M., & Chan, C. M. (2017). Energy conservation through smart homes in a smart city: A lesson for Singapore households. *Energy Policy*, *104*(February), 230–239. https://doi.org/10.1016/j.enpol.2017.01.032

Brandt, J. (2015). 50 billion connected IoT devices by 2020. Retrieved from https://www.privacyrisksadvisors.com/news/a50-billion-connected-iot-devices-by-2020-by-jaclyn-brandt/

Brenkus, J., Stopjakova, V., Zalusky, R., Mihalov, J., & Majer, L. (2015). Power-efficient smart metering plug for intelligent households. *Proceedings of 25th International Conference Radioelektronika, RADIOELEKTRONIKA 2015*, (296131), 110–113. https://doi.org/10.1109/RADIOELEK.2015.7129031

Challa, S., Wazid, M., Das, A. K., Kumar, N., Goutham Reddy, A., Yoon, E. J., & Yoo, K. Y. (2017). Secure Signature-Based Authenticated Key

Establishment Scheme for Future IoT Applications. *IEEE Access*, *5*, 3028–3043. https://doi.org/10.1109/ACCESS.2017.2676119

Chen, D., Zhang, N., Qin, Z., Mao, X., Qin, Z., Shen, X., & Li, X. Y. (2017). S2M: A Lightweight Acoustic Fingerprints-Based Wireless Device Authentication Protocol. *IEEE Internet of Things Journal*, *4*(1), 88–100. https://doi.org/10.1109/JIOT.2016.2619679

Chen, J., Ma, J., Zhong, N., Yao, Y., Liu, J., Huang, R., … Cao, J. (2014). WaaS: Wisdom as a service. *IEEE Intelligent Systems*, *29*(6), 40–47. https://doi.org/10.1109/MIS.2014.19

Chen, J., & Zhu, Q. (2017). Security as a Service for Cloud-Enabled Internet of Controlled Things under Advanced Persistent Threats: A Contract Design Approach. *IEEE Transactions on Information Forensics and Security*, *6013*(c). https://doi.org/10.1109/TIFS.2017.2718489

Chen, S., Liu, T., Gao, F., Ji, J., Xu, Z., Qian, B., … Guan, X. (2017). Butler, Not Servant: A Human-Centric Smart Home Energy Management System. *IEEE Communications Magazine*, *55*(2), 27–33. https://doi.org/10.1109/MCOM.2017.1600699CM

Cheng, L., Shenwen, L., Yingbo, L., Na, L., & Xuren, W. (2015). A secure and lightweight authentication protocol for RFID. *ICEIEC 2015 - Proceedings of 2015 IEEE 5th International Conference on Electronics Information and Emergency Communication*, (2012), 317–320. https://doi.org/10.1109/ICEIEC.2015.7284548

Cherry, C., Hopfe, C., MacGillivray, B., & Pidgeon, N. (2017). Homes as machines: Exploring expert and public imaginaries of low carbon housing futures in the United Kingdom. *Energy Research and Social Science*, *23*, 36–45. https://doi.org/10.1016/j.erss.2016.10.011

Chiang, Y. T., Lu, C. H., & Hsu, J. Y. J. (2017). A Feature-Based Knowledge Transfer Framework for Cross-Environment Activity Recognition Toward Smart Home Applications. *IEEE Transactions on Human-Machine Systems*, *47*(3), 310–322. https://doi.org/10.1109/THMS.2016.2641679

Coetzee, L., Oosthuizen, D., & Mkhize, B. (2018). An Analysis of CoAP as Transport in an Internet of Things Environment. In *www.IST-Africa.org/Conference2018* (pp. 1–7).

Cremers, C. (2014). *Scyther User Manual*. Retrieved from http://users.ox.ac.uk/~coml0529/scyther/index.html%0AUsers

Cremers, C. J. F. (2008). Unbounded verification, falsification, and characterization of security protocols by pattern refinement. *Proceedings of the 15th ACM Conference on Computer and Communications Security - CCS '08*, 119. https://doi.org/10.1145/1455770.1455787

Cremers, C. J. F., Lafourcade, P., & Nadeau, P. (2009). Comparing state spaces in automatic security protocol analysis. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *5458 LNCS*, 74–94. https://doi.org/10.1007/978-3-642-02002-5-5

Cross, N. (2007). From a Design Science to a Design Discipline: Understanding Designerly Ways of Knowing and Thinking. *Design Research Now*, (1923), 41–54. https://doi.org/10.1007/978-3-7643-8472-2_3

Crossman, M. A., & Liu, H. (2016). Two-factor authentication through near field communication. In *2016 IEEE Symposium on Technologies for Homeland Security, HST 2016*. https://doi.org/10.1109/THS.2016.7568941

Daramas, A., Pattarakitsophon, S., Eiumtrakul, K., Tantidham, T., & Tamkittikhun, N. (2016). HIVE: Home Automation System for Intrusion Detection. *Proceedings of the 2016 5th ICT International Student Project Conference, ICT-ISPC 2016*, 101–104. https://doi.org/10.1109/ICT-ISPC.2016.7519246

Denning, T., Kohno, T., & Levy, H. M. (2013). Computer security and the modern home. *Communications of the ACM*, *56*(1), 94. https://doi.org/10.1145/2398356.2398377

Dolev, D., & Yao, a. (1983). On the security of public key protocols. *IEEE Transactions on Information Theory*, *29*(2), 198–208. https://doi.org/10.1109/TIT.1983.1056650

Fabi, V., Spigliantini, G., & Corgnati, S. P. (2017). Insights on Smart Home Concept and Occupants' Interaction with Building Controls. *Energy Procedia*, *111*(September 2016), 759–769. https://doi.org/10.1016/j.egypro.2017.03.238

Fan, X., Qiu, B., Liu, Y., Zhu, H., & Han, B. (2017). Energy Visualization for Smart Home. *Energy Procedia*, *105*, 2545–2548. https://doi.org/10.1016/j.egypro.2017.03.732

Fanti, M. P., Faraut, G., Lesage, J.-J., & Roccotelli, M. (2016). An Integrated Framework for Binary Sensor Placement and Inhabitants Location Tracking. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, *PP*(99), 154–160. https://doi.org/10.1109/TSMC.2016.2597699

Ford, R., Pritoni, M., Sanguinetti, A., & Karlin, B. (2017). Categories and functionality of smart home technology for energy management. *Building and Environment*, *123*, 543–554. https://doi.org/10.1016/j.buildenv.2017.07.020

Gamundani, A. M. (2015). An impact review on internet of things attacks. In *2015 International Conference on Emerging Trends in Networks and Computer Communications (ETNCC)* (pp. 114–118). IEEE. https://doi.org/10.1109/ETNCC.2015.7184819

Gao, Y., Ma, H., Abbott, D., & Al-Sarawi, S. F. (2017). PUF Sensor: Exploiting PUF Unreliability for Secure Wireless Sensing. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 1–12. https://doi.org/10.1109/TCSI.2017.2695228

Ge, M., Hong, J. B., Yusuf, S. E., & Kim, D. S. (2018). Proactive defense mechanisms for the software-defined Internet of Things with non-patchable vulnerabilities. *Future Generation Computer Systems*, *78*, 568–582. https://doi.org/10.1016/j.future.2017.07.008

Gehrmann, C., Tiloca, M., & Hoglund, R. (2015). SMACK: Short message authentication check against battery exhaustion in the Internet of Things. *2015 12th Annual IEEE International Conference on Sensing, Communication, and Networking, SECON 2015*, 274–282. https://doi.org/10.1109/SAHCN.2015.7338326

Ghosh, P., & Mahesh, T. R. (2016). A Privacy Preserving Mutual Authentication Protocol for RFID based Automated Toll Collection System. In *Proceedings of 2016 International Conference on ICT in Business, Industry, and Government, ICTBIG 2016*. Published by Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ICTBIG.2016.7892668

Gioia, D. A., Corley, K. G., & Hamilton, A. L. (2013). Seeking Qualitative Rigor in Inductive Research: Notes on the Gioia Methodology. *Organizational Research Methods*, *16*(1), 15–31. https://doi.org/10.1177/1094428112452151

Gope, P., & Hwang, T. (2016a). Authentication Protocol for Securing Real-Time Application Data Access in Wireless Sensor Networks. *IEEE Transactions on Infdustrial Electronics*, *63*(11), 7124–7132.

Gope, P., & Hwang, T. (2016b). Lightweight and Energy-Efficient Mutual Authentication and Key Agreement Scheme with User Anonymity for Secure Communication in Global Mobility Networks. *IEEE Systems Journal*, *10*(4), 1370–1379. https://doi.org/10.1109/JSYST.2015.2416396

Granjal, J., Monteiro, E., & Sa Silva, J. (2015). Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues. *IEEE Communications Surveys & Tutorials*, *17*(3), 1294–1312. https://doi.org/10.1109/COMST.2015.2388550

Gray, D. E. (2014). *Doing Research in the Real World*.

Griffin, P. H. (2015). Security for ambient assisted living: Multi-factor authentication in the internet of things. *2015 IEEE Globecom Workshops, GC Wkshps 2015 - Proceedings*. https://doi.org/10.1109/GLOCOMW.2015.7413961

Gu, Z. L., & Liu, Y. (2017). Scalable group audio-based authentication scheme for IoT devices. *Proceedings - 12th International Conference on Computational Intelligence and Security, CIS 2016*, 277–281. https://doi.org/10.1109/CIS.2016.69

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, *29*(7), 1645–1660. https://doi.org/10.1016/j.future.2013.01.010

Guesgen, H. W., & Marsland, S. (2016). Using contextual information for recognising human behaviour. *International Journal of Ambient Computing and Intelligence*, *7*(1). https://doi.org/10.4018/IJACI.2016010102

Haller, S. (2013). The Things in the Internet of Things. In *Poster at the (IoT 2010). Tokyo, Japan, November*. https://doi.org/10.1201/b13090

Halpern, J. Y., & Pucella, R. (2012). Modeling adversaries in a logic for security protocol analysis. *Logical Methods in Computer Science*. https://doi.org/10.2168/LMCS-8(1:21)2012

Han, J. (2016). Chaining the secret: Lightweight authentication for security in pervasive computing. *2016 IEEE International Conference on Pervasive Computing and Communication Workshops, PerCom Workshops 2016*, 0–2. https://doi.org/10.1109/PERCOMW.2016.7457084

Henderson, A. (2015). The CIA Triad: Confidentiality, Integrity, Availability. *Panmore Institute*. Retrieved from http://panmore.com/the-cia-triad-confidentiality-integrity-availability

Hevner, A., & Chatterjee, S. (2010). Design Research in Information Systems. *IntegratedSeries in Information Systems*, *22*, 9–23. https://doi.org/10.1007/978-1-4419-5653-8

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design Science in Information Systems Research. *MIS Quarterly*, *28*(1), 75–105. https://doi.org/10.2307/25148625

Hofer, T., Schumacher, M., & Bromuri, S. (2015). COMPASS: an Interoperable Personal Health System to Monitor and Compress Signals in Chronic Obstructive Pulmonary Disease. *Proceedings of the 9th International Conference on Pervasive Computing Technologies for Healthcare*. https://doi.org/10.4108/icst.pervasivehealth.2015.259186

Hossain, M., Noor, S., & Hasan, R. (2017). HSC-IoT: A Hardware and Software Co-Verification Based Authentication Scheme for Internet of Things. *Proceedings - 5th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering, MobileCloud 2017*, 109–116. https://doi.org/10.1109/MobileCloud.2017.35

Howell, S., Rezgui, Y., & Beach, T. (2017). Integrating building and urban semantics to empower smart water solutions. *Automation in*

Construction, *81*, 434–448. https://doi.org/10.1016/j.autcon.2017.02.004

Huang, J.-J., Juang, W.-S., Fan, C.-I., Tseng, Y.-F., & Kikuchi, H. (2016). Lightweight Authentication Scheme with Dynamic Group Members in IoT Environments. In *Proceedings of the 13th International Conference on Mobile and Ubiquitous Systems: Computing Networking and Services - MOBIQUITOUS 2016*. https://doi.org/10.1145/3004010.3004020

Hui, T. K. L., Sherratt, R. S., & Sánchez, D. D. (2017). Major requirements for building Smart Homes in Smart Cities based on Internet of Things technologies. *Future Generation Computer Systems*, *76*, 358–369. https://doi.org/10.1016/j.future.2016.10.026

Iinatti, J., Member, S., & Ha, P. H. (2017). Smart Home Environments. *Ieee Transactions on Information Forensics and Security*, *12*(4), 968–979.

Jacobsen, R. H., Mikkelsen, S. A., & Rasmussen, N. H. (2015). Towards the use of pairing-based cryptography for resource-constrained home area networks. *Proceedings - 18th Euromicro Conference on Digital System Design, DSD 2015*, 233–240. https://doi.org/10.1109/DSD.2015.73

Jacobsson, A., Boldt, M., & Carlsson, B. (2016). A risk analysis of a smart home automation system. *Future Generation Computer Systems*, *56*, 719–733. https://doi.org/10.1016/j.future.2015.09.003

Janbabaei, S., Gharaee, H., & Mohammadzadeh, N. (2017). Lightweight, anonymous and mutual authentication in IoT infrastructure. *2016 8th International Symposium on Telecommunications, IST 2016*, 162–166. https://doi.org/10.1109/ISTEL.2016.7881802

Jen-Ho, Y., Ya-Fen, C., & Chih-Cheng, H. (2013). A user authentication scheme on multi-server environments for cloud computing. *ICICS 2013 - Conference Guide of the 9th International Conference on Information, Communications and Signal Processing*, 1–4. https://doi.org/10.1109/ICICS.2013.6782791

Jha, A., & Sunil, M. C. (2014). *Security considerations for Internet of Things*.

Jiang, Q. I., Zeadally, S., & He, D. (2017). Lightweight Three-Factor Authentication and Key Agreement Protocol for Internet-Integrated Wireless Sensor Networks, *5*. https://doi.org/10.1109/ACCESS.2017.2673239

Joo, I., & Choi, D. (2017). Considering Consumer ’ s Electricity Bill Target. *IEEE Transactions on Consumer Electronics*, *1*(63), 19–27.

Kang, K., Pang, Z. B., & Wang, C. (2013). Security and privacy mechanism for health internet of things. *Journal of China Universities of Posts and Telecommunications*, *20*(SUPPL-2), 64–68. https://doi.org/10.1016/S1005-8885(13)60219-8

Kanuparthi, A., Karri, R., & Addepalli, S. (2013). Hardware and embedded security in the context of internet of things. *Proceedings of the 2013 ACM Workshop on Security, Privacy & Dependability for Cyber Vehicles - CyCAR ’13*, 61–64. https://doi.org/10.1145/2517968.2517976

Kaplan, B., & Duchon, D. (1988). Combining Qualitative and Quantitative Methods in Information Systems. *MIS Quarterly*, *12*(4), 571–586. Retrieved from http://www.jstor.org

Kara, M., Lamouchi, O., & Ramdane-Cherif, A. (2017). A Quality Model for the Evaluation AAL Systems. *Procedia Computer Science*, *113*, 392–399. https://doi.org/10.1016/j.procs.2017.08.354

Karthi, M., & Harris, P. (2016). A Realistic Lightweight Authentication Protocol for Securing Cloud based RFID System Surekha, 168–171. https://doi.org/10.1109/CCEM.2016.38

Kaur, K., Kumar, N., Singh, M., & Obaidat, M. S. (2016). Lightweight authentication protocol for RFID-enabled systems based on ECC. *2016 IEEE Global Communications Conference, GLOBECOM 2016 - Proceedings*, (Id). https://doi.org/10.1109/GLOCOM.2016.7841955

Khemissa, H., & Tandjaoui, D. (2016a). A Lightweight Authentication Scheme for E-Health Applications in the Context of Internet of Things. *Proceedings - NGMAST 2015: The 9th International Conference on Next Generation Mobile Applications, Services and Technologies*, 90–95. https://doi.org/10.1109/NGMAST.2015.31

Khemissa, H., & Tandjaoui, D. (2016b). A Novel Lightweight Authentication Scheme for heterogeneous Wireless Sensor Networks in the context of Internet of Things. *2016 Wireless Telecommunications Symposium (WTS)}*, 1–6.

Kim, Y. P., Yoo, S., & Yoo, C. (2015). DAoT: Dynamic and energy-aware authentication for smart home appliances in Internet of Things. In *2015 IEEE International Conference on Consumer Electronics, ICCE 2015*. https://doi.org/10.1109/ICCE.2015.7066378

Kishimoto, H., Yanai, N., & Okamura, S. (2017). An anonymous authentication protocol for smart grid. *Proceedings - 31st IEEE International Conference on Advanced Information Networking and Applications Workshops, WAINA 2017*, 62–67. https://doi.org/10.1109/WAINA.2017.41

Kothmayr, T., Schmitt, C., Hu, W., Brünig, M., & Carle, G. (2013). DTLS based security and two-way authentication for the Internet of Things. *Ad Hoc Networks*, *11*(8), 2710–2723. https://doi.org/10.1016/j.adhoc.2013.05.003

Kruusimagi, M., Sharples, S., & Robinson, D. (2017). Living with an autonomous spatiotemporal home heating system: Exploration of the user experiences (UX) through a longitudinal technology intervention-based mixed-methods approach. *Applied Ergonomics*, *65*, 286–308. https://doi.org/10.1016/j.apergo.2017.06.017

Lee, B., Kwon, O., Lee, I., & Kim, J. (2017). Companionship with smart home devices: The impact of social connectedness and interaction types on perceived social support and companionship in smart homes. *Computers in Human Behavior*, *75*, 922–934. https://doi.org/10.1016/j.chb.2017.06.031

Lee, J. S., Choi, S., & Kwon, O. (2017). Identifying multiuser activity with overlapping acoustic data for mobile decision making in smart home environments. *Expert Systems With Applications*, *81*, 299–308. https://doi.org/10.1016/j.eswa.2017.03.062

Li, G., Xu, X., & Li, Q. (2015). LADP: A lightweight authentication and delegation protocol for RFID tags. *International Conference on Ubiquitous and Future Networks, ICUFN*, *2015–Augus*, 860–865. https://doi.org/10.1109/ICUFN.2015.7182666

Li, J., Yan, Q., & Chang, V. (2018). Internet of Things: Security and privacy in a connected world. *Future Generation Computer Systems*, *78*, 931–932. https://doi.org/10.1016/j.future.2017.09.017

Li, S., Xu, L. Da, & Zhao, S. (2015a). The internet of things: a survey. *Information Systems Frontiers*, *17*(2), 243–259. https://doi.org/10.1007/s10796-014-9492-7

Li, S., Xu, L. Da, & Zhao, S. (2015b). The internet of things: a survey. *Information Systems Frontiers*, *17*(2), 243–259. https://doi.org/10.1007/s10796-014-9492-7

Li, X., Liu, H., Wei, F., Ma, J., & Yang, W. (2015). A lightweight anonymous authentication protocol using k-pseudonym set in wireless networks. *2015 IEEE Global Communications Conference, GLOBECOM 2015*. https://doi.org/10.1109/GLOCOM.2014.7417584

Li, Y., Wang, Y., Cheng, Y., Li, X., & Xing, G. (2015). QiLoc: A Qi wireless charging based system for robust user-initiated indoor location services. *2015 12th Annual IEEE International Conference on Sensing, Communication, and Networking, SECON 2015*, 480–488. https://doi.org/10.1109/SAHCN.2015.7338349

Lin, S. C., & Wen, C. Y. (2016). Energy-efficient device-based node authentication protocol for the Internet of Things. *2016 IEEE International Conference on Consumer Electronics-Taiwan, ICCE-TW 2016*, (1), 1–2. https://doi.org/10.1109/ICCE-TW.2016.7520962

Lin, Y. W., Lin, Y. B., Hsiao, C. Y., & Wang, Y. Y. (2017). IoTtalk-RC: Sensors As Universal Remote Control for Aftermarket Home Appliances. *IEEE Internet of Things Journal*, *4*(4), 1104–1112. https://doi.org/10.1109/JIOT.2017.2715859

Ling, Z., Luo, J., Xu, Y., Gao, C., Wu, K., & Fu, X. (2017). Security Vulnerabilities of Internet of Things: A Case Study of the Smart Plug System. *IEEE Internet of Things Journal*, *4662*(c), 1–1. https://doi.org/10.1109/JIOT.2017.2707465

Liu, Y., Hu, S., Member, S., Huang, H., Member, S., Ranjan, R., … Member, S. (2017). Game -Theoretic Market-Driven Smart Home Sceduling Considering Energy Balancing. *IEEE Systems Journal*, *11*(2), 910–921.

Liu, Y., Liu, L., Zhou, Y., & Hu, S. (2016). Leveraging carbon nanotube technologies in developing Physically Unclonable Function for cyber-physical system authentication. *Proceedings - IEEE INFOCOM*, *2016–Septe*, 176–180. https://doi.org/10.1109/INFCOMW.2016.7562067

Macal, C. M., & North, M. J. (2008). Agent-based modeling and simulation: ABMS examples. *Proceedings - Winter Simulation Conference*, 101–112. https://doi.org/10.1109/WSC.2008.4736060

Mahalle, P. (2013). Identity Authentication and Capability Based Access Control (IACAC) for the Internet of Things. *Journal of Cyber …*, *1*, 309–348. Retrieved from http://forskningsbasen.deff.dk/Share.external?sp=S72df67ac-3ea5-41da-8cf0-523c6f71bbf2&sp=Saau

Majeed, A. (2017). Internet of Things (IoT): A verification framework. *2017 IEEE 7th Annual Computing and Communication Workshop and Conference, CCWC 2017*, 2–4. https://doi.org/10.1109/CCWC.2017.7868461

Mandyam, G. D. (2017). Tiered Attestation for Internet-of-Things (IoT) Devices. In *2017 9th International Conference on Communication Systems and Networks (COMSNETS)* (pp. 480–483).

Mannion, P. (2015). Optimal Analysis Algorithms are IoT’s Big Opportunity | Electronics360. *Electronics 360*. Retrieved from http://electronics360.globalspec.com/article/4890/optimal-analysis-algorithms-are-iot-s-big-opportunity

Mano, L. Y., Faiçal, B. S., Nakamura, L. H. V., Gomes, P. H., Libralon, G. L., Meneguete, R. I., … Ueyama, J. (2016). Exploiting IoT technologies for enhancing Health Smart Homes through patient identification and emotion recognition. *Computer Communications*, *89–90*, 178–190. https://doi.org/10.1016/j.comcom.2016.03.010

Maple, C. (2017). Security and privacy in the internet of things. *Journal of Cyber Policy*, *2*(2), 155–184. https://doi.org/10.1080/23738871.2017.1366536

March, S. T., & Storey, V. C. (2016). Design Science in the Information Systems Discipline: An Introduction to the Special Issue on Design

Science Research. *MIS Quarterly*, *32*(4), 725–730. Retrieved from url: http://www.jstor.org/stable/25148869

Margulies, J. (2015). Garage Door Openers: An Internet of Things Case Study. *IEEE Security & Privacy*, *13*(4), 80–83. https://doi.org/10.1109/MSP.2015.80

Martina, J. E., dos Santos, E., Carlos, M. C., Price, G., & Custódio, R. F. (2015). An adaptive threat model for security ceremonies. *International Journal of Information Security*. https://doi.org/10.1007/s10207-014-0253-x

Mbarek, B., Meddeb, A., Ben Jaballah, W., & Mosbah, M. (2017). A broadcast authentication scheme in IoT environments. *Proceedings of IEEE/ACS International Conference on Computer Systems and Applications, AICCSA*. https://doi.org/10.1109/AICCSA.2016.7945807

Meana-Llorián, D., González García, C., Pelayo G-Bustelo, B. C., Cueva Lovelle, J. M., & Garcia-Fernandez, N. (2017). IoFClime: The fuzzy logic and the Internet of Things to control indoor temperature regarding the outdoor ambient conditions. *Future Generation Computer Systems*, *76*, 275–284. https://doi.org/10.1016/j.future.2016.11.020

Mohsin, M., Sardar, M. U., Hasan, O., & Anwar, Z. (2017). IoTRiskAnalyzer: A Probabilistic Model Checking Based Framework for Formal Risk Analytics of the Internet of Things. *IEEE Access*, *5*, 5494–5505. https://doi.org/10.1109/ACCESS.2017.2696031

Mokhtari, G., Zhang, Q., Hargrave, C., & Ralston, J. C. (2017). Non-Wearable UWB Sensor for Human Identification in Smart Home. *IEEE Sensors Journal*, *17*(11), 3332–3340. https://doi.org/10.1109/JSEN.2017.2694555

Mokhtari, G., Zhang, Q., Nourbakhsh, G., Ball, S., & Karunanithi, M. (2017). BLUESOUND: A New Resident Identification Sensor - Using Ultrasound Array and BLE Technology for Smart Home Platform. *IEEE Sensors Journal*, *17*(5), 1503–1512. https://doi.org/10.1109/JSEN.2017.2647960

Morsalin, S., Islam, A. M. J., Rahat, G. R., Pidim, S. R. H., Rahman, A., & Siddiqe, M. A. B. (2017). Machine-to-machine communication based smart home security system by NFC, fingerprint, and PIR sensor with mobile android application. *2016 3rd International Conference on Electrical Engineering and Information and Communication Technology, ICEEiCT 2016*. https://doi.org/10.1109/CEEICT.2016.7873048

Moskvitch, K. (2017). Securing IOT: In your smart home and your connected enterprise. *Engineering and Technology*, *12*(3), 40–42. https://doi.org/10.1159/000113927

Nguyen, H. V., & Iacono, L. Lo. (2016). REST-ful CoAP Message Authentication. *Proceedings - 2015 International Workshop on Secure Internet of Things, SIoT 2015*, 35–43. https://doi.org/10.1109/SIOT.2015.8

Nissar, N., Naja, N., & Jamali, A. (2017). Lightweight authentication-based scheme for AODV in ad-hoc networks. In *2017 International Conference on Wireless Technologies, Embedded and Intelligent Systems, WITS 2017*. https://doi.org/10.1109/WITS.2017.7934616

Offermann, P., Levina, O., Schonherr, M., & Bub, U. (2009). Outline of a Design Science Research Process. *Proceedings of the 4th International Conference on Design Science Research in Information Systems and Technology*, *May*, 1–11. https://doi.org/10.1145/1555619.1555629

Orpwood, R. (2012). Smart Homes. *Pathy's Principles and Practice of Geriatric Medicine: Fifth Edition*. John Wiley & Sons, Ltd. https://doi.org/10.1002/9781119952930.ch124

Oyegoke, A. (2011). The constructive research approach in project management research. *International Journal of Managing Projects in Business*, *4*(4), 573–595. https://doi.org/10.1108/17538371111164029

Paek, J. (2015). Fast and Adaptive Mesh Access Control in Low-Power and Lossy Networks. *IEEE Internet of Things Journal*, *2*(5), 435–444. https://doi.org/10.1109/JIOT.2015.2457940

Parikshit N.Mahalle, Bayu Anggorojati, N. R. P. and R. P. (2013). Identity Authentication and Capability Based Access Control (IACAC) for the Internet of Things. *Journal of Cyber …*, *1*, 309–348. Retrieved from http://forskningsbasen.deff.dk/Share.external?sp=S72df67ac-3ea5-41da-8cf0-523c6f71bbf2&sp=Saau

Park, H., Hwang, S., Won, M., & Park, T. (2016). Activity-aware Sensor Cycling for Human Activity Monitoring in Smart Homes. *IEEE Communications Letters*, *7798*(c), 1–1. https://doi.org/10.1109/LCOMM.2016.2619700

Patel, S., Patel, D. R., & Navik, A. P. (2016). Energy efficient integrated authentication and access control mechanisms for Internet of Things. *2016 International Conference on Internet of Things and Applications, IOTA 2016*, 304–309. https://doi.org/10.1109/IOTA.2016.7562742

Pienaar, J. P., Fisher, R. M., & Hancke, G. P. (2015). Smartphone: The key to your connected smart home. *Proceeding - 2015 IEEE International Conference on Industrial Informatics, INDIN 2015*, 999–1004. https://doi.org/10.1109/INDIN.2015.7281871

Pöpper, C., Tippenhauer, N. O., Danev, B., & Capkun, S. (2011). Investigation of signal and message manipulations on the wireless channel. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. https://doi.org/10.1007/978-3-642-23822-2_3

Premnath, S. N., & Haas, Z. J. (2015). Security and privacy in the internet-of-things under time-and-budget-limited adversary model. *IEEE Wireless Communications Letters*, *4*(3), 277–280. https://doi.org/10.1109/LWC.2015.2408609

Rahman, M., Sampangi, R. V., & Sampalli, S. (2015). Lightweight protocol for anonymity and mutual authentication in RFID systems. *2015 12th Annual IEEE Consumer Communications and Networking Conference, CCNC 2015*, 910–915. https://doi.org/10.1109/CCNC.2015.7158097

Rawashdeh, M., Al Zamil, M. G. H., Samarah, S., Hossain, M. S., & Muhammad, G. (2017). A knowledge-driven approach for activity recognition in smart homes based on activity profiling. *Future Generation Computer Systems*. https://doi.org/10.1016/j.future.2017.10.031

Ray, B., Chowdhury, M. U., & Abawajy, J. (2017). A Multi-Protocol Security Framework to Support Internet of Things, *198*(June). https://doi.org/10.1007/978-3-319-59608-2

Ray, B. R., Chowdhury, M. U., & Abawajy, J. H. (2016). Secure Object Tracking Protocol for the Internet of Things. *IEEE Internet of Things Journal*, *3*(4), 544–553. https://doi.org/10.1109/JIOT.2016.2572729

Ray, B. R. R., Abawajy, J., Chowdhury, M., & Alelaiwi, A. (2018). Universal and secure object ownership transfer protocol for the Internet of Things. *Future Generation Computer Systems*, *78*(February), 838–849. https://doi.org/10.1016/j.future.2017.02.020

Ren, H., Song, Y., Yang, S., & Situ, F. (2016). Secure smart home: A voiceprint and internet based authentication system for remote accessing. *ICCSE 2016 - 11th International Conference on Computer Science and Education*, (Iccse), 247–251. https://doi.org/10.1109/ICCSE.2016.7581588

Rigney, C., Willens, S., Rubens, A., & Simpson, W. (2013). RFC 2687 - Remote Authentication Dial In User Service (RADIUS). *Journal of Chemical Information and Modeling*, *53*(9), 1689–1699. https://doi.org/10.1017/CBO9781107415324.004

Rizzardi, A., Sicari, S., Miorandi, D., & Coen-Porisini, A. (2016). AUPS: An Open Source AUthenticated Publish/Subscribe system for the Internet of Things. *Information Systems*, *62*, 29–41. https://doi.org/10.1016/j.is.2016.05.004

Roy, S., Chatterjee, S., Das, A. K., Chattopadhyay, S., Kumari, S., & Jo, M. (2017). Chaotic Map-based Anonymous User Authentication Scheme with User Biometrics and Fuzzy Extractor for Crowdsourcing Internet of Things. *IEEE Internet of Things Journal*, *4662*(c), 1–1. https://doi.org/10.1109/JIOT.2017.2714179

Rwegasira, D., Kondoro, A., Kelati, A., Dhaou, I. B. E. N., Mvungi, N., & Tenhunen, H. (2018). CDE for ICT Innovation Through the IoT Based iGrid Project in Tanzania. In Paul Cunningham and Miriam Cunningham (Eds) (Ed.), *IST-Africa 2018 Conference Proceedings* (pp. 1–9). IIMC International Information Management Corporation.

Saadeh, M., Sleit, A., Qatawneh, M., & Almobaideen, W. (2016). Authentication techniques for the internet of things: A survey. *Proceedings - 2016 Cybersecurity and Cyberforensics Conference, CCC 2016*, 28–34. https://doi.org/10.1109/CCC.2016.22

Saied, Y. Ben, Olivereau, A., Zeghlache, D., & Laurent, M. (2014). Lightweight collaborative key establishment scheme for the Internet of Things. *Computer Networks*, *64*, 273–295. https://doi.org/10.1016/j.comnet.2014.02.001

Savola, R., Abie, H., & Sihvonen, M. (2012). Towards Metrics-Driven Adaptive Security Management in E-Health IoT Applications. *Proceedings of the 7th International Conference on Body Area Networks*, *250241*(SeTTIT), 276–281. https://doi.org/10.4108/icst.bodynets.2012.250241

Saxena, N., Choi, B. J., & Cho, S. (2015). Lightweight privacy-preserving authentication scheme for V2G networks in the smart grid. *Proceedings - 14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2015*, *1*, 604–611. https://doi.org/10.1109/Trustcom.2015.425

Saxena, N., Choi, B. J., & Lu, R. (2016). Authentication and Authorization Scheme for Various User Roles and Devices in Smart Grid. *IEEE Transactions on Information Forensics and Security*, *11*(5), 907–921. https://doi.org/10.1109/TIFS.2015.2512525

Schaumont, P., Moriyama, D., Gulcan, E., & Aysu, A. (2016). Compact and low-power ASIP design for lightweight PUF-based authentication protocols. *IET Information Security*, *10*(5), 232–241. https://doi.org/10.1049/iet-ifs.2015.0401

SDGs. (2017). The Sustainable Development Goals Report, The Unitd Nations. *United Nations*, 1–56. https://doi.org/10.18356/3405d09f-en

Seo, D. W., Kim, H., Kim, J. S., & Lee, J. Y. (2016). Hybrid reality-based user experience and evaluation of a context-aware smart home. *Computers in Industry*, *76*, 11–23.

https://doi.org/10.1016/j.compind.2015.11.003

Shahzad, M., Singh, M. P., & Carolina, N. (2017). Continuos Authentication and Authorization for the Internet of Things. *IEEE Internet Computing*, *21*(2), 86–90. https://doi.org/10.1109/MIC.2017.33

Shaju, S., & Panchami, V. (2016). BISC Authentication Algorithm : An Efficient New Authentication Algorithm Using Three Factor Authentication for Mobile Banking. In *2016 Online International Conference on Green Engineering and Technologies (IC-GET) BISC*.

Sharaf-Dabbagh, Y., & Saad, W. (2016). On the authentication of devices in the Internet of things. *WoWMoM 2016 - 17th International Symposium on a World of Wireless, Mobile and Multimedia Networks*, 1–3. https://doi.org/10.1109/WoWMoM.2016.7523532

Sharma, P., Khanna, R. R., & Bhatnagar, V. (2017). Application of TRIZ framework for resolving security issues in IOT. In *Proceeding - IEEE International Conference on Computing, Communication and Automation, ICCCA 2016*. https://doi.org/10.1109/CCAA.2016.7813921

Shen, C., Li, H., Sahin, G., & Choi, H. A. (2016). Low-complexity Scalable Authentication algorithm with Imperfect Shared Keys for Internet of Things. *2016 IEEE International Conference on Communications Workshops, ICC 2016*, 116–121. https://doi.org/10.1109/ICCW.2016.7503774

Shen, J., Liu, D., Chang, S., Shen, J., & He, D. (2016). A Lightweight Mutual Authentication Scheme for User and Server in Cloud. *Proceedings - 2015 1st International Conference on Computational Intelligence Theory, Systems and Applications, CCITSA 2015*, 183–186. https://doi.org/10.1109/CCITSA.2015.47

Shen, J., Tan, H., Chang, S., Ren, Y., & Liu, Q. (2015). A lightweight and practical RFID grouping authentication protocol in multiple-tag arrangements. *International Conference on Advanced Communication Technology, ICACT*, *2015–Augus*, 681–686. https://doi.org/10.1109/ICACT.2015.7224882

Shen, T., & Maode, M. (2016). Security Enhancements on Home Area Networks in Smart Grids. In *IEEE Region 10 Conference (TENCON)* (pp. 2444–2447).

Shin, D., Sharma, V., Kim, J., Kwon, S., & You, I. (2017). Secure and Efficient Protocol for Route Optimization in PMIPv6-based Smart Home IoT Networks. *IEEE Access*, *3536*(c). https://doi.org/10.1109/ACCESS.2017.2710379

Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks*, *76*, 146–164. https://doi.org/10.1016/j.comnet.2014.11.008

Silverajan, B., Luoma, J. P., Vajaranta, M., & Itapuro, R. (2015). Collaborative cloud-based management of home networks. *Proceedings of the 2015 IFIP/IEEE International Symposium on Integrated Network Management, IM 2015*, 786–789. https://doi.org/10.1109/INM.2015.7140376

Sivanathan, A., Sherratt, D., Gharakheili, H. H., Sivaraman, V., & Vishwanath, A. (2017). Low-cost flow-based security solutions for smart-home IoT devices. *2016 IEEE International Conference on Advanced Networks and Telecommunications Systems, ANTS 2016*. https://doi.org/10.1109/ANTS.2016.7947781

Skocir, P., Krivic, P., Tomeljak, M., Kusek, M., & Jezic, G. (2016). Activity Detection in Smart Home Environment. *Procedia Computer Science*, *96*, 672–681. https://doi.org/10.1016/j.procs.2016.08.249

Smirek, L., Zimmermann, G., & Beigl, M. (2016). Just a Smart Home or Your Smart Home - A Framework for Personalized User Interfaces Based on Eclipse Smart Home and Universal Remote Console. *Procedia Computer Science*, *58*(Euspn), 107–116. https://doi.org/10.1016/j.procs.2016.09.018

Song, T., Li, R., Mei, B., Yu, J., Xing, X., & Cheng, X. (2017). A Privacy Preserving Communication Protocol for IoT Applications in Smart Homes. *IEEE Internet of Things Journal*, *4662*(c), 1–1. https://doi.org/10.1109/JIOT.2017.2707489

Stephanie. (2017). Snowball Sampling: Definition, Advantages and Disadvantages. Retrieved January 15, 2018, from http://www.statisticshowto.com/snowball-sampling/

Tankard, C. (2015). The security issues of the Internet of Things. *Computer Fraud & Security*, *2015*(9), 11–14. https://doi.org/10.1016/S1361-3723(15)30084-1

Tao, M., Zuo, J., Liu, Z., Castiglione, A., & Palmieri, F. (2018). Multi-layer cloud architectural model and ontology-based security service framework for IoT-based smart homes. *Future Generation Computer Systems*, *78*, 1040–1051. https://doi.org/10.1016/j.future.2016.11.011

Tobin, G. A., & Begley, C. M. (2004). Methodological Rigour within a Qualittaive Framework. *Journal of Advanced Nursing*, *48*(4), 388–396. https://doi.org/10.1111/j.1365-2648.2004.03207.x

Tran, A. C., Marsland, S., Dietrich, J., Guesgen, H. W., & Lyons, P. (2010). Use cases for abnormal behaviour detection in smart homes. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* (Vol. 6159 LNCS, pp. 144–151). https://doi.org/10.1007/978-3-642-13778-5_18

Vermesan, O., Friess, P., Guillemin, P., Gusmeroli, S., Sundmaeker, H., Bassi, A., … Doody, P. (2016). Internet of Things Strategic Research Roadmap 2.1 Internet of Things Conceptual Framework 2.2 Internet of Things Vision. In *In Proceedings of 2016 International Conference on ICT in Business, Industry, and Government, ICTBIG 2016* (pp. 1–44). Institute of Electrical and Electronics Engineers Inc. https://doi.org/https://doi.org/10.1109/ICTBIG.2016.7892668

Wang, F., Xu, Y., Zhang, H., Zhang, Y., & Zhu, L. (2016). 2FLIP: A two-factor lightweight privacy-preserving authentication scheme for VANET. *IEEE Transactions on Vehicular Technology*, *65*(2), 896–911. https://doi.org/10.1109/TVT.2015.2402166

Weber, R. (2010). Internet of Things - New security and privacy challenges. *Computer Law & Security Review*. https://doi.org/10.1016/j.clsr.2009.11.008

Winter, R. (2008). Design science research in Europe. *European Journal of Information Systems*, *17*(5), 470–475. https://doi.org/10.1057/ejis.2008.44

Witkovski, A., Santin, A., Abreu, V., & Marynowski, J. (2015). An IdM and key-based authentication method for providing single sign-on in IoT. *2015 IEEE Global Communications Conference, GLOBECOM 2015*, (IdM). https://doi.org/10.1109/GLOCOM.2014.7417597

Wu, Q. X., & Li, H. (2013). Secure solution of trusted Internet of things base on TCM. *Journal of China Universities of Posts and Telecommunications*, *20*(SUPPL-2), 47–53. https://doi.org/10.1016/S1005-8885(13)60222-8

Yang, J. H., & Lin, P. Y. (2014). An ID-Based User Authentication Scheme for Cloud Computing. *2014 Tenth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*. https://doi.org/10.1109/IIH-MSP.2014.31

Yang, M. L., Narayanan, A., Parry, D., & Wang, X. (2016). A lightweight authentication scheme for transport system farecards. *2016 IEEE International Conference on RFID Technology and Applications, RFID-TA 2016*, 150–155. https://doi.org/10.1109/RFID-TA.2016.7750746

Yang, Y., Sun, J., & Guo, L. (2016). PersonaIA: A Lightweight Implicit Authentication System based on Customized User Behavior Selection. *IEEE Transactions on Dependable and Secure Computing*, *5971*(c), 1–1. https://doi.org/10.1109/TDSC.2016.2645208

Yao, X., Chen, Z., & Tian, Y. (2014). A lightweight attribute-based encryption scheme for the Internet of Things. *Future Generation Computer Systems*, *49*, 104–112. https://doi.org/10.1016/j.future.2014.10.010

Yaqoob, I., Ahmed, E., Rehman, M. H. ur, Ahmed, A. I. A., Al-garadi, M. A., Imran, M., & Guizani, M. (2017). The rise of ransomware and emerging security challenges in the Internet of Things. *Computer Networks*, *129*, 444–458. https://doi.org/10.1016/j.comnet.2017.09.003

Yoon, E.-J., Das, A. K., Yoo, K.-Y., & Goutham Reddy, A. (2016). Lightweight authentication with key-agreement protocol for mobile network environment using smart cards. *IET Information Security*, *10*(5), 272–282. https://doi.org/10.1049/iet-ifs.2015.0390

Yu, M.-D. M., Hiller, M., Delvaux, J., Sowell, R., Devadas, S., & Verbauwhede, I. (2016). A Lockdown Technique to Prevent Machine.pdf. *IEEE Transactions on Multi-Scale Computing Systems*, *2*(3), 146–159. https://doi.org/10.1109/TMSCS.2016.2553027

Zhang, D., Yang, L. T., Chen, M., Zhao, S., Guo, M., & Zhang, Y. (2014). Real-Time Locating Systems Using Active RFID for Internet of Things. *IEEE Systems Journal*, *10*(3), 1–10. https://doi.org/10.1109/JSYST.2014.2346625

Zhang, N., Wu, X., Yang, C., Shen, Y., & Cheng, Y. (2017). A lightweight authentication and authorization solution based on Kerberos. *Proceedings of 2016 IEEE Advanced Information Management, Communicates, Electronic and Automation Control Conference, IMCEC 2016*, 742–746. https://doi.org/10.1109/IMCEC.2016.7867308

Zhang, R. (2017). An enhanced lightweight authentication protocol for low-cost RFID systems. *Proceedings of 2016 IEEE International Conference on Electronic Information and Communication Technology, ICEICT 2016*, (Iceict), 29–33. https://doi.org/10.1109/ICEICT.2016.7879646

Zhang, Y., Xiang, Y., Huang, X., Chen, X., & Alelaiwi, A. (2018). A matrix-based cross-layer key establishment protocol for smart homes. *Information Sciences*, *429*, 390–405. https://doi.org/10.1016/j.ins.2017.11.039

Zhao, K., & Ge, L. (2013). A survey on the internet of things security. In *Proceedings - 9th International Conference on Computational Intelligence and Security, CIS 2013* (pp. 663–667). https://doi.org/10.1109/CIS.2013.145

Zhong, H., Shao, L., & Cui, J. (2016). A Lightweight and Secure Data Authentication Scheme with Privacy Preservation for Wireless Sensor Networks. *2016 International Conference on Networking and Network Applications (NaNA)*, 210–217. https://doi.org/10.1109/NaNA.2016.85

Zhu, Q., Uddin, M. Y. S., Qin, Z., & Venkatasubramanian, N. (2017). Data collection and upload under dynamicity in smart community

Internet-of-Things deployments. *Pervasive and Mobile Computing*, *42*, 166–186. https://doi.org/10.1016/j.pmcj.2017.10.003