DESIGNING AN ALGORITHM THAT CAN INFLUENCE CHILDREN'S BEHAVIOUR ONLINE AND RAISE THEIR CYBER SECURITY AWARENESS

by

Jennyphar Kavikairiua

212064053

Thesis submitted in partial fulfilment of the requirements for the degree of

Master of Computer Science

in the

Department of Computer Science

at the

NAMIBIA UNIVERSITY OF SCIENCE AND TECHNOLOGY

Supervisor: Prof. Fungai Bhunu Shava

Co-Supervisor: N/A

Submission Date: 18 December 2020

METADATA

TITLE:	Ms
STUDENT NAME:	Kavikairiua Jennyphar
SUPERVISOR:	Professor Fungai Bhunu Shava
CO-SUPERVISOR:	N/A
DEPARTMENT:	Computer Science
QUALIFICATION:	Master of Computer Science
SPECIALISATION:	Information Security
STUDY TITLE:	Designing an Algorithm that can Influence Children's Behaviour Online and Raise their Cyber Security Awareness
MAIN KNOWLEDGE AREA:	Human Computer Interaction Security (HCISec)
KEYWORDS:	Child Online Activities, Child Online Behaviour, Online Exposure, Cybercrimes, Influencing Algorithm, Cybersecurity Awareness
TYPE OF RESEARCH:	Applied Research
METHODOLOGY:	Mixed Methods
STATUS:	Thesis
SITE:	Namibia University of Science and Technology
DOCUMENT DATE:	30 August 2020
SPONSOR /Cluster:	DAAD, Digital Forensics and Information Security Research Cluster

DECLARATION

I, Jennyphar Kahimise Kavikairiua hereby declare that the work contained in the proposal for the Master degree project, entitled**: "Designing an algorithm that can influence children's behaviour online and raise their cybersecurity awareness",** 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.

Jennyphar Kavikairiua

17/12/2020
Date

RETENTION AND USE OF THESIS

I, **Jennyphar Kavikairiua** being a candidate for the degree of Master of **Computer Science** accept the requirements of the Namibia University of Science and Technology relating to the retention and use of thesis deposited in the Library and Information Services.

In terms of these conditions, I agree that the original of my thesis deposited in the Library and Information Services will be accessible for purposes of study and research, in accordance with the normal conditions established by the Librarian for the care, loan or reproduction of thesis.

Signature: 

Date: 17/12/2020

ACKNOWLEDGEMENTS

Thank you Heavenly Father, for the wisdom, the grace, the protection and the strength to help me to accomplish my set goal of completing my postgraduate studies.

I want to take this opportunity to express my thanks to those who made this study possible; without the love and encouragement of many people, it would not have been possible.

Firstly, I would like to most sincerely thank my supervisor, Professor Fungai Bhunu Shava: the path goes back to 2018, when I walked into your office with no idea as to what I wanted to research about. Your mentoring has helped me to grow spiritually, socially, academically and professionally. I will always carry that within my heart for the longest time possible. Your guidance, motivation, thoughtfulness and valuable advice will forever be appreciated. I will forever love and respect you. Thank you so much Prof., your belief in me has really helped me to believe in myself.

My parents and family: This study was made possible thanks to my family. I single out the enduring love and support from my father-in-law, Andronikus Kavikairiua, who would ask about my progress all the time and this gave me more courage to continue. I am deeply grateful for my parents, Orpa Kahimise and Ebenesiutus Kahimise, thank you for the prayers, inspiration, encouragement and upbringing. Finally, I would like to thank my wonderful husband and friend Harrison Kavikairiua. He is the most incredible partner and friend. His wonderful love and sacrifice made this possible. I am deeply grateful for his support. My babies Koviao and Muje (Kavikairiua), are indeed my sources of inspiration. My son Urioukuao Kahimise, I'm dedicating this work to you so that you'll do immensely more one day. Thanks to my sister Fiona Kahimise for always being there for me.

Colleagues: I would like to thank you all who helped me and were a part of my academic journey and life. If I have not mentioned you all by name, I will write another thesis and do so, your support really meant a lot.

DAAD: The financial assistance that you gave me would surely be of great benefit to the nation. Thank you for investing in me and believing in me to be a true leader for the nation. I have grown so much from this experience.

PUBLICATIONS

Kahimise, J., & Bhunu Shava, F. (2020). *An analysis of social networking threats*. 15th International Conference on Cyber Warfare and Security. (ICCWS2020). Virginia. doi:10.34190/ICCWS.20.127

Kahimise, J., & Bhunu Shava, F. (2019). *An analysis of children's online activities and behaviour that expose them to cybercrimes. 27th Telecommunications Forum (TELFOR).* Belgrade, Serbia. doi:10.1109/TELFOR48224.2019.8971089.

ABSTRACT

Title: Designing an Algorithm that can Influence Children's Online Behaviour and Raise their Cyber Security Awareness

The Internet offers children incredible opportunities by enhancing their communication, social connections and technical skills. But it can't just guarantee them a secure environment. With no experience and knowledge, children's behaviours potentially expose them to cyber criminals as they share information innocently and become friends with strangers. Cyber security threats are highly present in social media and many people don't know about them. In particular, children voluntarily reveal personal and private details about themselves from which cybercrimes can emerge either in their real world or in the virtual world, if this shared information ends up in the wrong hands. This is most likely due to previous knowledge or exposure of the children on the Internet. This study sought to examine the online habits and actions of children who are vulnerable to cybercrimes and evaluated suitable behaviour influencing tools for children's online activities. Employing a design science research method began with a comprehension of the problem. This was achieved by analysing the literature and the research findings that were self-constructed, as well as the use of open-ended questionnaires and close-ended questions. Once the problem was identified, the next step was to identify ideas which could solve the problem. These ideas were taken from the domains which were considered important to solve the problem. The behaviour influencing algorithm was then designed and evaluated following the literature and persuasion theory, as a solution to overcome the children's insecure behaviour problem online. The vital contribution of the research is that it can benefit children that will be introduced to this algorithm by influencing and assisting them on how to securely behave online. In addition, the thesis provides contributions to the knowledge base by identifying and analysing the online activities and behaviours of children which can expose children to cybercrimes and it also provided some guidelines on how to influence children's online behaviour, which can be used elsewhere in the world.

Keywords: Child Online Activities, Child Online Behaviour, Online Exposure, Cybercrimes, Influencing Algorithm, Cybersecurity Awareness

Table of Contents

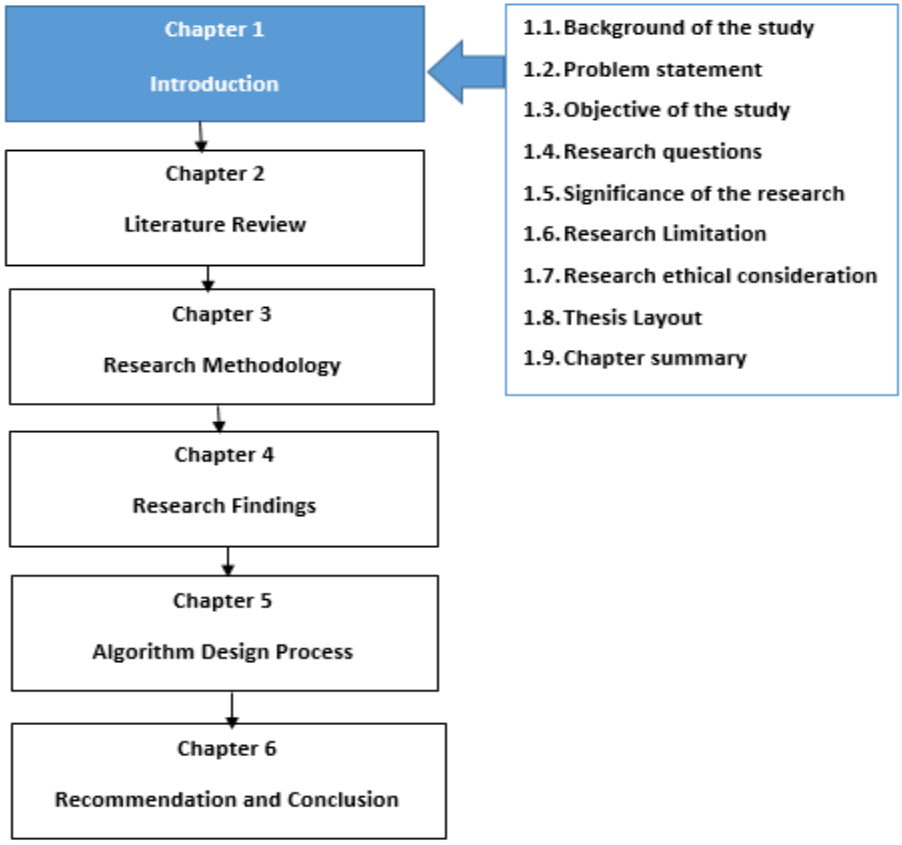
LIST OF FIGURES

LIST OF TABLES

Abbreviation	Full Text
ITU	International Telecommunication Union
FNB	First National Bank
HCI	Human-Computer Interaction
HCISec	Human Computer Interaction and Security
ICT	Information and Communication Technology
NUST	Namibia University of Science and Technology
CJCP	Centre for Justice and Crime Prevention
UNICEF	United Nations Children's Fund
HDC	Higher Degree Committee
FPGC	Faculty Postgraduate Committee
OSN	Online Social Networking
IPS	Intrusion Prevention Software
URL	Uniform Resource Locator
MATEP	Monitoring and Analysis Tool for E-learning
VisMOOC	Visualizing Video Clickstream Data Massive Open Online Course
COSBIA	Child Online Secure Behaviour Influencing Algorithm

Chapter 1: Introduction

This chapter presents the study's context, the description of the problem, the purpose of the study and also the research questions, research significance, research limitations, ethical considerations and the layout of this thesis as outlined in the chapter map below.



1.1. Background of the study

The Internet offers spectacular opportunities for children through enhancing their interactions, socialisation and practical skills. But it cannot guarantee them a safe environment. With little background and awareness, children's actions potentially expose them to cyber criminals as they exchange details innocently and can make friends with strangers. In particular , children willingly reveal personal and confidential information about oneself from which cybercrimes will occur in their actual world or in the digital world if this information sharing ends up in the wrong hands (Fire, Goldschmidt, & Elovici, 2014). Namibia has been ranked at the Initiating Stage in a survey carried out by ITU (2017) to measure member states' commitment to cybersecurity with a view to raise awareness. This means that Namibia has just

started to commit itself in cyber security. Additionally, Namibia in 2018 was ranked at a low level of cyber commitment around the world according to the Global Cybersecurity Index 2018 (ITU, 2018). In January 2020, there were 1.28 million Internet users in Namibia. Namibia's number of Internet users increased by 24 thousand (+1.9 percent) between 2019 and 2020, and Namibia's Internet penetration stood at 51 percent in January 2020 (Kemp, 2020).

According to Nashuuta (2018), in a newspaper article on the International Safer Internet Day, children's rights supporters in Namibia encourage the government to speed up the accession of cyber security legislation to protect children from sexual exploitation and abuse online. The article outlined that Namibia has had an increase in the cyber-criminal acts over the past years, with pornography revenge taking its toll on society and specifically on the families of emotionally abused victims. The article further revealed that the latest incident had been a video reportedly showing a married woman engaging in a sexual act with her secret boyfriend. The video which went viral on social media led to the married woman being humiliated with insults on social platforms, and the embarrassing sex act was posted online and this led her to an emotional wreck. In another newspaper article by Kangootui (2019), a young boy in Katutura took his own life after playing an online game named "the Momo Challenge" with his friends. Apparently the game encouraged players to commit suicide after having received a certain picture on their phone. Kangootui (2019), further reported that the so called "Momo Challenge" had dominated headlines with parents being warned of the viral "suicide game" that was purportedly on the rise on YouTube. In another newspaper article by Olivier (2018), it was argued that the most prone country to cybercrime is Namibia due to a lack of cyber security measures that are in place to guard the country against such a phenomenon. The banking sector also suffered in this regard as in May 2016 Standard Bank was hacked, and as a result, 1600 forged credit cards were generated and used within two hours which cost Standard Bank N$300 million. Moreover, banks in Namibia, mainly First National Bank (FNB), have been warning their clients against mails that are spams, have trojans, result in card fraud and many more types of attacks to prevent cyber criminals from obtaining clients' information and gaining access to transactional systems through phishing and malware. According to Kemp (2020), Namibia had 710.0 000 people using social media in January 2020. Namibia's number of social media users grew by 73 thousand (+12 per cent) between April 2019 and January 2020. In January 2020, Namibia's social media penetration stood at 28 per cent (Kemp, 2020). Children having less knowledge, online experience and the fact that Namibia does not have a national legislation pertaining to child online protection means that more children are affected in this manner by being exposed to illegal, age-inappropriate and or harmful content (Kemp, 2020).

The first exploratory research study conducted in 2016 by the Namibia University of Science and Technology (NUST) and the Centre for Justice and Crime Prevention (CJCP), under the support of the British High Commission Windhoek and UNICEF, provided data on Internet access for children, their behaviour online as well as various knowledge on Internet aspects, children's experience online and the perceived advantages as well as concomitant outcomes of the Internet, their online behaviour and insights of contrasting aspects of the Internet, children's experiences online and concomitant outcomes and recognised uses of the Internet. A projection of 68% children in Namibia were shown to have seen pornographic content they didn't want to see, while 31% submitted graphic sexual photos of people they didn't know, 29% saw sexual content involving children and 63% saw worrying or savage photos (Bhunu Shava, Chitauro, Mikka, Nhamu, & Gamundani, 2016). A framework that could be used to protect children online through societal governance was proposed, and recommendations were given on child online protection and awareness raising (Sanord, 2016).

This present research falls within the Human-Computer Interaction (HCI) domain, which consists of different disciplines. The research focuses on influencing child online behaviour. HCI is indeed a various-face field (Rozanski & Haake, 2003) that involves influencing and raising awareness of children's behaviours. Figure 1.1: outlines the scope of this research.

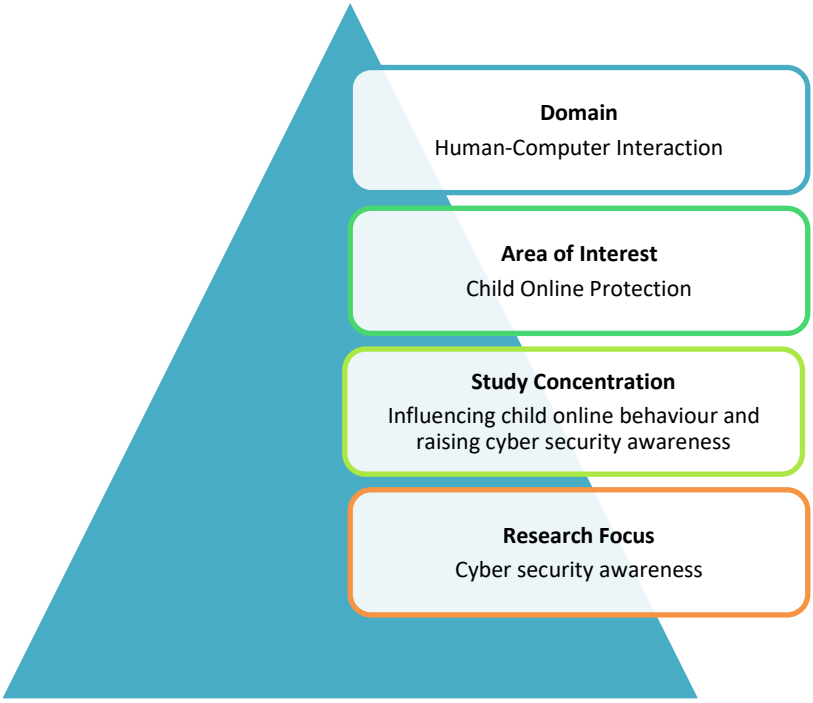


Figure 1.1: Scope of the research

This study falls within the Human-Computer Interaction (HCI) domain, with a special attention to child online protection. The research's concentration is to design an algorithm to influence children's behaviour online. Generally, children use the Internet, therefore it is important to raise cyber secure awareness, which was the research focus. This research adds a new dimension to the child online protection area, that is to influence child online behaviour and raise cyber security awareness.

1.2. Problem statement

Out of innocence, the children's behaviour likely discloses them to cyber criminals as they share information unknowingly and make friends with strangers online. The first exploratory research study on the knowledge, attitudes and practices of information and communication technology (ICT) use and online safety risks by children in Namibia was by Bhunu Shava et al. (2016). The study revealed data on Internet access for children, their behaviour online as well as various knowledge aspects of the Internet, children's experiences online and their perceived Internet benefits. In another study, a framework for addressing child online protection issues in Namibia focusing on societal governance was developed by Sanord (2016), and in another study by Maoneke Blessings et al. (2018), an exploration on the use and abuse of ICTs by teenagers in Namibia was done, that emphasised on recognising threats that teenagers are exposed to in the cyberspace. However, these initiatives towards solving child online abuses do not educate children on how to behave securely when online as they do not inform secure online behaviours. There was therefore, prior to the present study, a need for algorithms to be developed that focus on influencing children's behavioural patterns online so as to reduce their risk to cybercriminals. The following research objectives were formulated to address the above problem statement:

1.3. Objectives of the study

The following research objectives were formulated in order to provide a solution to the problem described:

Main research objective
To design an algorithm that can influence children's behaviour online in order to reduce cyber security risks

To accomplish this objective, the following research sub-objectives were formulated:

Sub-research objectives

1. *Analyse how children behave online;*
2. *Evaluate online activities that expose children's interaction with strangers; and*
3. *Evaluate behaviour analysing tools that are suitable for child online activities*.

1.4. Research questions

To achieve the above stated main objectives, the following main research questions were addressed;

Main research question

How can a suitable behaviour influencing algorithm be constituted to influence children's online activities?

To achieve the above stated sub-objectives, the following research questions were addressed:

Sub-research questions

1. *How do children behave online?*
2. *What activities specifically expose children who interact with strangers?*
3. *What are the existing behaviour analysing tools that are suitable for child online activities?*

1.5. Significance of the research

This study aimed at designing an algorithm that can influence children's behaviour online and raise their cyber security awareness. This can significantly benefit children that are introduced to this algorithm by assisting with decision making on how to behave securely online. This study is also significant to future researchers as it provides a baseline of solutions for children's online secure behaviour. Guidelines are provided on how to influence children's behaviour online, which adds to the body of knowledge.

1.6. Research limitations

The study was conducted in Windhoek only, hence contextual bias might have been introduced by the environment. However, effort was made to have participants from all socio-economic backgrounds represented in the study so as to ensure its application to all Namibian children.

1.7. Research ethical considerations

Research participants need the confidence that the materials they provide to the researcher are handled and used sensitively and responsibly (Toader , Damir, & Toader , 2010). The researcher first sought

authorisation to conduct the research from the relevant authorities at the University and line Ministries before conducting the research study. Applications for ethical clearance were submitted with the Ministry of Education, NUST's Higher Degrees Committee (HDC) and NUST's Faculty Postgraduate Committee (FPGC). In addition, research participants were provided with full information on what the research was all about, its purpose, how long the study would take, the research procedures and the expected benefits of the research study. In order for the research participants to make a free and informed consent, they were provided with full details of the research proposal, data collection tools and consent forms to ensure their right of self-determination and autonomy. Parental consent was also sought as minors were involved in the study.

1.8. Thesis layout

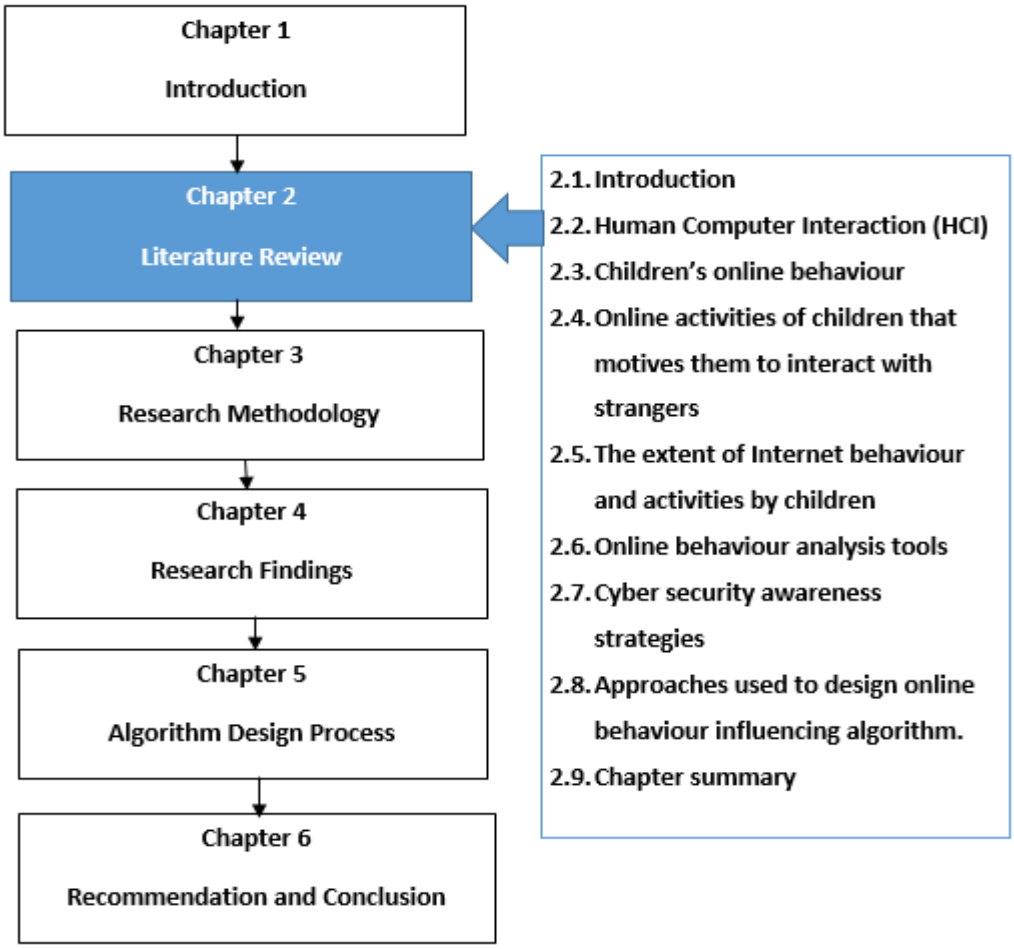
This research is broken down into six chapters. Chapter Chapter 1: introduces the study, as well as presents the entire study process by providing a summary of the importance of the problem, research objectives, research question, research scope, research methodology and potential research contribution. Chapter Chapter 2: addresses the findings of the reviewed literature according to each of the main objectives and sub-questions posed. Chapter Chapter 3: addresses the research methodology, introduces the methodological setup of the study, and justifies it. Chapter Chapter 4: addresses the findings of the research using surveys and literature collected during this research. Chapter Chapter 5: addresses the design of the algorithm and lays a theoretical structure guiding the responding process to the fourth research question. Chapter Chapter 6: completes this research by providing some reflections, lessons learnt, shortcomings of the study, recommendations and possible future research.

1.9. Chapter summary

This chapter presented the context of this study, the problem statement, objectives of the study, research questions, significance of the research, research limitations, research ethical considerations and the layout of the thesis. The next chapter reviews the available literature that is relevant to the study.

Chapter 2: Literature Review

This chapter presents a review of relevant literature to this study. The chapter starts off with an introduction, then an overview of children's online risks, online behaviour, online activities that expose them to interact with strangers and the extent of Internet behaviour and activities. Furthermore, an analysis is done on the different online behaviour analysis tools in general and the different online behaviour analysis tools that are specifically for children. Additionally, a review of the approaches used to design a behaviour influencing algorithm is done as outlined in the chapter map below.



2.1. Introduction

The Internet offers incredible opportunities by improving children's interaction, educational, and practical skills. Nevertheless, it alone cannot guarantee them a secure environment. People use technology within their social experience, but children do not have sufficient information about how to use the Internet at home or in school in their social context (Razaque Chhachhar, Qureshi, Ahmed Maher, & Ahmed, 2014).

Because most aspects in life have twofold features, there are doubts in the digital world regarding potentially inappropriate content. Various studies have shown that young users of the Internet still have limited knowledge and understanding of online security (Anderson & Jiang, 2018; Livingstone, Davidson, Batool, Haughton, & Nandi, 2017; Fire et al., 2014; Livingstone, Davidson, Batool, Haughton, & Nandi, 2017; OECD, 2012; United Nations Children's Fund, 2012).

Irregular behaviour such as cybercrime and cyber-misbehaviour have been paved by the Internet because of the way it's designed (Safa et al., 2015). The Internet is designed in a way where all users are placed on an equal footing by enabling users to communicate globally regardless of their age or identity (Safa et al., 2015). Therefore, it is important to educate both school children and young people with access to Information and Communication Technology (ICT) on how to recognise and mitigate potential cyber threats and how to be cyber-secure (Safa et al., 2015). The results from the study done by Bhunu Shava et al. (2016) highlight the potential significant opportunities, benefits and threats on the access of the Internet for young people today. Table 2.1 presents the results on what children mostly use the Internet for, the different activities they engage in and their gender. From the the table, it is evident that children mostly spend their time online playing online games, and watching online videos, movies, news or the TV. However, they spend less time online watching news, as well as reading or researching school work related information.

Table 2.1: Internet use by children

Type of platforms	Activities	Gender	Ranking
Online Games	Playing online games	Male 63 Female 52	57.5%
YouTube	Watching videos, movies, news online or TV online	Male 46 Female 43	44.5%
Internet search engines / Google	School work / Create and upload content	Male 38 Female 46	42%
Facebook, Instagram, snapshot & Tumblr	Social Networking sites	Male 35 Female 36	35.5%
Gmail, Yahoo, Ymail, Hotmail, Outlook	Sent / received messages / Read or watch the news	Male 32 Female 36	34%

In particular, the Internet has provided a new interactive forum for children that use e-mail, blogs, instant messaging, web cams, chat rooms, social networking sites and text messaging that is growing globally

(Mishna, Cook, Saini, Wu, & MacFadden, 2011). There is proof, for instance, that young people's use of the Internet is now a favoured pastime over television viewing (Mishna et al., 2011).

Child online protection is a multi-stakeholder network that involves promoting the awareness of safety for children in the online world and to build useful resources to support governments, industry and educators (The International Telecommunication Union (ITU), 2015). In order to fully provide COP, it is imperative to understand human computer interaction principles. Section 2.2 below presents the human computer interaction domain.

2.2. Human Computer Interaction (HCI)

Human-Computer Interaction (HCI) is a multidisciplinary field that deals with ways of evaluating how humans use and interact with computing devices, theories, design and implementation (Kim, 2015b). As a multidisciplinary field, HCI's theoretical origins include a diversity of other disciplines including Psychology, Computer Science, Ergonomics, and Social Sciences (Dix, 2017). The focal area for this study is Computer Science, as HCI deals with the methods that humans use to communicate with computing devices from a computer science perspective (Kim, 2015). Atanasova and Hristova (2015) define HCI as a study, design and plan between computers and humans (users). It is often considered as the interaction of computer science, behavioural science, design and many other fields of research (Atanasova & Hristova, 2015). According to Sharpe, Rogers, and Preece (2019), a good interactive design should be easy to use, effective and enjoyable. Khalil, Zahoor, and Amber (2018) outline Human Computer Interaction as follows;

- Human - the person using the device
- Computer - Hardware on which the system runs on
- Interaction - The way the user interacts, uses and communicates with the device

The present study focused on influencing children's online behaviour and to raise their cybersecurity awareness, which has the human as the focal point as they interact with devices. Information Security can be defined according to the five security services standards of ISO7498-2 standards, namely identification and authentication, authorisation, confidentiality, integrity and non-repudiation, which ensure that the information is safe and protected during its storage, transmission and use (Eloff & Eloff, 2002). The interaction of humans and devices is key to ensuring information security. HCIs are aimed at enhancing the performance, efficacy and satisfaction of users, but do not take into account the potential risks and vulnerabilities they can bring (Kainda, Flechais, & Roscoe, 2010). Human-Computer Interaction

and Security (HCISec) emerged because of the need to enhance the usability of secure systems found by Human-Computer Interaction (HCI) experts (Kainda et al., 2010) and Human Computer Interaction Security (HCISec) has adopted many HCI methods and procedures (Kainda, Flechais, & Roscoe, 2010b). According to Conlan (2005), the Human Computer Interaction Security study occurs at the intersection of HCI and information security. Studies have shown that for security to be effective, it has to be designed with the end user in mind hence it should be usable. In most platforms and online activities that children interact with, security is not the primary function and as such it may be overlooked. In addition, HCISec is designing and assessing usable security techniques (efficient, effective, and satisfying) where the human and the computer interact (Just 2016). The security and usability considerations apply to the legitimate user who has no malicious intention of harming the device (Kainda et al., 2010b) and this is presented in Figure 2.1.

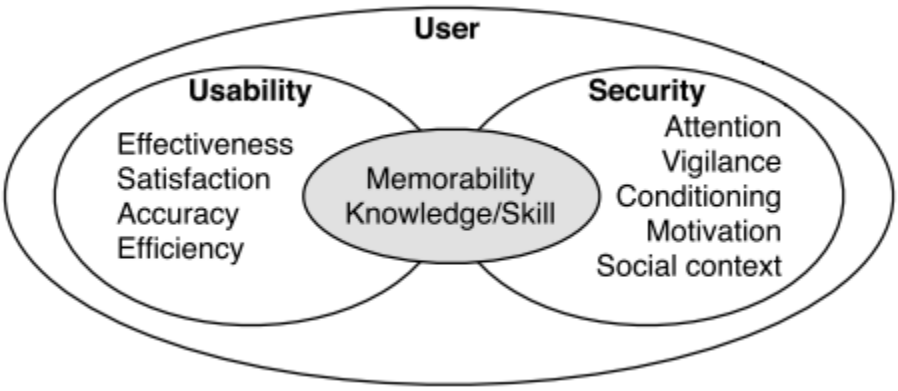


Figure 2.1: Security –Usability threat model (Kainda et al., 2010b)

For children to stay safe online, they need to be knowledgeable about the security capabilities of their devices and platforms and use them effectively. Since they primarily use devices for other purposes that are not security related, it is important that they are motivated to secure themselves because repeated exposure to security functionality and application will enable safe interaction. Human Computer Interaction and Security is widely recognised as one of the most important research areas for computer security today, and it is the development of techniques that will promote the use of security systems and make easy-to-use systems more secure (Garfinkel, 2005). User experience is an overall experience consisting of all aspects of the interaction of users with a product or service (Law, Roto, Vermeeren, Kort, & Hassenzahl 2008; Kuniavsky 2007). Knowing the wider factors affecting the experience for users is as

critical as fully understanding the cognitive science behind the behaviour of the user to build effective Human Computer Interaction systems (Kuniavsky, 2007).

The most needed feature for the digital environment is secure human computer interaction (Khalil et al., 2018). In this study, HCISec is used to assure children that the interface by which they enter their personal information will be protected against cybercrime. Moreover, Khalil et al. (2018) outline that the strength of HCISecs is to make the system stronger and more secure. Figure 2.2 presents the Human Computer Interaction Influence.

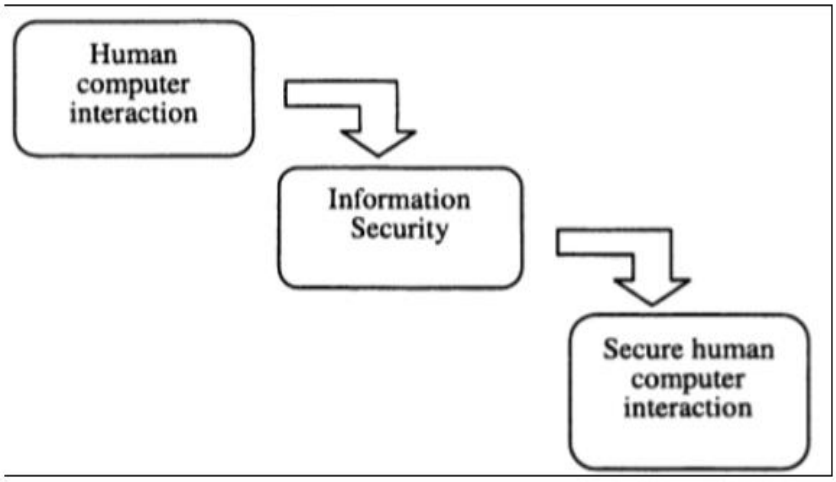


Figure 2.2: Human Computer Interaction Influence (Khalil et al., 2018)

Most security-related interfaces today offer low-level control over basic functions that could be performed by the operating system or application programme, and do not provide controls for higher-level needs of the computer user (Garfinkel, 2005). Children using online platforms may also place their lives or computer system at risk by disseminating their personal information without knowing the possible implications of online privacy (OECD, 2012).

HCI provides research clusters for cybersecurity, e-participation, big data, and community (Peters & Winschiers-Theophilus, 2017). In previous years, HCI played a vital role in every computer science student's life in universities in Namibia, and it was embedded in most of the research clusters (Peters & Winschiers-Theophilus, 2017). As such, students have been introduced to HCI programmes, and a robust HCI aspect is available for research projects (Peters & Winschiers-Theophilus, 2017).

2.3. Children's online behaviour

Children's online behaviour focuses on how children behave online. This emerges from a positivist worldview that is linked to cause and effect, where action causes a reaction in simple terms (Picciano, 2017). The present section thus outlines the supporting theories on children's online behaviour. Theory is characterised as a series of statements, concepts, or ideas that relate to a specific topic (Picciano, 2017). Typically, a theory explains, clarifies, and/or predicts phenomena (Picciano, 2017). The supporting theories on children's online behaviour are;

- **Theories of Cognitive Development:** Cognition is a broad concept that encompasses mental functions such as concentration, perception, awareness, memory, and solving problems (Johnson, 2006). Cognitive growth refers to cognitive improvements over time (Johnson, 2006). There is a growing body of research that indicates that playing video games affects certain basic brain functions and cognitive processes (Johnson, 2006).
- **Social Learning Theory:** This theory is based on the premise that in a social context, we benefit from our experiences with others (Nabavi, 2014). Children develop similar habits by watching other children's behaviours (Nabavi, 2014).
- **Social Cognitive Leaning theory:** The theory of social learning became known as social cognitive theory (Nabavi, 2014). A structure for understanding, predicting and modifying human behaviour is provided by this theory (Nabavi, 2014). It also focuses on how children and adults act on their social interactions cognitively and how behaviour and growth are then influenced by these cognitions (Nabavi, 2014).
- **Social or Observational Learning:** Behavioural researchers have debated that observational learning can be clarified by generalised imitation, conditioned reinforcement, and rule-governed behavioural processes (Fryling & Hayes, 2011). Children have been found to learn about the environment and to learn about how to solve problems directly and indirectly from the media (Fryling & Hayes, 2011).

The supporting theories on children's online behaviour are based on concepts that include mental functions, social context and observation learning. The theories highlight that cognitive growth refers to cognitive improvement over time. Additionally, in the social context, children develop similar habits by watching other children's behaviours. The behaviour and growth of the children are influenced by their social interaction cognitively and observational learning is influenced by imitation, conditioned reinforcement and rule-governed behavioural processes. The supporting theories help to identify how

children's behaviour is influenced, which gave direction on defining the objectives of a solution in this study as presented in section 5.2.3. The target children in this study were those aged from 13 to 17 years who are at the formal operation stage (12-18) of cognitive development according to the Piaget's theory (Ojose, 2008). This group of children is influenced by the behaviours of close friends and pubertal milestones (Ojose, 2008) and this supports the supporting theories of children's online behaviour. According to Johnson (2006), an increasing body of research shows that some essential brain functions and cognitive processes are influenced by playing video games. Therefore, in the present study, the designed algorithm that influences children's behaviour and raises their cybersecurity awareness was gamified.

According to Fire et al. (2014), most young people and children are uninformed of the numerous security risks posed by most Internet platforms. With little training and intelligence, children's actions potentially expose them to cybercriminals because children are innocently willing to exchange information and connections with strangers. In particular, children willingly reveal sensitive and private information about themselves that can result in cybercrimes either in their physical world or in their digital environment when the provided information ends up in the wrong hands (Fire et al., 2014). Uher (2016) define behaviour as:

> *"Something a person does that is observable, measured, and repeatable. When we define behaviour clearly, we describe specific actions."*

In the digital world, there are some questions about potentially inappropriate content because most aspects in existence have dual aspects. Young children are engaged in risky online activities such as giving strangers personal details and images, browsing inappropriate websites (racist content, violence and pornography), meeting strangers, and cyber bullying. Figure 2.3 presents the different online threats posed to children as adopted from Sharma and Advisor (2016).

Figure 2.3: Online threats to children

Although there may be many advantages resulting from digital communication, the Internet is, at the same time, a potential site for abuse and stigmatisation, whereby young people can be stigmatised by sexual perpetrators, stalkers, exploiters, and friends who bully them online (Mishna et al., 2011). Moreover, it can be argued that the greater the use, the greater the risk exposure, whether generated from conduct, contact, or content (Atkinson, Alqahtani, Stengel, & Furnell, 2017). Furthermore, most children participate in risky Internet behaviours such as surfing inappropriate websites and supplying strangers with private information and images. Livingstone et al. (2017), showed that children's and young people's use of the Internet is rapidly evolving where social, business, and technological revolution is playing a major role. The Internet use by children differs depending on the child's socioeconomic status, gender, and age and these differ according to the rate at which they access it, the device they are using, and their location (Livingstone et al., 2017). Moreover, the greater the children's Internet connectivity, the broader and more complex their Internet activities become (Livingstone et al., 2017). McAfee (2013) outlines that a quarter of children spend between four to six hours each day online and much of this Internet usage takes place away from a parent's watchful eye. Recent research has shown that the social context of Internet usage and access influence the behaviour of children online. In particular, the circumstances under which children access and use the Internet could expose them to online risks (Mascheroni & Ólafsson, 2013). This being the case, it is important to empower children to behave securely regardless of the circumstances under which they access the Internet. Section 2.4 outlines the online activities of children that make them to interact with strangers.

2.4. Online activities of children that motivates them to interact with strangers

The Internet is used for various reasons such as social media, sharing images and schoolwork, which is commonly utilised by older children compared to younger children who use the Internet for particular reasons, such as watching online videos and gaming (Livingstone et al., 2017). According to a study conducted by Phyfer, Burton, and Leoschut (2016) 86.3% of children in South Africa had a social media account, with WhatsApp getting the highest number, followed by Facebook and then Instagram. Phyfer et al. (2016) also state that from the interviews, the older children than the younger ones mostly used the Internet. Phyfer et al. (2016) also proffer that overall, more than half of the participants used the Internet for social and educational purposes, but the community, business and civic participation were far less frequent. In a recent study, children reported that social media can pressure them to post certain types of content which may lead to drama while it also helps to strengthen friendships and provides emotional support (Anderson & Jiang, 2018). There are many negative online behaviours that are practiced by children such as downloading music, programmes or other information illegally on the Internet as this is considered to be stealing according to copyright law (Al-Badi, Al Mahrouqi, Ali, Al-Badi, & Khaled Hassan, 2016). Recent reviews suggest that engaging in particular Internet behaviour may contribute to symptoms of addiction such as online gaming and online social networking, suggesting that certain Internet behaviours may be more troublesome than others (Kuss, Griffiths, Karila, & Billieux, 2014). Additionally, this means that adjusting to the increasing use of computer technology in the society may entail some changes, among other things, in how we raise children, conduct research and develop policies (Kardefelt-Winther, 2017).

Children in general develop differently according to their age stages. According to Ojose (2008), Piaget believes that a child's growth takes place through a gradual transition of thinking processes. Piaget asserts that in the various phases, children grow slowly and progressively and that the experiences in one phase form the basis for movement to the next (Ojose, 2008). Therefore, the type of online activities children perform online can be influenced by the developmental stage that the child is at. Children's levels of development and their impacts are presented using Piaget's theory as adopted from Ojose (2008) and Cacciatore and Kaltiala (2019);

- Sensorimotor stage (1-2 years): Mostly concerned with physical growth with evidence of sexual arousal in both males and females and exploring of genitals if they have a chance to.

- Pre-operational stage (3-6 years): The completed phases create a sense of confidence that carries over to relationships other than primary care, an increasing sense of independence and autonomy, and an initiative that enables interpersonal skills to be explored.
- Concrete operational stage (7-11 years): More conscious of reproduction, masturbation and sexual intercourse mechanics. Friends are beginning to play a growing role in disseminating sex knowledge and are beginning to be included in the masturbation fantasy phase.
- Formal operational stage (12-18 years): Influenced by behaviours of close friends and pubertal milestones. The child actively explores possibilities for identity, where sexuality and gender identity are central. Intimacy, the core component of adult life, is made possible by effectively overcoming the identity crisis.

In this study, the target children were those that are 13-17 years old, and according to Piaget's theory, they are at the formal operational stage (12-18) of cognitive development (Ojose, 2008). The behaviours of close friends and puberty milestones affect this group of children (Ojose, 2008). The designed algorithm focuses on influencing children's behaviour on social networking sites by promoting secure online behaviour through reward and penalties. It focuses on raising Internet security awareness and educating the child on secure online behaviour as a way to achieve secure online experience.

Namibia is still at its infancy in providing child online protection, and as such, the present study adds to current efforts by raising children's cybersecurity awareness and enhancing secure online behaviour. Section 2.5 below outlines the extent of Internet behaviour and activities by children.

2.5. The extent of Internet behaviour and activities by children

Question one: *How do children behave online?*

Question Two: *What activities specifically expose children to interact with strangers?*

The effects of this exposure on the actions and wellbeing of children is the harvesting of private information such as gathering private information to tailor online ads to a user's profile or even exchanging private information on the Internet through companies or social networking websites (Fire et al., 2014). This can result in teenage harassment and bullying in the United States of America (Anderson, 2018), and online grooming and recruitment of young children for prostitution (Hillman, Hooper, & Choo, 2014). Moreover, Maoneke et al. (2018) further outline the online risks such as child online abuse and stigmatisation. Furthermore, Kardefelt-Winther (2017) allude that the use of digital technology impacts

the mental well-being of children, their social interactions and physical activities as well. These factors then led us to further investigate on the Internet activities and the behaviours of children that expose them to cybercrimes.

In this section, we present the outcomes of the explanatory variables of interest which are online child activities, online child behaviour, online exposure and cybercrimes which are listed in Table 2.2 as adapted from Kahimise and Bhunu Shava (2019).

Table 2.2: Child online activities, online behaviour, exposure and cybercrimes (Source: Kahimise & Bhunu Shava, 2019)

Author (Year)	**Child online activities**	**Child online behaviour**	**Exposure**	**Cybercrimes**
(Livingstone et al., 2017)	Watch videos 59%, 56% Listen to music, 54%, play games 47%, complete homework 47%, interact with family and friends 40%, social networking 38%, information look up 27%, and photos and videos upload and music 27%	Children utilise the Internet to encourage and promote kindness and respect	Add contacts they don't know on social networking sites, or sent pictures they regret now, or disclose private data to strangers online	Self-harm, violence, bullying and sexual abuse, digital identity theft
(Fire et al., 2014)	Children visit social networks online, including Facebook, Google+, LinkedIn, Sina, Weibo, Twitter,	On Facebook, children have been shown to accept requests for friendship from people they don't know but just have several friends with	Many children expose personal and intimate details about themselves, their friends and their relationships	This information exposes them to theft of identity, malware, false profiles and sexual harassment

	Tumblr and VKontakte			
(Bhunu Shava et al., 2016)	Watching Internet videos, films, or TV, school work, social networking sites, and seeking data about health	Sharing data on the following; hobbies (61%), school details (60%), real name (53%), and age/date of birth (51%), with the least likely to be shared being details of parents' bank details (2%) and other details of parents (4%), home details (11%)	Lie on the Internet about their era (e.g. when establishing an account, accessing certain websites, or meeting someone online). That leads to Internet harassment and abuse	Violent content that they didn't want to see, had someone stalked them, hacked data and asked for sexual pictures. Pornography, phishing and sexual intercourse
(Phyfer et al., 2016)	Social networking sites (WhatsApp, Facebook and Instagram)	Children are vulnerable to seeing sexual images online and meeting strangers online. They are directed to X-rated online sites with links and advertisements that they did not want.	Many children were comfortable in their technological skills, claiming that they learned a lot of things online and that they understood Internet more than their parents did.	Online bullying and limited access to resources. Exposed to hate speech photos and gory videos.
(Anderson & Jiang, 2018)	Social networking websites	Children immediately interact and share their life through status updates, photos and videos online	Post on their successes, their friends, share their thoughts and emotions, post on their love lives, and share their personal or spiritual opinions	The large number of teenagers (90 percent in this case) agree that online abuse is a problem that affects children their age. They present themselves in the same manner of drama and fear or

				pressure they are exposed to
(Kardefelt-Winther, 2017)	Playing online games, visiting social networking websites, and chatting online	Children investing quite enough time on the Internet could have a negative effect on their well-being		The use of the Internet could re-draw the minds of children or hijack them
(Santisarun & Boonkrong, 2015)	The very first thing children do is review their social media site's (Facebook) newsfeed every time they turn on their smart phone or computers.	About 52.5 percent of children shared their cell phone number online, and 35 percent shared their real home address. Furthermore, out of 35 percent, 14 percent of those sharing their home address were simply primary school students who did not know that their shared photos or photographs were geo-tagged automatically	School children acknowledged welcoming strangers into their Facebook profile and exchanging private details at all times	An opponent can use the shared information to impersonate or track that specific user through personal data and geo-tagging
(Atkinson et al., 2017)	Myspace accounts and Facebook are used by a 65% of European kids.	Movies or music downloads. Video clip viewing (e.g. on YouTube) online. Attaining your own social networking profile. To share with others, upload images, videos, or music.	Parents' lack of consciousness can mean that their Internet exposure has an unintended negative effect on children. Children will face severe hazards and become victims of the Internet if no	As well as unwanted or potentially harmful contact such as abuse and online predator grooming, online racial hateful material of child pornography.

			protective policies are enforced.	
(Broughton, 2009)	Facebook and Myspace social networking website	Children with low self-esteem, poor relationships with family members or who feel unpopular may be particularly at risk of forging such relationships in the relative 'security' of the Internet. Young people often take offensive photographs or even videos of themselves or friends or make outrageous comments just to feel a sense of belong	Children also placed very private information on their blogs or exchange substantial information in other online platforms	Chat rooms are also used by abusers as a mechanism for meeting vulnerable young people to sexually assault
(Hillman et al., 2014)	Visit websites for social networking	Respondents between the ages of 13 and 19 reported sending or sharing their own nude or semi-nude photographs to someone they only met online	Children may often engage in illegal activities, such as talking or sending photos or videos of themselves (an activity also referred to as 'sexting')	Cyber criminals sweep through social networking sites and then draw and groom women into their prostitution business (children's sexual abuse)
(Livingstone, Kirwil, Ponte, & Staksrud, 2013)	Gaming, social networking sites, blogs and YouTube video sharing sites.	Sharing their parents' private data online and buying stuff back online. Visit the game website and click on the action games to	Most kids are concerned about web content that is violent, violent or gory. In seeing brutality, killings, animal abuse	Collecting data from children to post violent and aggressive content online. Cyberbullying,

		see the Alien vs Predator trailer. It was a lot of blood, gory and upsetting. Children spend so much time on the internet	and even on the news, they express horror and indignation when much is real rather than fictional crime, which adds to the depth of children's responses	sexting, gory Internet content, pornography
(Tennakoon, Saridakis, & Mohammed, 2018)	Social Networking sites	Clip and photo sharing, online games and contact with both known and unknown people online	Sexual violence, cyberbullying and exposure to violent content online	The improved online communications and heavy use of online media expose vulnerable individuals and young children to hazards such as cybercrime
(Magkos, Kleisiari, Chanias, & Giannakouris-salalidis, 2014)	Online Social Networking (OSN)	Befriending strangers, exchanging details and offline meeting them. Exchange of sexual messages or other content (such as images, videos)	Insufficient material and interactions, addictions to the Internet, psychosocial deviation, loss of personal or confidential data	Malware, phishing, identification and information theft, hatred, abuse, racism, gambling, alcohol and suicides, anorexia / bulimia
(Zucule De Barros & Lazarek, 2018)	Social networking	Kids who visit websites that offer harmful content	Children read notifications such as violent or gory material, pornographic material, hateful racial content and embedded ads. Kid with cyberbullying involvement	Cyberbullying, child pornography and identity theft

(Maoneke et al., 2018)	Social networking, watching movies, playing sports, researching health issues and doing school work, among other things	Internet friendship with strangers and the sharing contact details with strangers	Online violence, demanding someone's private data, and then electronically sharing the data with others without permission, impersonation, cyber-stalking, and human sexting	Child porn, online bullying, online sexual harassment and harassment remain inaccessible in Africa

In general, we found from the study that most children spend most of their time on social networking sites, thereby making them more likely to be exposed to cybercriminals and having less time to do other potentially more satisfying things. We have also found clear evidence that children prefer to share personal details and embracing connections they don't know without having to know that they may be exposed to cyber risks. Cyberbullying, sexual assaults, impersonation, online sexual harassment and access to inappropriate content are the threats associated with various activities online. Children have indicated that they can be themselves online and use the Internet to foster respect and kindness and inspire them (Livingstone et al., 2017). Broughton (2009), however, notes that the severity of the issue is that kids with low self-esteem and bad relationships with family members can pose a particular risk of forging those relationships through Internet convenience. Children often put offensive images or videos of themselves or friends just to get Internet recognition and approval (Broughton, 2009). Anderson and Jiang (2018), also describe children posting on social media about their successes and their families, expressing their emotions and thoughts, posting about their dating lives and personal problems or religious or political beliefs. Therefore, we found that sexual harassment, cyberbullying and exposure to violent content was the usual exposure of children to the Internet. It is mentioned in a study by Hillman et al. (2014) that cyber criminals go through social networking sites and attract and groom children into their prostitution institutions. In fact, cyberporn is now available in a number of ways, such as pop-up advertisements, blogs, searches on the Internet and emails (González-ortega & Orgaz-baz, 2013).

Table 2.3 presents a review of papers on social networking sites, social networking threats and solutions on social networking threats.

Table 2.3: Social networking sites, threats and solutions (Source: Kahimise & Bhunu Shava, 2020)

Author (Year)	Social networking sites	Social networking threats	Solutions on Social networking threats
(Nakerekanti & Narasimha, 2019)	LinkedIn, Facebook and Twitter	• Viruses/worms/Trojan horse • Spam • Adware and Spyware • Keyloggers • Ransomware • Browser Hijacker • Crimewares	• Ordinary Data Backup • Client mindfulness • Principles in Intrusion Prevention Software (IPS) • Rogue security software
(Soumya & Revathy, 2018)	Facebook, Tweeter, Instagram and YouTube	• Phishing attacks • Spamming • Stalking • Fake attack on profile • Attack on Location Leakage • Attack on Account Compromise • Click jacking • Cross Site Scripting • Applications of malicious codes	• Guard against spams • Use websites that are trusted • Pop ups alert • Spam filters and Firewall • Bot unfriendly questions and use of CAPTCHA • Unwanted contacts block • Avoid auto-follow • Profile privacy and Disable geo tagging • Avoid strangers and report stalkers • Social account auditing • Analyse red flag words
(Tarun, 2017)	Facebook, Twitter, Pinterest, Reddit and Instagram	• Facebook depression • Social anxiety of stress • Catfish • Cyber bullying • Cyber terrorism • Human trafficking • Cyber drug dealing	• Ensure social media understanding and evaluation of what's happening in the world awareness constantly

(Kirichenko, Radivilova, & Anders, 2017)	Facebook, YouTube, Twitter, Vine Camera, Ask.fm, Pinterest, Tumblr, Flickr, Google+, LinkedIn, VK, ClassMate and Meetup	• Social engineering • Possibility of substitution of person or masquerade • Stealing passwords and phishing • URL shortening service usage • Using the same usernames and credentials on the external social resources and company network • Internet attack • Leakage of data • Induction of minors for sexual purposes (grooming) • Content with signs of incitement to racial, ethnic or religious hatred, propaganda of totalitarian sects • Public justification of terrorism and propaganda • Cyber humiliation and cyber bullying • Promotions and distribution of drugs	• Special software to monitor and analyse the social networks
(Trivedi, Dave, & Sridaran, 2016)	Facebook, Google+, LinkedIn, Twitter, Tumblr and VKontakte	• Phishing attack • Spammers • Stalking • Attacks on fake profile • Attack on Location Leakage • Compromise Attack account	• Social authentication based trustee • Adversarial Model • Change privacy & security setting • Installation of Internet security software • Disable installed third-party tools etc. • Authentication, security and privacy mechanism • Internal protection mechanism • Report users • Education building • Cyber defence access control and authentication systems • Appropriate settings of defaults
(Nalinipriya & Asswini, 2016)	Facebook, MySpace, Twitter, LinkedIn, Watsapp, socialight, Dodge ball	• Internet abuse, spammers, SQL injection, malware, Cross-site scripting, phishing attacks • De-anonymization attacks, Fake Apps, Socialbots, Doxing, Spoofing, Baiting, Plug-in Scams,	• Watch dog and social enabler • User-control • Structural anomaly detection

		Click-jacking, Elicitation, Like-Jacking, Pharming, Identity-clone, Phreaking, Identity Theft, Spoofing • Cyber-bullying/stalking, cyber harassment and digital predators	• Virtual individual servers • Reputation mechanisms • Proxy-based protection
(Wang, 2015)	Facebook, Flickr, Twitter	• Malware exposure • Data loss • Attacks on Phishing • Attacks on social engineering • Attacks on Inference • Attacks de-anonymization attacks • Spam • Attacks on Sybil	• Social spam detector • SybilGuard • SybilLimit • Naïve Bayes algorithm
(Fire et al., 2014)	Facebook, Google+, LinkedIn, Sina Weibo, Twitter, Tumblr and Vkontakte, MySpace	• Privacy risks • Identity theft • Malware • Attacks on Phishing • Spammer • Cross-Site Scripting (XSS) • Web fraud • Clickjacking • De-Anonymization • False profiles/ Socialbots • password Clone Attacks • Inference Attacks • Information Leakage • Location Leakage • Socware • Sexual harassment	• Solutions on Internet Security • AVG privacyFix • FB phishing defender • Norton secure web • McAfee Social security • MyPermissions • NoScript safety Suite • Facebook Privacy scanner • Defensio • ZoneAlarms privacy scanner • Net Nanny • MinorMonitor • Enhanced privacy interfaces settings • Phishing Detection • Clone profile detection • Fake profile detection • Socware Detection • Preventing Information and Location leakage
(Sadeghian, Zamani, & Shanmugam, 2013)	Facebook	• Phishing • Short URLs • Identity Theft • Malicious Third application • Spam • False Users • Redirects Legitimate look	• URL security tools • Privacy adjustment • Application access level adjustment • Limited sharing • Thinking twice before performing any action in social

			networking environment
(Ghari, 2012)	Friendster, MySpace, Facebook, Twitter, Hi5, Youtube, Flicker, Netlog, Orkut, Xianonei, Xing, Mixi, Badoo, Bedo, Skyrock, Ployaheod, Odnoklassniki.ru. V Kontakte, Digg	• Social engineering • Spammers, phishing and malicious attacks • Theft of identities • Defamation • Stalking • Personal dignity injuries and cyber harassment • Impersonation	• Encouraging awareness • Modifying existing legislation • Enable authentication • Using the most powerful antivirus tools • Providing appropriate security tool
(Nuha, Molok, Chang, & Ahmad, 2010)	Facebook, Twitter	• Risk of malware • Net Reconnaissance • Spear-phishing • Aurora attacks • Advanced persistent threat or cyber industrial espionage	• Information Security Policy • Safety Education, Training and knowledge • Preventive Security Systems
(Hasib, 2009)	MySpace, Facebook and others	• Digital personal information dossier • Face Recognition • Content-based Image Retrieval • Image Tagging and cross-profiling • Complete Account Deletion difficulty • Spamming • Cross-Site Scripting, Viruses and worms • SNS Aggregators • Phishing • Information Leakage • Identity theft profile squatting • Stalking • Corporate Espionage	• Encourage awareness-raising and education programs • Reviewing and reinterpreting the regulatory framework • Promoting better encryption and access-control where appropriate • Setting acceptable defaults • Providing appropriate security tools
(Luo, Liu, Liu, & Fan, 2009)	Myspace, Facebook, Bebo, Orkut and Friendster	• Spam attack • Worm attack • XSS attack • Plug-in attack • Phishing	• Personal information protection • Install patches • Classify users • Spam block • Filter suspicious links • Notify security alerts • Detection of vulnerability • Anti-virus detections • Transmission encrypted

In particular, from the analysis we found that most of the common threats on social networking sites are phishing, social engineering, spamming, cyberbullying/cyberstalking, data leakage and malware attacks. Phishing is a major Internet problem and social networking challenge (and malware) and distributed phishing links are becoming increasingly common (Watters, 2011). Sadeghian, Zamani, and Shanmugam (2013) outline that, a phishing attack can happen when a user clicks on a URL that forwards the user to a phishing webpage which could be a fake Facebook account. So the user assumes that his/her session has ended and he/she may try to log in to see what they have been watching, but then signs into the false page, and his/her username and password will be sent to the hacker (Sadeghian, Zamani, & Shanmugam, 2013). Increasingly, social network websites are also being used for phishing attacks that are designed to obtain bank or credit card details (Hunter, 2008). Because the number of social networking sites is increasing, spammers use different techniques of spamming to gain benefits. Spam on social networking is more effective than spams that are distributed over the email due to social connections in social networking sites that generate trust (Soumya & Revathy, 2018). Malware developers use many common social networking sites to infect worms with huge user data networks (Nakerekanti & Narasimha, 2019). Apart from all the short comes that social networking sites may have, there are few advantages it may have, organizations may engage in social media intelligence to control the spread of false news, identify the sources that spread the information and, if appropriate fight back with legal action (Bizzi & Labban, 2019). Schools are a promising place for the use of social networking sites, and some learners at school have used social networking sites to target specific pupils or to spread gossip and speculations against these pupils (Weir, Toolan, & Smeed, 2011). The existing solutions from literature can mitigate the threats of phishing, spamming, cyberbullying and malware in social networking platforms. .

Table 2.4 presents the solution against common threats in social networking sites based on literature.

Table 2.4: Common social networking threats and solutions

Common Social Networking threats	Solutions on Social Networking Threat	Source/s
Phishing	Firewall and spam filters, Using trusted websites, URL safety tools, Limited sharing, Building self-awareness about social networking threats, Profile privacy settings, Facebook phishing protector, phishing detection	Soumya & Revathy (2018); Trivedi et al. (2016); Sadeghian et al. (2013);

Spamming	Firewall and spam filters, Prevent unwanted contacts, Stop auto-follow, Privacy settings on profiles, Spams protection, Use of trusted websites, Attention to pop ups, URL safety tools, Limit sharing, Building self-awareness on social networking threats, social spam detector, block spam	Trivedi et al. (2016); Sadeghian et al. (2013); Wang (2015); Fire et al. (2014); Ghari (2012); Al Hasib (2009); Luo *et al.* (2009)
Cyberbullying/ cyberstalking	Geo tagging disable, Limited sharing, Privacy settings on profiles, Avoid strangers, Report stalkers, Social account audit, Red flag words analysis, Block unwanted contacts, Proxy-based protection, Watch dog and social enabler, Building self-awareness about information disclosure, protect personal information	Nalinipriya and Asswini (2016); Al Hasib (2009)
Malware	URL safety tools, Firewall and spam filters, Awareness, Mechanisms on cyber defence, anti-virus detection, vulnerability detection, notify security alerts	Wang (2015); Fire et al. (2014); Sadeghian et al. (2013)

More particularly, Internet exposure to children contributes to Internet addiction, which in turn can change the development of the adolescents' brain structure, leading to low academic results, participation in unsafe activities, harmful nutritional habits, low personal interactions and self-injurious activities (Al-Badi et al., 2016; Ramos-Soler, López-Sánchez, & Torrecillas-Lacave, 2018) The key features of a cautious person on the Internet is characterised by a good awareness of online risks such as not spending too much time on the Internet, avoiding dangerous conduct, talking to parents about Internet problems, getting advice and having specific rules on Internet use. Table 2.5 presents online activities for Internet safety that can be integrated into the designed algorithm as a behaviour influencing content (Juhari & Mat Zin, 2013).

Table 2.5: Internt activities categorised by the guidelines for Internet

Activities	**Guidelines**
Playing online games	• Be wary of stranger • Get parents' permission to meet online friends • Ignore insulting messages and report to parents

Watching videos, movies or TV online	• Children to confirm parental regulations and rules • Report inappropriate web content upon finding out • Ignore popups
Internet surfing	• Children to confirm parental regulations and rules • Report inappropriate web content upon finding out • Ignore popups
Social networking	• Do not add strangers • Safely guard personal information • Picture sharing to close friends should be limited • Once you have written something you cannot delete it.
Chatting	• Be wary of stranger • Parents' permission is required to meet online friends • Ignore and report insulting messages to parents • Once you have written something you cannot delete it.
Online Purchasing	• No purchasing without parents' consent
Email	• Do not open emails from strangers • Scan emails that contain file

Section 2.5 outlines the extent of Internet behaviour and activities by children. Children's online activities and their online behaviour unknowingly expose them to cyber threats. This shows that most children have less knowledge on how to behave securely online. Therefore, it is important to influence children's online behaviour and raise their cyber security awareness as soon as they start using the Internet. There are many existing tools online that can be used to analyse and influence children's behaviour online. Section 2.6 outlines the different existing tools that can be used to influence behaviour online, which may help to formulate the design of the algorithm.

2.6. Online behaviour analysing tools

Question Three: *What are the existing behaviour tools that are suitable for child online activities?*

The best approach to influence and analyse behaviour online would be through tools, and below is a table presenting online behaviour analysis tools in general, their strengths and weakness and if the tool is applicable to influence the behaviour of children online. Table 2.6 presents the online behaviour analysing tools.

Table 2.6: Online behaviour analysing tools

Tool	Strengths	Weakness	Applicability of tools to influence children's behaviour online	Source
Webminersystem	• It is a tool that is used to mine information on the browsing and access patterns of users. • It uses server access logs to automatically discover association rules and sequential patterns • Uses an algorithm to find maximal forward reference sequences • It uses cookies, cache busting, and explicit user registration to record all important access	• All log entries with filename can be removed • May not record all the important access data • Users may delete sookies • The Cache busting can be disabled • User registration is voluntary which can provide false information	Yes	Cooley, Mobasher, and Srivastava (1997)
E-Web Miner	• Web content analysis • Web structure analysis • Web usage analysis • Web log analysis • It uses an AprioriAll Algorithm	• It only mines for web content, structure, logs and usage.	Yes	Yadav (2012)
SysProf	• Offers a flexible framework for monitoring individual activities at granularity • Dynamically configurable runtime capture of data monitored in order to enable tradeoffs between the granularity, overheads, and delays of runtime diagnoses	• Could be costly	No	Agarwala and Schwan (2006)

	• Generate dynamic code, binary encodings for monitoring data, low overhead kernel-level public- subscribed messaging and efficient event hashing • Low perturbation and high performance for low granularity • Diagnoses and Improves runtime client requests scheduling • Bottlenecks in proxies are dynamically detected			
Monitoring and Analysis Tool for e-Learning Platforms (MATEP)	• Used to monitor and analysis e-learning • Tool is very convenient works at any-time and anywhere • It uses a collaborative tools that support different styles of learning	• No direct interaction between teachers and students	No	Zorrilla and Alvarez (2008)
Visualizing Video Clickstream Data from Massive Open Online Course (VisMOOC)	• To help analysis learning behaviours of users, a Video clickstream data from MOOC platform is used (visual analytic system) • Analyses student access and their activity patterns • Analysis of student interaction in forums • Analysis of student performance in their assignment and exams • Simple visual design • Video embedded design • Multi-level scale exploration • Multi-perspective exploration	• No direct interaction between teachers and students • Content of videos may be big • The length of videos may be too long • The release time of videos • The number of videos released in one week may be many	Yes	Shi, Fu, Chen and Qu (2015)

Pin	• The design of Pin emphasises ease of use, portability, transparency, efficiency and robustness. • Uses a Just-In-Time (JIT) compiler to insert and optimise the code. • Pintools include profiles, cache simulators, trace analysers and memory bug checkers. • It writes portable instrumentation tools by abstracting away the underlying instruction set features	• Its open source • Only runs in Linux	Yes	Luk Robert Cohn Robert Muth Harish Patil Artur Klauser Geoff Lowney Steven Wallace Vijay Janapa Reddi and Hazelwood (2005)
SecureString 3.0	• Emphasises on authenticity, integrity, privacy, resilience and blacklisting of harmful words • A abolishment of ciphertext repetitions • Facilities blind computing on encrypted character string through an untrusted host.		Yes	Fahrnberger and Heneis (2015)
Secure Whitelisting of Instant Messages	• Is a technique developed to scans instant messages and only forwards those with solely harmless words to their destination • Emphasises on authenticity, integrity, privacy, resilience and payload confirmation (whitelisting)		Yes	Fahrnberger and Heneis (2015)
Webalizer	• It is known for web analytics activity • Its current version 2.13. 1 • It is very easy to install • Supports 30 languages • Runs on cross-platform operating system • The log files it analysis are CLF, XLF, ELF and FTP • Its capable to handle regular schedule activities because of its in-built features	• Produce statistics that do not discriminate the number of visits between human and robots	Yes	Kundu and Garg (2017)

	• Reports are created automatically on a daily basis. • Automatically create respective reports			
Piwik	• It's a web analytic tool • Used for log files that contain massive amount of data • Current version is 2.13.1 • It's not difficult to install • Its own interfaces are built in using python language • Works on cross-platform operating system • It supports plug-in explore reporting format of log files like Apache and IIS	• Users are the only people who see their own data • Provide limited details only	Yes	Kundu and Garg (2017)
Open Web Analytics	• It a weblog analyser tool • Available in PHP language • Works on cross-platform operating system • Current Version is 1.5.7 • Easy to install • Provide click stream information • The site visited , the path followed in the web pages and the time spend on each page is determined by analysing of click stream	• It's a server software anyone can run and install on their own host	Yes	Kundu and Garg (2017)
Fire Stats	• It's a web statistic system • Used to interpret the cookies in the log files such as CLF, XLF and ELF • Its current version is 1.6.7 • Trouble free to install • Its available in PHP, MySQL 4.0.17 languages • Works in Window/ Unix operating system • It separates the instructions for each content based system by extracting the information of source file retrieved by the end users	• Only basic details are provided	No	Kundu and Garg (2017)

Google Analytics	• It's a web analytics provided by Google as a free utility tool • Supports CLF, XLF, ELF with unlimited size • It is used to trace log files • A report of detailed information is provided which helps in examining the guests traffic	• Does not work on Raw logs. • Importing Raw logs is missing	Yes	Kundu and Garg (2017)
SafeChat 2.0	• Designed to work with AIM Instant Messaging that uses a protocol called Open System for Communication in Real-time (OSCAR). • A detection algorithm is used to classify chat participant as potential predators. • It's a third party plugin for the Pidgin (most popular open source instant messaging) • It works on any Windows or Unix-based environment • Supports multiple protocols including AIM, MSN, ICQ IRC and Yahoo • Unsupported protocols e.g. Facebook Chat, can be used in Pidgin with the use of third party plugins • it uses XML file system to keep track of all of the users' interactions • Uses a rule-based approach to detect predators • Uses WinpCap library have control over the transmission and retrieval of packets in windows environment	• The age function may misidentify the age of a potential predators • Does not contain filters that blocks or filter prohibited terms in messages before it reaches the receiver	Yes	Thom, (2011)
Butterfly software	• Chat room monitoring and analysing software • It identifies a suitable chat group based on user-defined parameters	• Multiple conversations occur simultaneously in chat rooms that makes it hard to	Yes	

	• The main focus is on Internet Relay Chat (IRC) • Uses ChatTrack tool to detect and prevent potential threats in the chat room. • Uses a keywords based approach to input types of interested channels by users of the agent • Builds term vectors of occurrence counts of keywords from conversations then uses these term vectors to recommend a chat room based on the users' requirements • Uses a cognitive modelling approach for the language interaction detection which is similar to signature based intrusion detection methods	determine member of each conversation • One needs to first have knowledge of who is communicating in the chat room		Penna, Clark, and Mohay (2005)
NetNanny	• It's an Internet filtering tool • Each time you browse the Internet and in real time the netnanny will review the content of any website visited • Uses an Internet filter that can distinguish between the use of the terms • Detects the contextual usage of words and will either allow or block a website based on the preferences customized for each individual user	• Hasn't been patched for many years now and it hasn't taken care of any bugs and improvements it needs to make. • No tracking features • The specialized screen time control settings are also missing. • It does have minimal features for the iOS phone. • No text tracking feature or call tracking. • lacks control of the social media site.	Yes	Dawson, Burnett, and McArdle (2005); Nanny (2002); (Walsh, 2020b)
Qustodia	• Extensive reporting, pornography block, screen time balance, games & app access,	• Costly. • In desktop browsers, VPN breaks web filter.	Yes	(Rubenking & Moore, 2020b)

	YouTube tracking, social network activity view, Android track calls & SMS, family locator and Android panic button	• Tracking social media limited to Facebook.		
Kaspersky Safe Kids	• Affordable • No restriction on equipment or child profiles • Flexible computer- and app-use power • Durable web filtering • Geofensing • Wide alerting system Share expert device and tips from child psychologists on online topics	• Several drawbacks to iOS • Filtering of the web restricted to different browsers • Online tracking deals only with Facebook and VK • Low Web interface	Yes	(Rubenking & Moore, 2020a)
Norton Family	• Affordable • Good dashboard on the web • No limit for number of devices being monitored • Fast installations and setups	• Does not run on Macs • No geofensing • Time limits apply per machine • Tracking of social media lackeys	Yes	(Rubenking & Moore, 2019)
Mobicip	• Protect your family on the Internet, limit screen time, manage apps & track location with the best parental control software	• Compared with Web edition, the Mobile Interface is limited. • Some contact issues and delays between the online console and the local device occurred during testing. • Requires two downloads to the app. • No monitoring, blocking your call, or blocking your email.	Yes	(Rubenking & Minor, 2016)
McAfee	• See what you kids are up • Set rules and time limits for apps and websites	• Slows down the system • Costly	Yes	(Whiting, 2020)
KidsGuard Pro	• Very quick to install • Operates in stealth mode • Installation does not require rooting or jailbreaking of the apps.	• There is no free trial • Only one device can be monitored at a time	Yes	(Walsh, 2020a)

	• multilingual assistance • Packed with over 30 exciting apps • It can monitor the WhatsApp, Facebook, Screenshots and so on activities. • Tracking position in real time functionality. • This operates on all versions of Android and iOS (including the most recent ones).	• The functionality of iOS devices is very minimal (no remote control features		

From the analysis presented in Table 2.6, there are many existing behaviour analysis tools in general that could be applicable to children, however, there are four tools that interested me more, which are (i) VisMOOC because it analyses the behaviour of users, analyses what they access and their activity patterns (ii) Web miner that mines for browsing information and access patterns of users (iii) Webalizer that is also used to analyse online activities, and (iv) E-web miner, which uses an algorithm that mines for web content, web structure, web logs and web usage. In addition, there are many online behaviour analysis tools that focus on influencing online behaviour. Figure 2.4 presents the online behaviour analysis that can be integrated into the designed algorithm as a behaviour influencing content.

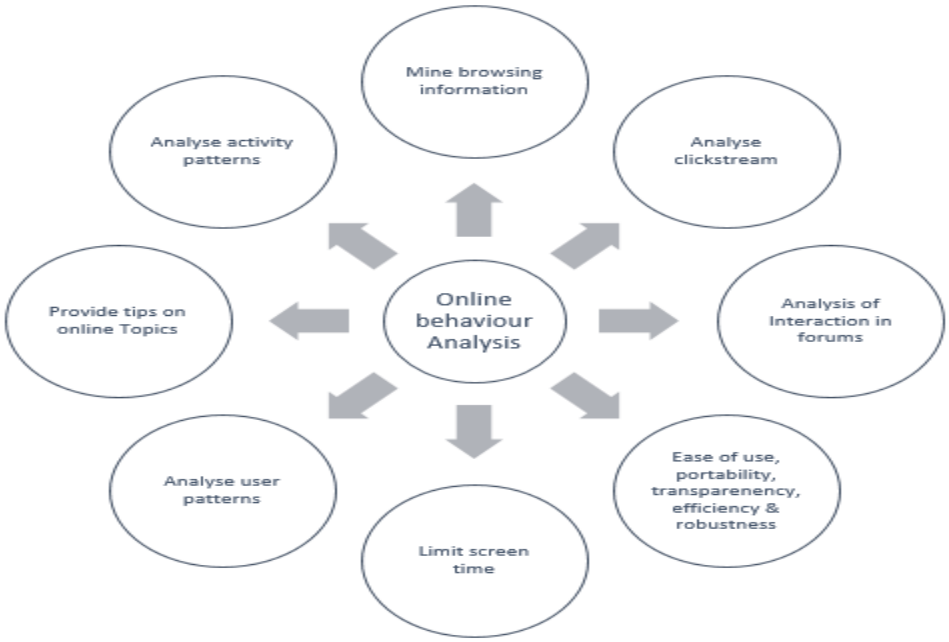


Figure 2.4: Online behaviour analysis

From the summary in Figure 2.4, the existing online behaviour analysis tool analyses online behaviour by analysing clickstream, interactions in forums, user patterns, activity patterns, and limiting screen time by providing tips on online topics and mine browsing information. However, tools such as SysProf, MATEP, Piwik, Open Web Analytics, Free Stats, Google Analytics, SafeChat 2.0, Net Nanny, Qustodia, Norton Family, McAfree and Kids Guad Pro emphasise more on managing apps, tracking, filtering content, detecting predators, etc. Such emphasis however has nothing to do with influencing online behaviour but has to do with the prevention of online threats. Some of the metrics like time spent online were measured in this study to gauge its impact on cybersecurity threat exposures for children. Providing tips was used as an empowerment tool to raise cybersecurity awareness on the gadget, platform, activity or environment specific threats. This study sough to raise cyber security awareness among children and as such, section 2.7 presents suitable strategies for cyber security awareness in children.

2.7. Cyber security awareness strategies

Cyber security is the protection of inter-connected devices namely hardware, software, and data from cyber threats and this can be achieved through methods that are technology, procedure or human focused (Sundaresan, 2018). Security, which is intended to protect data confidentiality, integrity and availability, is a sub-set of cybersecurity (Sundaresan, 2018). Human measures include cyber security education, cyber security training and cyber security awareness (Wilson, Hash, & Division, 2003). Cybersecurity awareness is intended to allow people to identify and respond accordingly to IT security concerns (Wilson et al., 2003). It can be achieved by developing the awareness and training material and implementing the programme. The methods and strategies in raising cyber security awareness are:

- Applying game dynamics to non-gaming situations in order to induce interest and raise motivation levels, and elements of this can be extended to keep a user interested in learning (Scholefield & Shepherd, 2019).
- A wide variety of public options (i.e. websites, booklets, information graphics, blogs, posters, video clips) are useful resources for raising security awareness levels (Kovacevicˇ & Radenkovic, 2020).
- Applying serious games, that is games with an intent other than pure entertainment (Hendrix, Al-Sherbaz, & Bloom, 2016). In areas such as healthcare, advertisement, and behavioural change, serious games have gained growing interest (Hendrix et al., 2016). Studies have shown that not only can games be efficient teaching tools, but they can also be efficient tools to encourage behavioural change (Hendrix et al., 2016).

Measures that generate the greatest possibility of success in cybersecurity awareness include the use of creativity in content distribution and participatory experiences (Peker, Ray, Silva, & Gibson, 2016). The cybersecurity methods, strategies, framework, and models that can be applied to children are presented in Table 2.7.

Table 2.7: Cybersecurity methods, strategies, frameworks, and models for children

Cybersecurity exiting frameworks/models/strategies that can be applied to children	**Framework/model/ strategies focus area**	**Source**
NIST Cybersecurity Framework (CSF)	Identify; protect; detect; respond; and recover	Calder (2019)
Cybersecurity Strategy	Risk identification; vulnerability reduction; threat reduction; consequence mitigation; and enable cybersecurity outcomes	U.S Department of Homeland Security (2018)
Guidelines for Industry on Child Online Protection	Integrating aspects of children's rights into all relevant organisational policies and management processes; The establishment of standardised guidelines for the handling of materials for child sexual exploitation; establishing an online community that is more secure and age-appropriate; Educating children, parents, and educators about children's protection and responsible use of ICTs; and digital technology promotion as a way to promote civic engagement	The International Telecommunication Union (ITU) (2015)
Guidelines for Children on Child Online Protection	Digital etiquette; digital access; digital law; digital security (self-protection); digital communication; digital rights and responsibilities; and digital literacy, digital commerce	ITU (2014)
Guidelines for Parents, Guardians and Educators on Child Online Protection	Personal device safety and security; Law, education of parents guardians and teachers; education for children; and communication	The International Telecommunication Union (ITU) (2009)
Standards for measuring child online protection	Risk-prone conduct of children (activities and time spent online); cyber threats and incidents; reaction of children to such incidents; and preventive measures	ITU (2010)
Child Protection in the Online/Offline environment Strategies	Understand the social and cultural context; online / offline sexual harassment and abuse; actions of children using information and communication technology; vulnerability and harm to risks; and sources of help and assistance	United Nations Children's Fund (2012)

Table 2.7 presents the methods focusing on cybersecurity awareness and training of children. The methods mostly highlight awareness and training on risk identification, establishing a more secure and age appropriate online environment and children's risk-prone behaviour, online threats and incidents and how children respond to those incidents and preventive measures. Section 2.8 presents literature on the different approaches that are used to constitute the online behaviour influencing algorithms.

2.8. Approaches used to constitute online behaviour influencing algorithms

Question Four: *How can a suitable behaviour influencing algorithm be constituted to influence children's online activities?*

The behaviour of children online could be influenced through interactive modules. There are several complementary levels that can be operated to increase the safety of children online which are namely, service provider level, web browser level, application level and the network equipment level (Magkos et al., 2014). The different levels can be used to implement the designed algorithm to influence the behaviour of children online. Table 2.8 outlines the approaches that are used to design online behaviour influencing algorithms.

Table 2.8: Approaches used to design online behaviour influencing algorithm

Online behaviour algorithm	**Description**	**Source**
K-Nearest Neighbours (KNN)	The KNN instant-based learning algorithm that is an automated program built to analyse the text of a conversation and to identify the probability of online child grooming. It uses a pattern detection scheme.	Gunawan, Ashianti and Sekishita (2018)
Semantic-Enhanced Marginalized Denoising Auto-Encoder (SEMdae)	The SEMdae prevents the occurrence of cyber bullying messages on online social networking sites. It uses expert knowledge for feature learning and uses the Machine learning approach to classify the posted semantic context.	Leela Prasad *et al.* (2019)
Deep Belief Networks and Stacked Denoising Auto-Encoders	Is a software that uses deep learning algorithms to predict user intentionality against a specific product, or category, based on their interaction on a website. Through keeping track of users' search habits to get a clearer understanding of their preferences and intentions.	Vieira (2015)
Rule-based Approach	The objective is to discover patterns of user interaction in learning processes and to react by making decisions based on adaptive rules on User Profiles collected. The method applies semantic recording of activity logs throughout the learning cycle so as to automatically discover patterns by semantic reasoning.	Okoye, Tawil, Naeem, Bashroush, & Lamine (2014)
Limited-Recursive Algorithm (LRA),	Is based on the common PageRank algorithm that served as the basis for the Social Influence Algorithm 1.0. The algorithm takes Facebook	Smailovic & Podobnik (2016)

	data for each user as input and outputs the Score for Social Impact. Using Facebook data is: i) number of a user's friends; ii) number of posts shared by the user on his / her Wall; and iii) number of Likes / Comments posted on those links.	
SmartSocial Platform (SSP)	SSP is based on the concept of heavy-backend thin clients. User first installs the Android app for providing users with personal data. Teleco data had been collected from the Android smartphone itself. Once the Android app acknowledges the terms of use, social data is collected from Facebook server. Component which enables users to check their SmartSocial Influence scores. The Android app is available to those who wish to become involved in the SmartSocial project. Android app includes several steps that allow: i) input the user's smartphone number; ii) providing Facebook data by logging in; iii) accepting usage terms of user data; iv) uploading Telco and social data; v) receiving notification of successful completion and the ability to view the created profile and SmartSocial influence score.	(Smailovic & Podobnik, 2016)

This analysis of the selected online behaviour influencing algorithms highlights the approaches used to constitute algorithms. The algorithms use approaches such as machine learning and deep learning to analyse and predict online behaviour. According to Hangtwenty (2018), machine learning is the science of getting computers to learn and act as humans do, and improving their learning in an autonomous fashion over time by feeding them with data and information in the form of observations and interactions in the real world. Deep learning enables computational models that are composed of multiple layers of processing to learn data representations with different abstraction levels (Lecun, Bengio, & Hinton, 2015). These approaches are used in speech recognition, visual object recognition, object detection and many other domains such as drug discovery and genomics and these have significantly enhanced the state of the art (Lecun et al., 2015). The suitable approach that relates more to this study from the solutions is the Deep Belief Networks that uses deep learning algorithms to predict the intentionality of users based on their website interactions. In this study, this is applied in the demonstration stage in section 5.2.5.

2.9. Chapter summary

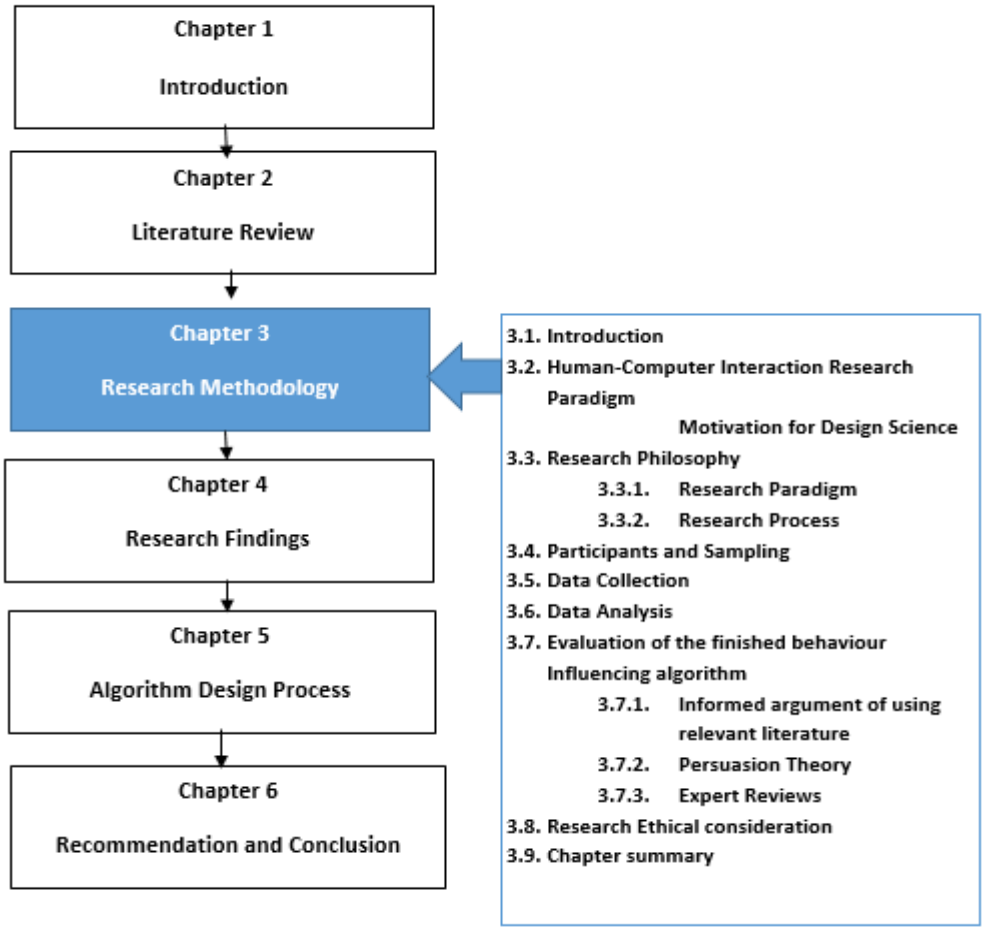
This chapter presented a review of relevant literature to this study. The area of Human Computer Interaction was adopted in this research since the study focuses on influencing children's behaviour online

and raising their cybersecurity awareness, which has the human as the focal point as they interact with devices. An analysis of children's online risk was done and the identified types of children online risk are cyberbullying/cyberstalking, sexting, digital identity theft, exposure to hate speech images and gory images, brain hijacking, online predator grooming, sexual exploitation and malware attacks. From the children's online behaviour analysis, it emerged that children accept friendly requests from strangers, they share personal information online, share pictures, videos and status updates, spend too much time on the Internet, download movies or music, and meet strangers offline, and this is attributed to the lack of cyber security awareness and the development stage of the child. Ojose (2008) outlined that Piaget believed that a child's development occurs through a continuous transformation of processes of thought depending on their maturity, experience, culture, and their ability. The reason why children post, trust and share online, according to Piaget's theory is because children in that age group's (12-18 years) behaviours are affected by the behaviour of their close friends and their puberty milestones. The common online activities by children were visiting social networking sites, playing online games, Internet surfing, chatting, online purchasing, emailing and watching online videos, movies or TV. This chapter also outlined that children's behaviour online can be influenced through awareness and training by applying game dynamics to non-gaming situations in order to induce interest and raise motivation levels and elements of this can be extended to keep a user interested in learning. The next chapter discusses the methodology used to answer the study's research questions.

Chapter 3: Research Methodology

3.1. Introduction

This chapter presents the research design as well as the methodology used in the study. The chapter also explains the research process, participants and sampling, techniques and the analysis of data collection, research limitations, ethical considerations and the conclusions of the study. The layout of this chapter is outlined in the chapter map.



3.2. Human-Computer Interaction research paradigms

The area of Human Computer Interaction (HCI) is a research that contributes to the user's understanding (Rozanski & Haake, 2003). Like any educational qualification, HCI is based on three wide foundations namely theoretical principles, professional practice and community of individuals. HCI's theoretical origins

as an interdisciplinary field includes psychology, computing, ergonomics, and social science (Dix, 2017). Furthermore, Rozanski and Haake (2003) outline that Human-Computer Interaction is a collaborative field that incorporates behavioural psychology and cognitive, ergonomics, anthropology, sociology, computer science, engineering, and graphic design concepts and methods, among others.

This section presents HCI's research paradigms namely Design Science, Traditional Scientific Approach and Engineering Approach. The foundation of selecting the appropriate research design and methodology is from an analysis of the theoretical backgrounds of each of the research paradigms as shown in Table 3.1.

Table 3.1: Research paradigms

Research design	Explanation	Source
Design Science Approach	● Design science research (DSR) is a research paradigm with great potential to address the relevance of information systems (IS) research as opposed to the rigorous gap. ● DSR brings both practical relevance to IS research (through its emphasis on useful artefacts) and scientific rigor (through the formulation of design theories). ● IS prides itself as a discipline within the field of IT-related technological science. ● The artifacts developed in the research phase of design science include, but are not restricted to, algorithms, interfaces between humans and computers, and methodologies or languages of system design.	(Baskerville, Baiyere, Gregor, Hevner, & Rossi, 2018)
Traditional Science Approach	● The traditional approach to science makes use of a positivist interpretation of research. This focuses on quantitative data collection based on empirical measurements using analytical methods to build and test simulation models. ● Traditional research in science is meant to investigate how things are based on observable facts that can be seen, heard and touched. ● The researcher collected knowledge through questionnaires and tests, and developed and tested hypotheses prior to empirical analysis. Within HCI, this approach creates awareness that helps researchers to derive deductive and inductive theories from empirical experimental findings. The conventional approach to science enables researchers to grasp the relation between variables and prediction of results.	(Kuechler & Petter, 2012)
Engineering Approach	● The Engineering approach borrows its features predominantly from both design science and traditional approaches to research.	(Pather & Remenyi, 2005)

	• The researcher examines exiting solutions with the aim of creating better solutions propositions. • A selection of appropriate alternatives will be measured, analysed, and evaluated on the basis of the proposal. • The process is repeated until the product is really for use and no further improvements are needed for further changes.	

Motivation for design science

Vaishnavi and Kuechler (2013) define design as to invent and build. In this study, a definition of design science is adapted from Peffers, Tuunanen, Rothenberger, and Chatterjee (2007) and it is defined as:

Design science creates and evaluates IT artefacts that are designed to solve identified organisational problems. "It involves a rigorous process of designing artefacts to solve observed problems, contributing to research, evaluating designs and communicating the results to the appropriate audiences"

The purpose of this study is to design a solution for an existing problem. Therefore, this study takes on a research paradigm of design science towards the designing of an algorithm that will influence children's behaviour online and raise their cyber security awareness. Vaishnavi and Kuechler (2013) further define design science as something that involves the creation of data through design of novel or innovative artefacts and the analysis of the use and performance of such artefacts together with reflection and abstraction to improve and perceive the behaviour aspects of Information systems. Such artefacts include but actually don't seem to be restricted to algorithms (e.g. for information recovery), human/computer interfaces, and system design methodologies or languages. Section 3.3 outlines the research philosophy.

3.3. The research philosophy

Heyvaert, Maes and Onghena (2013) describe research as a scientific or academic examination into a phenomenon intended to identify, report and create new artifacts and contribute new knowledge. The study takes on a design science research paradigm towards the designing of an algorithm that will influence children's behaviour online and raise their cyber security awareness. According to Vaishnavi and Kuechler (2013), Design science research involves the creation of data through design of novel or innovative artifacts and analysis of the use and performance of such artifacts together with reflection and abstraction to improve and perceive the behaviour aspects of Information systems. It can also position it in light of establishing information systems and computer science methods. The design of this research is based on the concept of the research onion proposed by Saunders, Lewis, and Thornhill (2019).

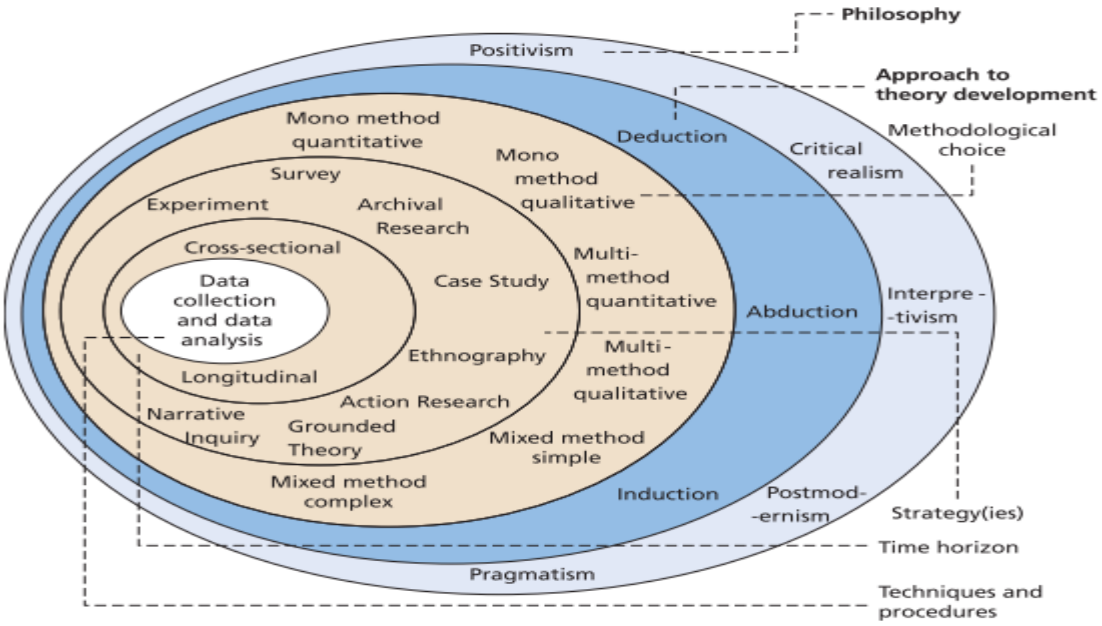


Figure 3.1: Research onion (Source: Saunders et al., 2019)

This study adopted a mixed method, involving both qualitative and quantitative methods. According to Plano Clark (2017), mixed methods research involves assembling, studying and interpreting quantitative and qualitative data in a series of studies that investigate the same underlying phenomenon. This study aims to understand the behaviour of youngsters in-depth for this reason qualitative methods are suitable, however to be aware of the magnitude of the phenomena, a quantitative study suffices as a complement to the qualitative method (Creswell, 2007). According to Muskat, Blackman, and Muskat (2012), there are five foundations for conducting the mixed method research;

- **Triangulation:** seeking for validation and convergence of outcomes from diverse methods and design reviewing the same phenomenon
- **Complementarity:** seeking for elaboration, improvement, illustration, and interpretation of the outcomes from one method with outcomes from the other methods
- **Initiation:** discovering inconsistencies and paradoxes that lead to a re-framing of the research question
- **Development:** using the judgement from one method to help enlighten the other method
- **Expansion:** seeking to enlarge the breadth and the range of research by using diverse methods for diverse inquiry components

For a broader understanding of the study, the suitable approach to use for this study was a mixed method approach. Quantitative analysis techniques such as graphs, charts and records allowed the researcher to explore, present, describe and examine relationships and tendencies inside the data (Saunders et al., 2019). The qualitative approach offers an in-depth understanding of the social, political and cultural context. This allows the researcher to consider the background in the preparation of an effective response using an evolving qualitative approach to investigation and data collection in a natural setting that is responsive to people and places under study. An inductive data analysis that identifies trends or themes (Creswell, 2007) and the contextualisation of the solutions which are informed by responses from the patterns and themes are then used to inform the design of the algorithm. Section 3.3.1 outlines the different research paradigms and a motivation for the selected paradigm was outlined.

3.3.1. Research paradigm

According to Saunders (2009), Walliman (2010) and Melnikovas (2018), to enhance the researcher's understanding of the way in which to approach the study of a specific area, one of the four paradigms can be applied to the studies;

- **Positivism** – the approach to scientific research is based on accepting that the world around us is genuine and that we are able to find out about these realities. It mainly represents a natural scientist's philosophical approach. Ontology is based on the objectivist assumptions of the observation of entities, atomic events that are currently external to social actors, and as such, only observation and empirical information can be called "credible". Knowledge is achieved through the observation and discovering of regularities of events based on causal, policy-like and functional relationships.
- **Critical realism** - is based on two ontological assumptions: (1) the world is made up of actual entities; (2) the sensation and pictures of actual entities is perceived, not the actual entities themselves. Knowledge is gained by finding generative accesses.
- **Interpretivism** - Is a method based on subjectivist ontological assumptions that entities are made up of discourse and therefore exiting or socially constructed truth can only be investigated through social constructions such as awareness or language. Reality is built socially and develops constantly, therefore, information and facts are relative and subjective.
- **Pragmatism** - Is based on the premise that both positivist and interpretative positions can be adapted in the course of studies, whatever, operates best for specific study questions.

Motivation for pragmatism paradigm

The study followed a philosophy of pragmatism research, which is guided primarily by an inductive qualitative approach. Pragmatism supports the utilisation of both qualitative and quantitative in the same study and rejects inconsistency approaches. However, pragmatism also considers the research questions to be more necessary than either the method or paradigm that underlies the method (Plano Clark, 2017). Section 3.3.2 presents the research process.

3.3.2. Research process

Vaishnavi and Kuechler (2013) define research as an activity which helps to understand a phenomenon. In the case of research into design science, all or part of the phenomenon can be produced as opposed to occurring naturally. The phenomenon is typically a set of behaviours of some entity(ies), which the researcher or a group finds interesting. Table 3.2 presents the application of design science research methodology in this study.

Table 3.2: Application of design science research methodology (Kuechler & Petter, 2012)

DSRM activities	**Activity description**	**Knowledge method**
Problem identification and motivation	*What is the problem?* Out of innocence, the behaviour of children potentially exposes them to cyber criminals as they innocently share information and befriend strangers.	Literature review on children's online activities and behaviour that expose them to cybercrimes. Current solutions on how children's online behaviour are being influenced and the solutions weaknesses
Define the objectives of a solution	*What are the goals of the solution?* • Influence children's behaviour online • Promote secure online behaviour through reward and penalties • Raise Internet security awareness • Educate children on secure online behaviour • Increase awareness	Knowledge of what is possible and what is feasible. Knowledge of methods, technologies and theories that can help with defining the objectives

	• Ensure secure online experience • Reward secure behaviour • Gauge the security on child behaviour online	
Design and develop	*Create an artefact that solves the problem* Designing an algorithm that will influence children's behaviour online and raise their cyber security awareness	Application of methods, technologies, and theories to create an algorithm that will influence the behaviour of children online and raise their cyber security awareness
Demonstration	*Demonstrate the use of the artifact* An algorithm was designed to influence the behaviour of children online. A flowchart was designed to demonstrate the implementation of the algorithm. A game was further developed to implement the flowchart of the algorithm.	Knowledge of how the algorithm will be used to influence the behaviour of children online
Evaluation	*How well does the artifact work?* The algorithm, its components and their relationship were evaluated by experts with specialized knowledge in Information security and children digital rights.	Knowledge on the relevant behaviour influencing models and evaluation techniques
Communication	This study is communicated through raising awareness at schools in Namibia through game play (by giving access to the game platform to learners), thesis and scholarly publications.	Knowledge of the disciplinary Thesis documentation, presentation process, publication and contribution.

3.4. Participants and sampling

Sampling can be defined as the method by which individuals or sampling units from the sample frame are selected (Martínez-mesa & González-chica, 2016). According to Gray (2014), there are two ways to choose a research sample; (i) probability sampling is one of the defining features of quantitative research which involves selecting random samples, and (ii) non-probability sampling's defining features depend on the purpose of the study. Saunders, Lewis and Thornhill (2008) further explain that having decided the likely appropriate sample size, you need to select the most suitable sampling technique to enable you to answer your research questions from the range of non-probability sampling techniques available. Martínez-mesa and González-chica (2016) allude that purposeful sampling is used where a diverse sample is required or experts' opinions in a specific filed is the topic of interest. The purposeful sampling technique, also called judgmental sampling, is a participant's intentional choice due to the attributes that the participant possesses (Etikan, 2017). This includes the identification and selection of people or groups of people who are knowledgeable and well-informed about a phenomenon of interest (Etikan, 2017). Therefore, a purposeful sampling technique was used in this study because purposive sampling it is known to the agent of the whole population, or it is known that creates well-coordinated bunches (Clark, 2017).

According to Anderson (2016), parents of 13-17 year olds teenagers now live in a world that is heavily influenced by digital devices and online platforms. In another report by OECD (2012), 12-17 year olds mostly access the Internet through mobile devices instead of using fixed computers. Thus, the target population for this research was purposefully selected after investigating the literature as well as identifying the resources that would afford the value of the concepts of this research. Children between the age of 13 and 17 years in primary and high schools were considered to answer the survey questionnaires and be part of the algorithm evaluation.

A predictive evaluation was used to evaluate the COSBIA, as Sharpe et al. (2019) outline that it foresees usability problems, and experts apply their experience of typical users that involve heuristics and users do not have to be present.

3.5. Data collection

Questionnaires were used to collect data on children's behaviour and the different activities that expose them to cybercrimes through surveys. This allowed the researcher to gather data which cannot be

obtained from resources like books, reports and records. Additionally, for the evaluation of COSBIA, an online questionnaire was used to evaluate the COSBIA's components and relationship relevance.

3.6. Data analysis

The collected data was analysed using qualitative analysis methods, Microsoft Excel and SPSS. Below is a Table 3.3 that illustrates the research objectives, questions and the tools that were used to carry out the study.

Table 3.3: Research objectives, related research questions and tools that were used

Research objectives	Research questions	Data collecting technique (s)
Analyse how children behave online	How do children behave online?	Literature review, questionnaires
Evaluate online activities that expose children's interaction with strangers	Which activities specifically expose children to security risks when they interact with strangers?	Questionnaires and literature review for data collection and mixed data analysis approaches was used (coding for qualitative data and statistical for quantitative data)
Evaluate behaviour analysing tools suitable for child online activities	What are the existing behaviour analysing tools suitable for child online activities	Literature review
Design a behaviour influencing algorithm suitable for the security of children online activities	How can a suitable behaviour influencing algorithm be constituted to influence children's online activities?	Results from objectives (i) and (ii), as well as literature review will serve as inputs on designing an algorithm using the Design Science Research Method.

3.7. Evaluation of the finished behaviour influencing algorithm

To ensure that the proposed algorithm is useful to influencing children's behaviour and contributes to the body of knowledge, the algorithm evaluation process aimed at validating the relevance and rigor of the identified algorithm constructs and content in order to determine how well the algorithm targets influencing children's behaviour online and thereby solve the identified problem. An expert review and a descriptive methods were chosen as suitable for the evaluation of the proposed algorithm (Gardikiotis & Crano, 2015). The following descriptive methods were used to evaluate the algorithm:

- Informed argument of using relevant literature
- Persuasion Theory
- Expert reviews

3.7.1. Informed argument of using relevant literature

The aim of using argumentation is to reach a mutually accepted conclusion about the importance, relevance and usefulness of the proposed algorithm. A detailed review of children's online activities and behaviour that expose them to cybercrimes literature in section 2.5 helped to build a convincing problem definition and argument that there is a need for a behaviour influencing algorithm for children. The literature review helped to identify the presence of the gap in children's online activities in section 2.4 and online behaviour in section 2.3 that expose them to cybercrimes, hence a need for an algorithm that influence children's behaviour and raise their cyber security awareness was designed in section 5.2.

3.7.2. Persuasion theory

According to Gardikiotis and Crano (2015), persuasion is a basic human process which affects almost every aspect of social interaction. Individuals seek to manipulate the perceptions and attitudes of others in interpersonal relationships, mass communication, politics, economics and even international relations. Persuasion is generally concerned with shifting behaviours and thus (under specific conditions) people's actions in a sense of relative freedom. To evaluate the Child Online Secure Behaviour Influencing Algorithm, the study used the following two persuasion theory approaches which were applied in the design and demonstration stage of the COSBIA:

i. **The Learning Approach -** The learning approach promoted the idea that the persuasion target first had to understand and learn the ideas communicated by the message, in order to be influenced. In this context, the effect was mainly concerned with the way attitudes were shaped and formed (Gardikiotis & Crano, 2015). In this study the algorithm was gamified to evaluate and promote awareness.

ii. **Operant conditioning -** In this context, a behaviour is influenced because it is reinforced, that is, it is accompanied by a positive outcome, or it is prevented because it is punished (Gardikiotis & Crano, 2015). Operant conditioning is a learning method that comes from rewards and behavioural penalties. A person makes a connection between a particular action and a consequence through operant conditioning (McLeod Saul, 2018). According to McLeod Saul

(2018), Skinner defined three types of responses or operators that are capable of following actions.

1. Neutral operators: contextual responses which do not increase or decrease the probability of repeating a behaviour.
2. Reinforcer: Contextual responses which increase the likelihood of repeating a behaviour. The straighteners may either be positive or negative.
3. Punishers: Contextual reactions that lower the risk of repeating a behaviour.

Figure 3.2 illustrates that the positive and negative reinforcement and positive and negative punishment increase and decrease the frequency of the individual's desired behaviour.

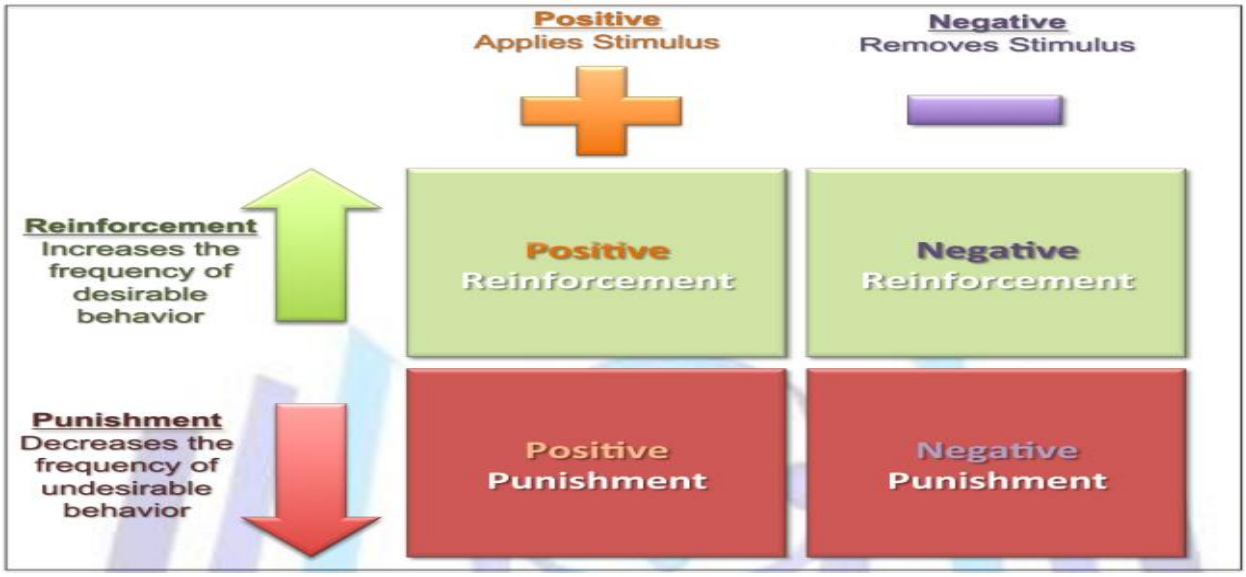


Figure 3.2: Reinforcement Theory (Source: Amutan, 2014)

A token reinforcement was used with children that behave more securely on the Internet. For example, a security token may be granted to a child who has behaved securely online and has the highest point. This act helped to encourage children that are exposed to the behaviour influencing the algorithm to be more positive and stay more secure on the Internet. This was achieved through different levels in a game implementing COSBIA.

Application of reinforcement - an appropriate technique can be implemented for positive reinforcement based on guidelines below (Amutan, 2014):

- The enhancement needs to be implemented regularly, based on a scheduled reinforcement system
- The reinforcement should be delivered to the child quickly to keep them from losing their influence. If there is a need, a verbal reinforcement to the child can be proposed if they need to get another reinforcement
- Whenever the child's behaviour is secure online, COSBIA should promote the secure online behaviour by giving the child a reward
- There should be no uncertainty about the child's social reinforcement, it should be transparent and comprehensible.

3.7.3. Expert reviews

Various Human Computer Interaction (HCI) evaluation techniques, namely focus groups, field experiments, and expert reviews, have been used extensively in research studies. These approaches aim to produce qualitative results and require fewer participants than experiments that are controlled (Tory & Moller, 2016). We focused on domain expert reviews in this study to evaluate the algorithm using design science research process. According to Beaudouin-Lafon (2006), to predict missing requirements, experts apply the experiences of typical users. This can involve heuristic and theoretically based phenomenon and users do not need to be present (Beaudouin-Lafon, 2006). The expert review is under the predictive evaluation paradigm in Human Computer Interaction (Beaudouin-Lafon, 2006). In this study, domain experts evaluated the relationship of components and its relevancy aspects using an online questionnaire. The questionnaire was structured to gather expert biography, algorithm components, and the algorithm itself as presented in Appendix G: Expert Review Evaluation Form. Section Chapter 1690710027: outlines the research's ethical consideration.

3.8. Research ethical considerations

Research participants should have confidence that the materials will be handled and used sensitively and responsibly (Toader, Damir, & Toader, 2010). The researcher first sought authorisation through the use and presentation of the research proposal from the relevant authorities before starting with this research study. The application for ethical clearance Appendix A: Faculty Postgraduate Committee Ethical Approval Letter was submitted to the Higher Degrees Committee (HDC) through the Faculty Post Graduate Committee (FPGC) and this was approved. Permission to conduct the study in schools was sought from

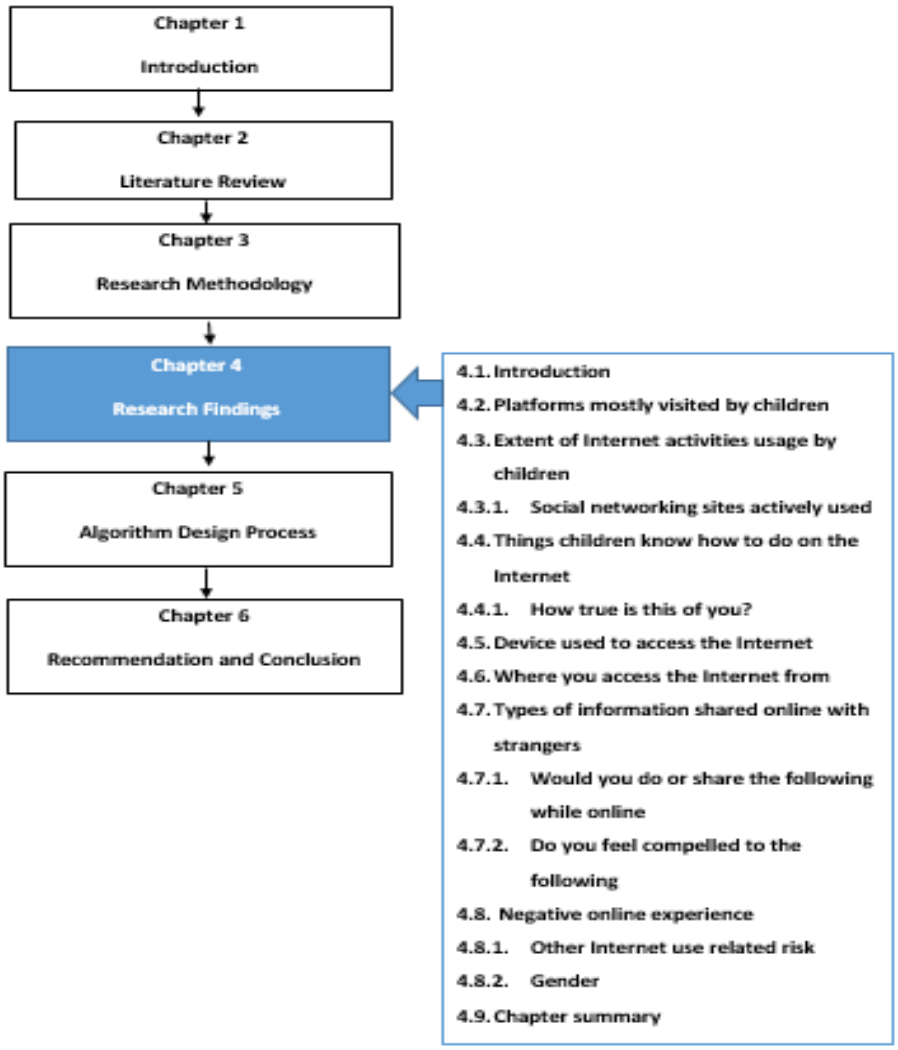
the Ministry of Education as presented in Appendix B: Ministry of Education Permission Letter. Subsequent to this, permission was sought from the principals of each participating school and the permission letters are in Appendix C: Ministry of Education Approval Letterand Appendix D: Schools Permission Letter. Parental consent was sought as minors were involved in the study using the informed consent form in Appendix E: Parental Consent Letters. In addition, research participants were provided with full information on what the research is about, its purpose, how long the study would take, research procedures and the expected benefits of the research study. In order for research participants to make a free and informed consent, they were provided with full details of the research study to ensure their right of self-determination and autonomy.

3.9. Chapter summary

This chapter presented the research design as well as the methodology used in the study. This research falls under the Human-Computer Interaction (HCI) domain, and the objectives were achieved using the design science research model. The research paradigm that was used is pragmatism following the Design Science Research Methodology (DSRM) to design the algorithm. This study followed a mixed method approach where questionnaires were used as a data collection tool and they were analysed using Microsoft excel and SPSS. The participant populations were purposefully sampled as this allowed for knowledgeable participants to participate. The participants were conveniently selected from the target population using a self-selecting strategy. For qualitative data, the target sample size was 40 participants as they allowed for data saturation. An expert review was used to review the designed algorithm. The participants were selected from predefined strata based on their active involvement in COP. Gamification of the algorithm was used to demonstrate functionality by embodying persuasion theory in implementation. The next chapter discusses the research findings of this study.

Chapter 4: Research Findings

This chapter presents the research findings of this study. The chapter also shows the data analysis of platforms visited by children, Internet activities usage, devices used to access the sites and more as outlined in the chapter map below.



4.1. Introduction

This chapter focuses on the research findings from the questionnaires. The instrument for data collection was an open-ended questionnaire and close-ended questions which were designed to collect basic information to address Objective 1 and Objective 2 of this study, which are (i) to evaluate online activities that expose children's interaction with strangers, and (ii) to analyse how children behave online. They were then distributed to 40 learners in four different schools in Windhoek. The schools are namely, Dobra

High School, Eldorado Secondary School, Highline Secondary School and Windhoek Technical High school. The 40 learners between the ages of 13 and 17 years were granted permission by their parents to complete the questionnaires. The questionnaires included a total number of 16 questions. Question 1-5 focused on analysing the online behaviour of children, Internet knowledge and the frequency of Internet access. Question 6-15 assessed how the behaviour of children is influenced by their online activities, online risk and exposures. This chapter is divided into two parts, the first part reports on the types of online platforms mostly visited by children and online activities that expose children's interactions with strangers. The second part reports on the things children know how to do on the Internet, the devices children used to access the Internet, the time spent on these devices, types of information shared on the Internet and the types of online risks. Section 4.2 reports on the types of online platforms mostly visited by children and children's Internet activities, their Internet activities and things they know how to do on the Internet.

4.2. Platforms mostly visited by children on the Internet

Respondents were asked to identify the types of online platforms they mostly visited on a scale of 1-5. The majority of respondents highlighted that they access social networking sites (50%) almost all the time (scale 5) or Internet (37%), communication platforms like Skype or YouTube (26%), and gaming platforms (26%), with the email (3%) being the least visited. Most respondents stated that they never access emailing platforms (40%), however, access the Internet at least daily (20%) and access gaming platforms (20%) at least weekly. The summary of the responses is presented in Figure 4.1.

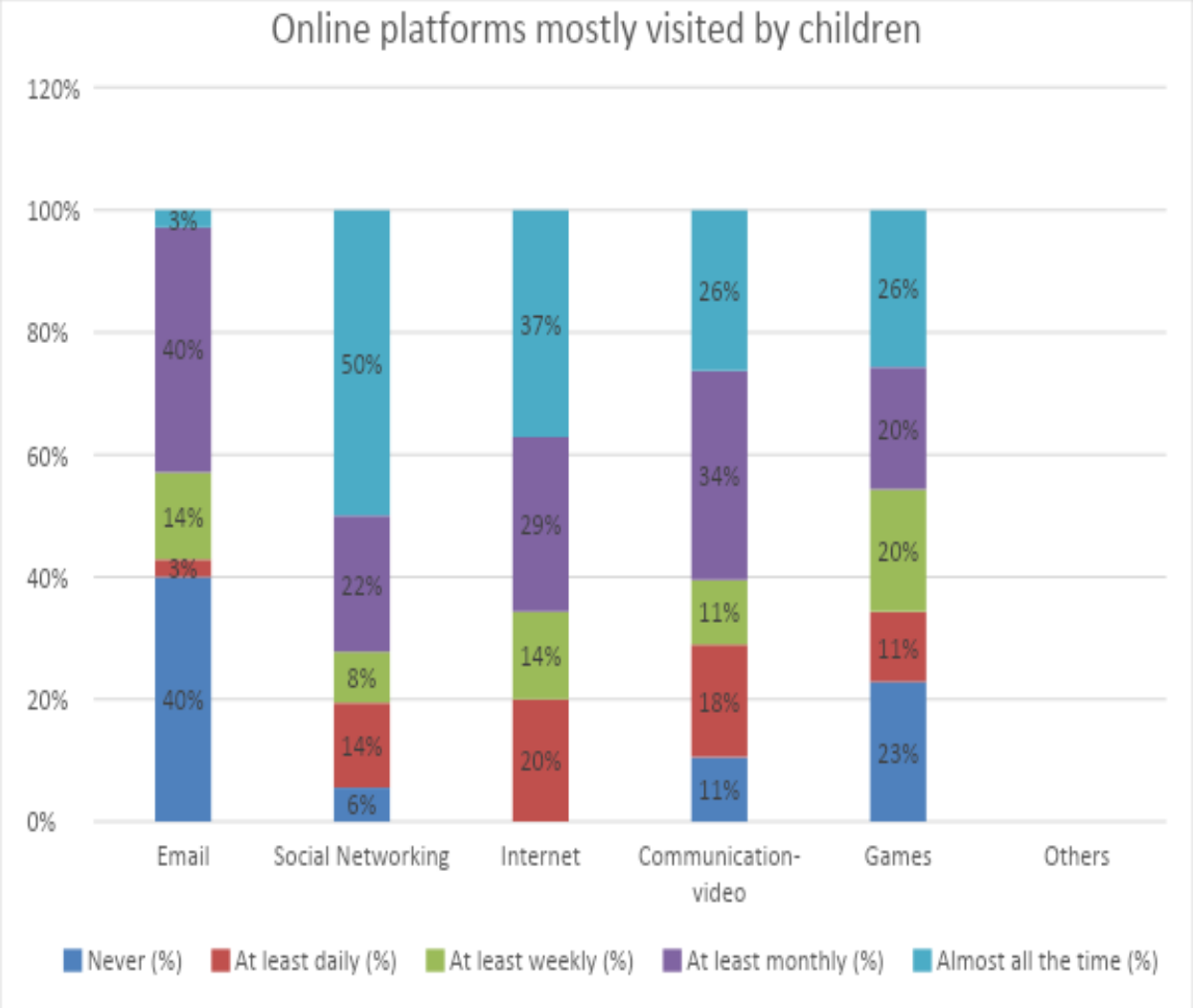


Figure 4.1: Types of online platforms visited

The results highlight that children mostly spend their time on the Internet on social networking platforms, followed by searching on the Internet in general and visiting video and voice communication platforms and gaming platforms when they are online. These results are consistent with the findings of Ghari (2012), Hamat et al. (2012), Mascheroni and Ólafsson (2013), Eke, Omekwu, and Odoh (2014), Braimllari (2017), Kirichenko, Radivilova, and Anders (2017), and Livingstone, Haddon, Görzig, and Ólafsson (2010), who confirmed that social networking takes the top spot of daily activities by children. Listening to music, watching video clips and using Instant Messaging like Skype or WhatsApp follow afterwards in this report. These results also match with those by Kirichenko, Radivilova, and Anders (2017) who found out that the World Wide Web's love child is social media that comes in many ways like blogs, forums, business

networks, photo sharing sites, social gaming, microblogs, chat apps, and other social networks. Eke, Omekwu, and Odoh (2014) also affirm that the more the person depends on the Internet to communicate his or her thoughts and share his or her ideas, the more the Internet affects the individual.

From the analysis, 50 percent of children spend almost all their time on social networking platforms, 36 percent of children spend almost all their time on the Internet, followed by 26 percent of children who spend their time on games and videos on the Internet almost all their time. Hence, they may be at risk as they visit social networking sites because they might not always completely understand the potential impact of the use of the Internet and mostly social networking sites.

This means that the more children rely on social networking sites to network and mingle with their peers, the more it will change their behaviours, awareness and emotional states. Ofcom (2017) outlines that social media can be difficult for children and parents to manage.

4.3. Extent of Internet activities usage by children

In order to understand what children use the Internet for, respondents were asked the extent they use the Internet for the listed activities on a scale of 1-5. Figure 4.2 illustrates the extent of Internet usage by children.

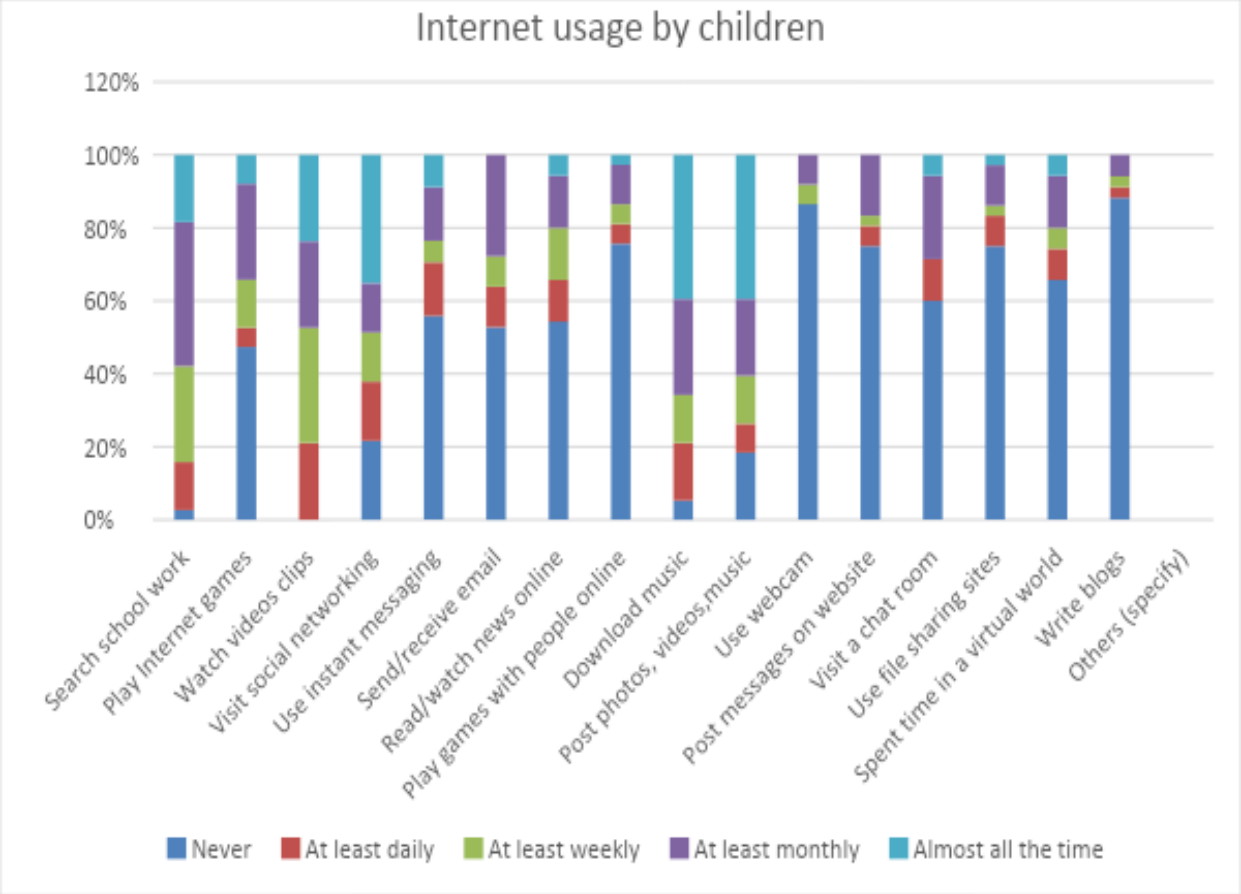


Figure 4.2: Internet usage by children

These results highlight the Internet usage by children and it shows that children access almost all the time or at least daily on social networking sites, download music and post photos, videos and music, watch video clips and search for school work information on the Internet. Children reported to have never used the Internet to write blogs, spent time in a virtual world, use files sharing sites, visit chat rooms, post messages on websites, play games with people online, read/watch news online, send/receive emails and use instant messages. At least monthly they search for school work related information, play Internet games, send or receive emails, watch video clips online, download music, post pictures, video and music, and visit chat rooms. What children mostly do daily is to watch video clips, visit social media, download music, use instant messages and search for school work. On a weekly basis, children search for school work related information, watch video clips, visit social media, read/ watch news online, download music, post photos, videos, and music and play Internet games. From the analysis, most popular activities on the Internet by children are downloading music, watching videos, searching for school work related

information, visiting social networks, posting pictures and playing Internet games. The report shows that when children download music and watch videos on the Internet, they reported to have experienced online risk such as pornography, unwanted content and commercial content. This means that when children download music or watch videos on the Internet they become more vulnerable to unwanted content, inappropriate contact and unwelcome conduct on the Internet.

4.3.1. Social networking sites actively used

The results in Figure 4.2 demonstrate that one of the most popular online activities as reported by the respondents is social networking. Additionally, Figure 4.3 illustrates the types of social networking sites children actively use.

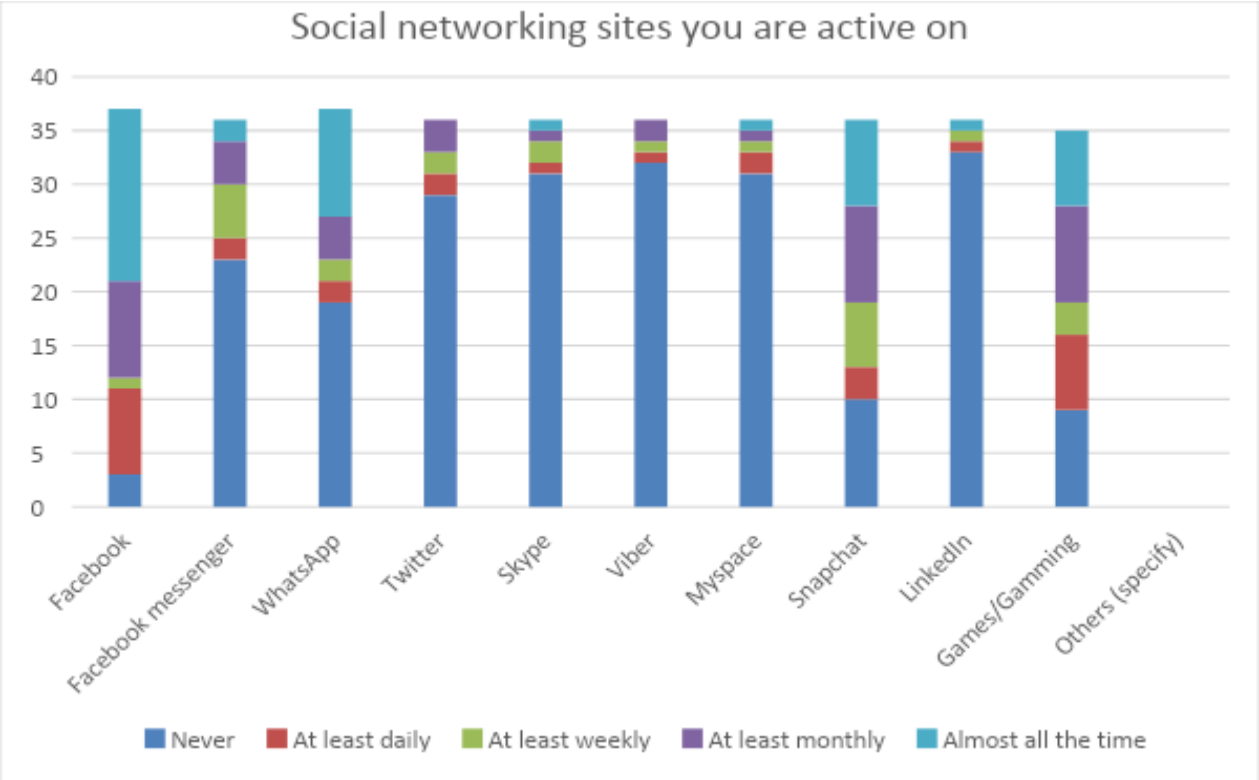


Figure 4.3: Social networking sites visited

These results highlight the different social networking sites children visit on the Internet and it is shown that the visited social sites “Almost all the time” and “At least monthly” are Facebook, WhatsApp, Snapchat and Games/gaming. For at least weekly, children reported to have visited Snapchat and Facebook messenger. At least daily children report to have visited Facebook, Games/gaming, Snapchat,

WhatsApp and Facebook messenger. Overall from this analysis, it is shown that all the other platforms have a higher rate of "Never" being accessed except the following platform that were less presented, Facebook (3%), Snapchat (10%) and Games/Gaming (9%). Since Facebook was presented less, this means that Facebook is the most frequently accessed platform amongst children aged 13 to 17 years. These results are consistent with the findings of Braimllari (2017) and Ofcom (2017), who confirmed that Facebook is the most popular social networking site used by children.

From this analysis, most children that spend most of their time on social networking sites reported to be experiencing the risk of spending too much time online where they would miss their homework or even miss their sleep. Additionally, they also reported to have experienced health related risks such as muscular conditions and eye-sight problems. This means that spending too much time on the Internet does not only pose Internet risks but can bring health related problems too. In section 4.4 we report on the things children know how to do on the Internet, the devices children use to access the Internet, the time spent on the devices, the type of information shared on the Internet and the types of online risks encountered.

4.4. Things children know how to do on the Internet

In order to measure respondents' knowledge on the Internet, they were asked whether they knew how to bookmark a website, block messages, find information on how to use the Internet safely, change privacy settings, compare different websites to decide if information is true, delete the record of which site they visited, block unwanted adverts or junk mail/spam and change filter references when using the Internet. Figure 4.4 shows the things children know how to do on the Internet.

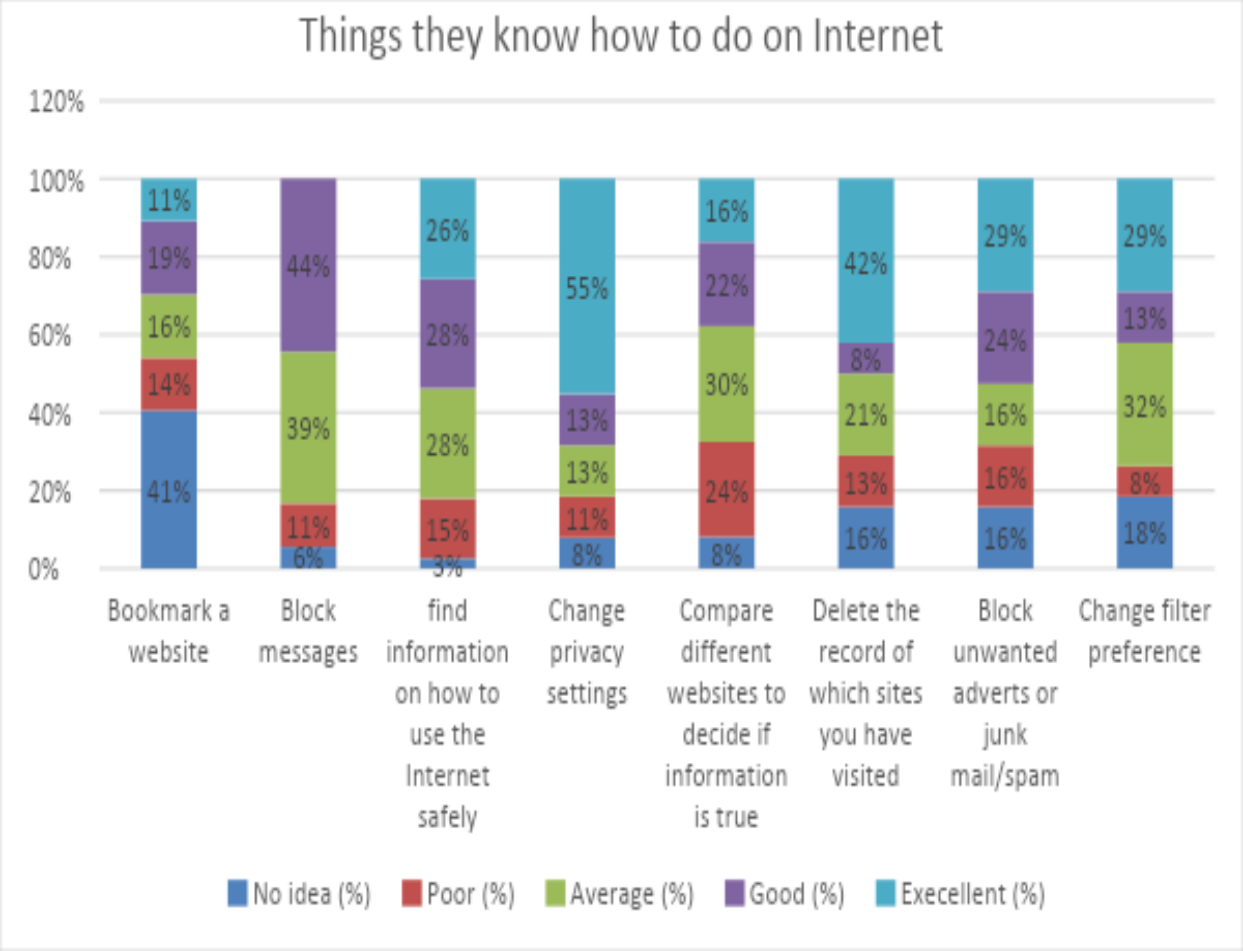


Figure 4.4: Security settings knowledge

Overall the respondents demonstrated only a moderate level of knowledge on some of the security settings that need to be configured on the Internet to improve their safety on the Internet. The results show that 41% of children had “No idea” on how to bookmark a website, 24% are “Poor” in comparing different websites to decide if information is true, 39% have “Average” and 44% “Good” knowledge on blocking messages. And the majority of children of have “Excellent” knowledge on changing privacy settings, delete the record of which sites they have visited, block unwanted adverts or junk mail/spam and changing filter preferences. From the analysis, it shows that children spend more of their time on the Internet, and they have knowledge on most of the security settings that need to be configured on the Internet.

These results are consistent with the finding of Mascheroni and Ólafsson (2013), who confirmed that online activities are not entirely useful or risky, and that children who take up a broader range of online

interactions are usually exposed to more risks, and they are also trained to deal with those risks, hence experiencing less harm. More use of the Internet is likely to promote competencies in computer literacy and safety skills (Haan & Livingstone, 2009). Montenegro (2016) outlines that children become considerably more knowledgeable as they grow older, including in terms of skills in managing the harmful footprints they leave on the Internet.

4.4.1. How true is this of you?

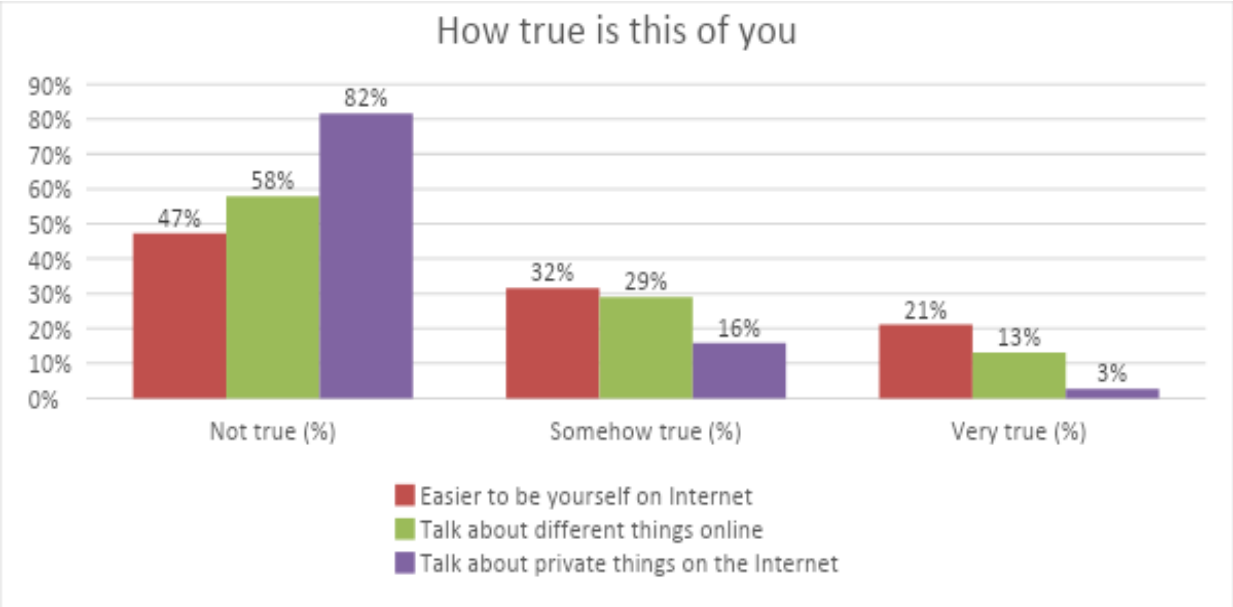


Figure 4.5: Online behaviour

For the purpose of this study, online behaviour was explored in terms of children's expressions when using the Internet. Respondents were asked how true this is with regards to their online behaviour. The majority of respondents reported that it was not true that it is easy to be themselves on the Internet, and they do not talk about different things and private things on the Internet. However, 32% feel that it's easier to be themselves on the Internet and 29% talk about different things and 16% talk about private things on the Internet. In addition, 21% reported to be "very true" that it is easy to be themselves on the Internet, 13% do talk about different things and only 3% talk about private things on the Internet.

Based on this analysis, children talking about different things and private things on the Internet is irregular. However, children feel comfortable to be themselves on the Internet, which means that they can express themselves freely on the Internet than in person. Children that reported that they can express themselves

freely on the Internet than in person also reported to have been sharing their personal information on the Internet which could pose online risks to them.

4.5. Devices used to access the Internet and time spent on the device per day

Respondents were asked which devices they use to access the Internet and how much time in hours they spend on the device per day. The majority of respondents reported that they use smartphones to access the Internet, 15 respondents reported spending 6h-10h per day, 9 respondents reported spending 1-5hours and another 9 respondents stated that they spend 11-15 hours per day using their smartphones, followed by using a laptop and spending 1h-5h per day and 6-10h per day as shown in Figure 4.6. This is similar to other findings by Green, Ólafsson, & Hartley (2011) that showed that 76 percent of children go online daily or almost daily, 22% use the Internet once or twice a week, leaving just 2 percent who go online less often.

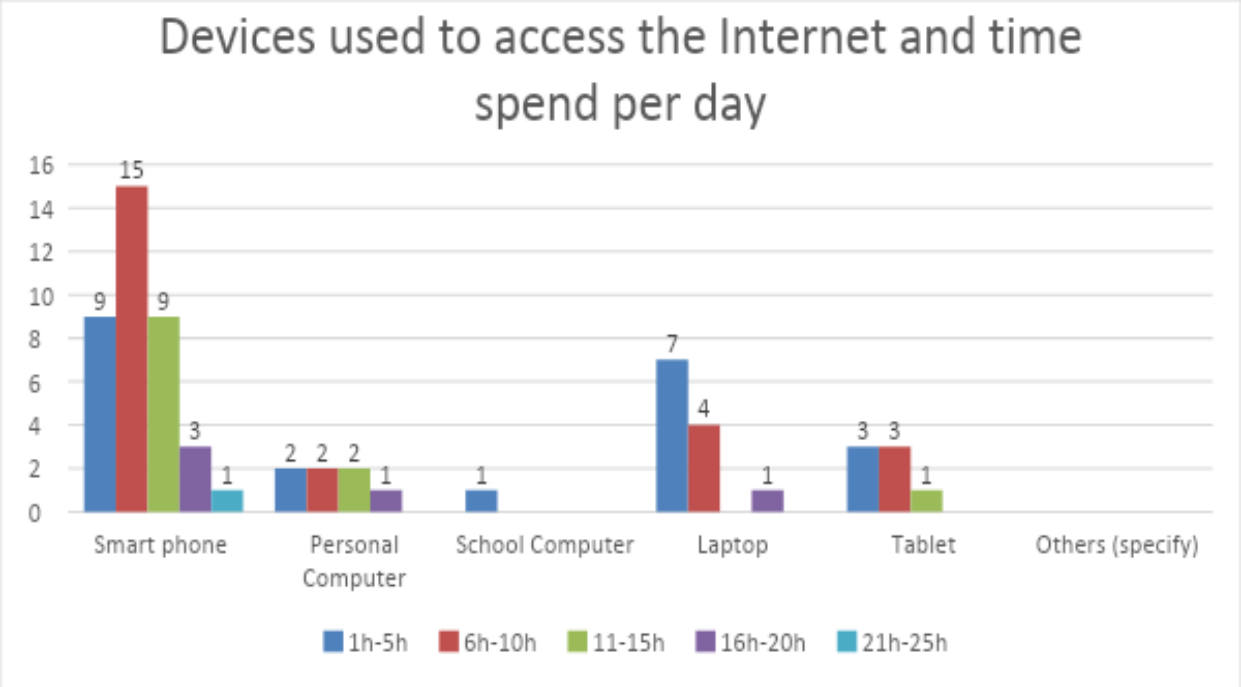


Figure 4.6: Devices used to access the Internet and time spent per day

From the analysis, it shows that children that spend most of their time on the Internet are children who either own or have access to smartphones, and mostly access the Internet from home. This means that when children have smartphones and have Internet at home, they tend to spend most of their time on the Internet. This implies more opportunities for a child to be exposed to inappropriate content or Internet dangers because of the more time they spend on the Internet with little supervision.

4.6. Where you access the Internet from

Respondents were asked to indicate where they access the Internet from and the majority of respondents reported accessing the Internet from home, followed by a public library, at school and at an Internet café. Two respondents chose the other option to specify where they access the Internet from and they reported to access it from their aunt's place and another specified that they access the Internet everywhere using a pocket Wi-Fi. Furthermore, the findings support other established researches by Haan and Livingstone (2009), Bhunu Shava, Chitauro, Mikka, Nhamu, and Gamundani (2016), Phyfer, Burton, and Leoschut (2016), and Livingstone, Davidson, Batool, Haughton, and Anulekha (2017) concerning how children access the Internet. Internet access has become easily accessible just at the comfort of the home, and as such the main Internet access point for children is their home. Internet usage is becoming more private, in children's own house, or when out and about, as children grow older (Livingstone et al., 2017). Additionally, Mascheroni & Ólafsson (2013) report that home is the most common place to go on the Internet as many children have private access to the Internet. Hence, it is important to raise awareness and influence children's behaviour on how children can behave online to prevent online risks that may be posed to them. Figure 4.7 illustrates the Internet access locations as indicated by children.

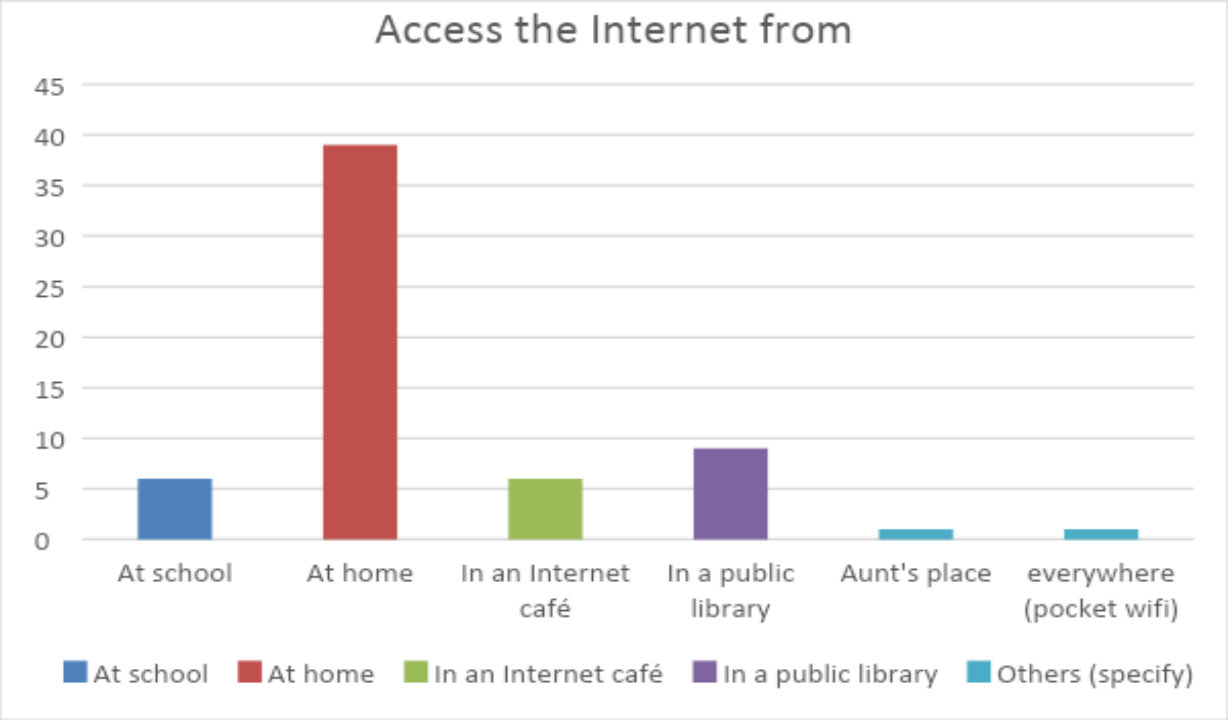


Figure 4.7: Internet access location

4.7. Types of information shared online with strangers

Respondents were asked to indicate the type of information they had shared online with people they had never met in real life using the different platforms. The majority of respondents reported to have shared their gender, their age or birth date, their actual name, and their phone number while on social networking sites, accessing their emails, gaming and while browsing or searching for information on the Internet. Most respondents reported to have been mostly using social networking sites when sharing this information online with people they had never met in real life, followed by while accessing emails and playing games and browsing the Internet. Figure 4.8 illustrates the type of information shared online with people that the respondents never met in real life using the different platforms.

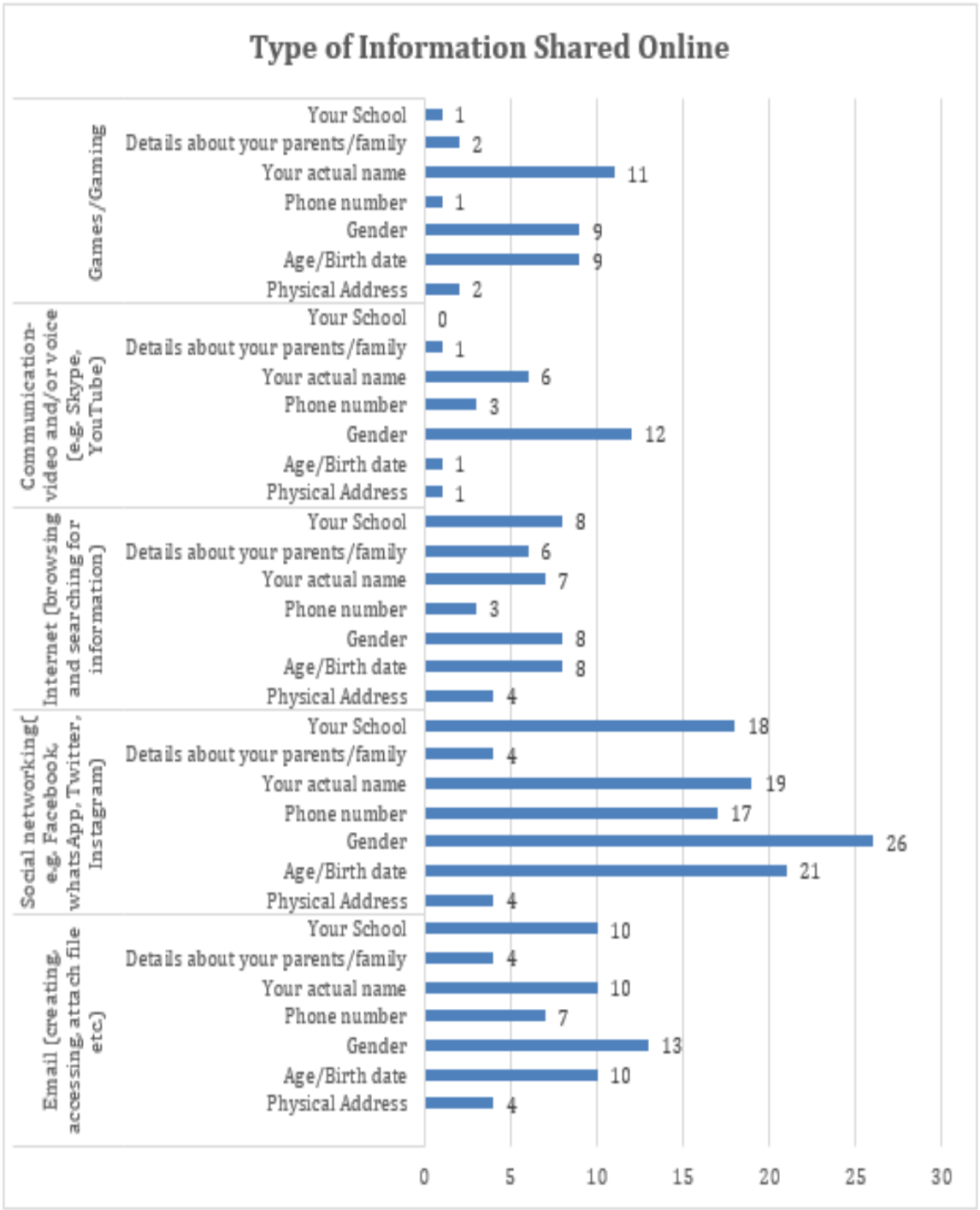


Figure 4.8: Type of information shared online

Respondents were further asked to indicate the type of information they have shared online with strangers when doing their activities on the Internet and the majority of respondents reported to have shared their gender while watching video clips, on social networking sites, and while playing Internet

games. The second most frequent information shared online with strangers was their actual name on social networking sites, their actual name while sending or receiving emails and while watching video clips. The third most frequent information shared was their age or date of birth on social networking sites, while sending and receiving emails (6), and playing Internet games, followed by sharing their phone numbers on social networking sites, while watching video clips and while sending and receiving emails as shown in Figure 4.9.

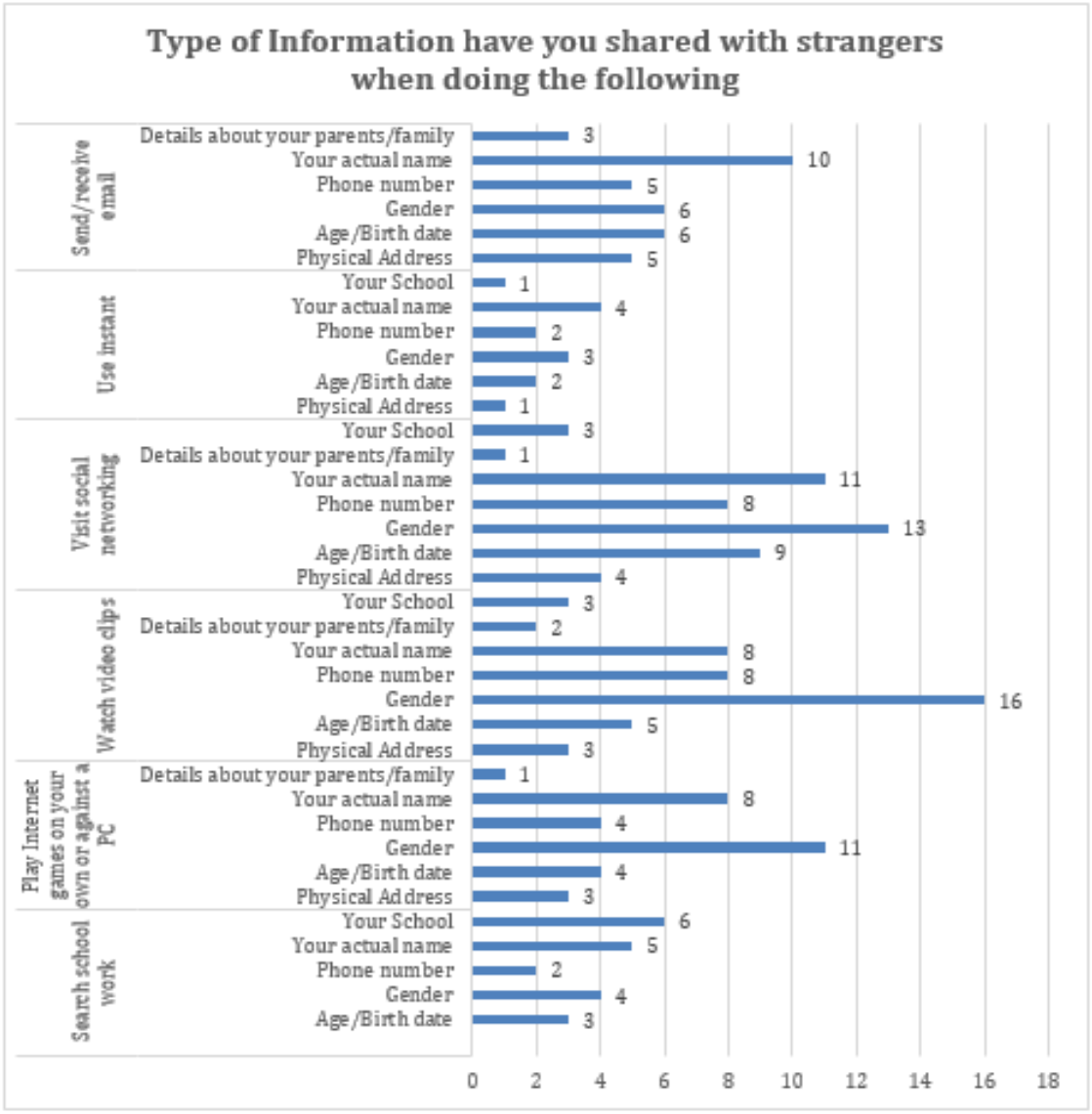


Figure 4.9: Type of information shared with strangers online

4.7.1. Would you share the following while online?

Respondents were asked if they would share the information outlined in Figure 4.10 while online. The results demonstrate that slightly more of the respondents are fully aware of the risks of sending personal information, adding people to their friends or contact that they never met face to face and sending a photo or video of themselves to someone they have never met face to face. While the other number of respondents reported that they occasionally but not always delete the record of which sites they have visited, look for new friends or contacts on the Internet (19) and pretend to be a different kind of person online from who they really are (19). Other respondents reported to always block unwanted adverts or junk mails/spams, always send a photo or video of themselves to someone they have never met face to face (12) and to always change filter preferences (10).

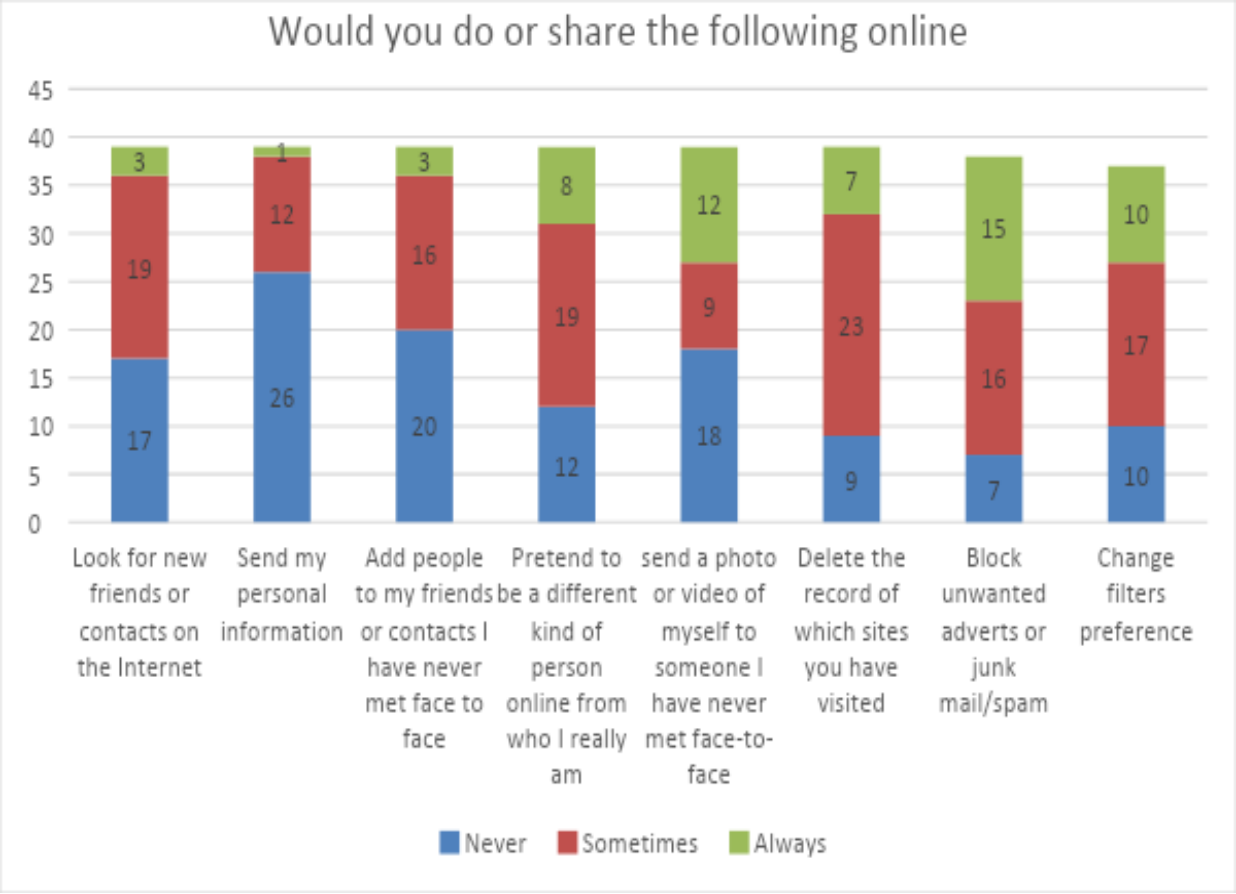


Figure 4.10: Would you do or share the following while online

4.7.2. Do you feel compelled to the following?

Respondents were asked if they felt compelled when strangers or friends present the following to them;

- To read and pay attention to friendly requests of strangers before accepting the request and 13 of the respondents reported to always and 8 to have never read when asked if they paid attention,
- To be polite to strangers online (never 20 respondents, sometimes 14 respondents and always 4 respondents),
- To understand the request presented to them by a stranger online (never 19 respondents, sometimes 15respondents and always 4 respondents),
- Taking advantage of the weakness of other online friends (never 20 respondents, sometimes 2 respondents and always 7 respondents), and
- To please others on the Internet (never 17 respondents, sometimes 6 respondents and always 4 respondents).

The results demonstrate that the majority of respondents are fully aware of the importance of reading and paying attention to details presented to them on the Internet before responding to it but only a few of them don't really understand the importance of reading and paying attention to requests presented to them on the Internet before accepting them. A moderate of respondents feel compelled to be polite to strangers online and to understand the request presented to them by a stranger online as shown in Figure 4.11.

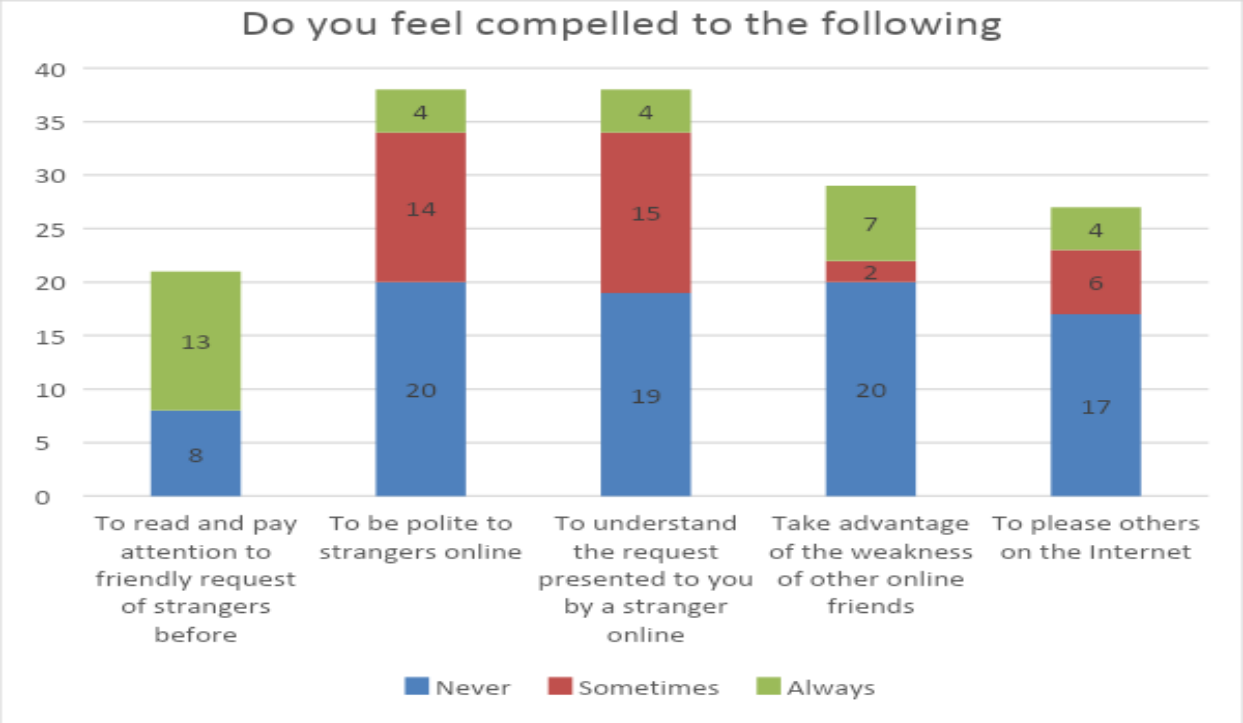


Figure 4.11: Feel pressured towards the following

4.8. Negative online experience

The questionnaires contained questions related to the interaction of respondents to a range of online negative experiences and how they felt about such experiences. Respondents to the questionnaires were asked if they had ever encountered a variety of negative online events relating to content, contact and conduct risk behaviour in their lives. From the respondents, the most prevalent forms of negative online experience was the content related risk in the form of commercial content, pornography or sexual content and seeing scary content. For example, 62.5 % of the respondents reported having seen commercial content (e.g. advertising to make money), another 62.5% of respondents reported having seen pornographic or sexual content (e.g. see naked people, etc.), while 60% had seen scary content, 55% had seen gory content (e.g. blood, pain, etc.) and content about drugs, and 52.5% had seen hateful content. Where 13 respondents felt fear to seeing scary content, 12 respondents had a positive reaction to commercial content, 11 respondents felt disgusted at seeing pornographic or sexual content and 10 respondents felt fear to seeing violent/aggressive content.

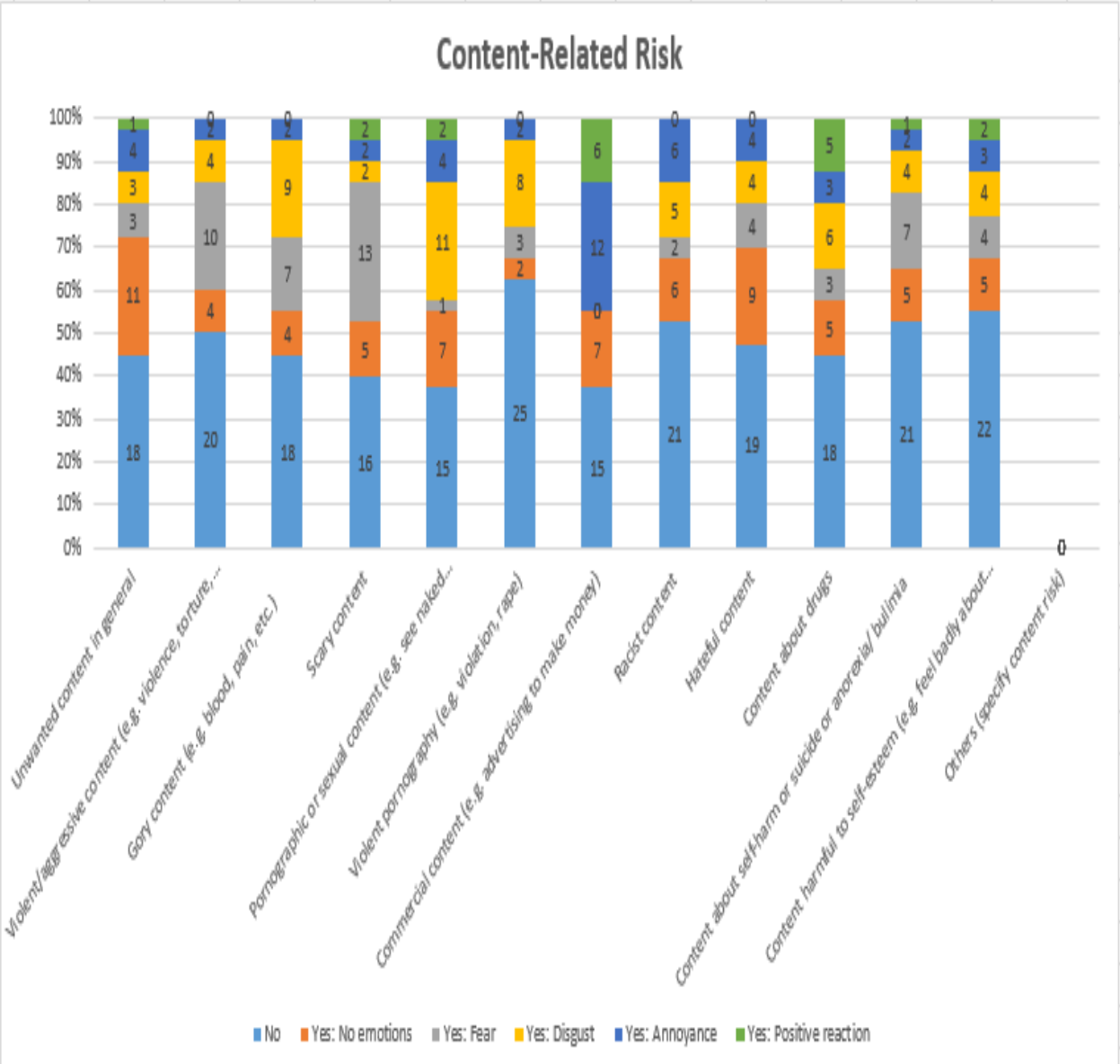


Figure 4.12: Content risk

From the analysis, it is reported that children that mostly visit social networking sites, watch videos online and that reported to be downloading music on the Internet are the ones that reported to have experienced content risk.

The larger number of respondents found out that they had not encountered most of the online contact-related risks, while only a few respondents indicated that they had contact risk related experience such as people pretending to be someone else, the possibility of inappropriate contact from strangers, face

to face meetings following online contact, actual or attempted inappropriate content in general and ideological or religious or fundamentalists' influence and shared how they felt about the encounter as shown in Figure 4.13.

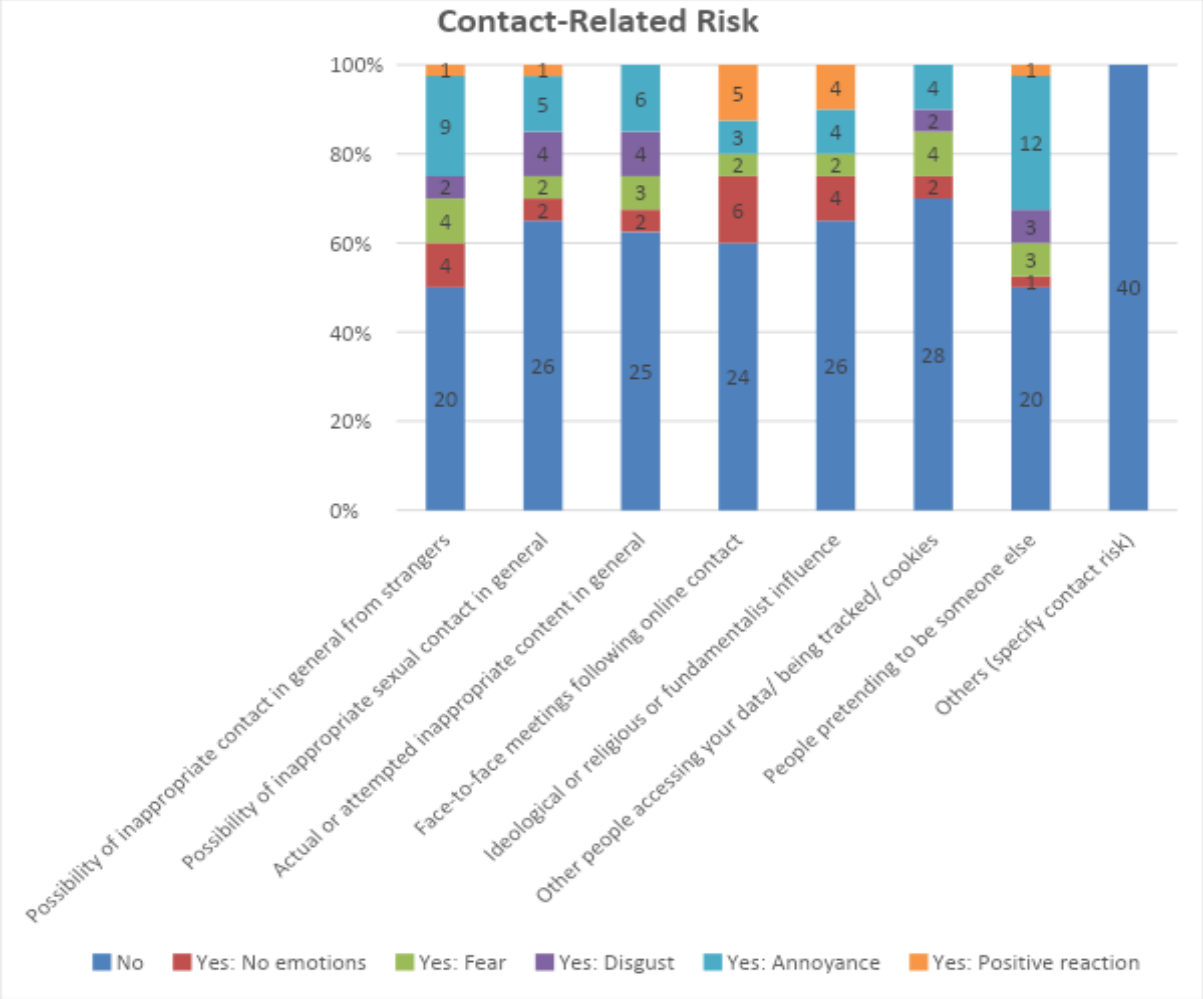


Figure 4.13: Contact risk

From this analysis, it is reported that children that mostly share their phone numbers over the Internet are the ones that reported to have inappropriate contact and face-to-face meetings after online contact with strangers.

The results show that 6 respondents had no emotions, 2 respondents felt fear, 5 respondents felt positive and 3 respondents felt annoyed to have had face-to-face meetings following online contact. Furthermore, respondents were asked whether one or more of the following conduct related risks had ever been

encountered. A larger number of respondents found out that they had not encountered most of the online conduct related risks, while only a few respondents indicated that they had experienced conduct related risks and shared how they felt about the encounter as shown in Figure 4.14.

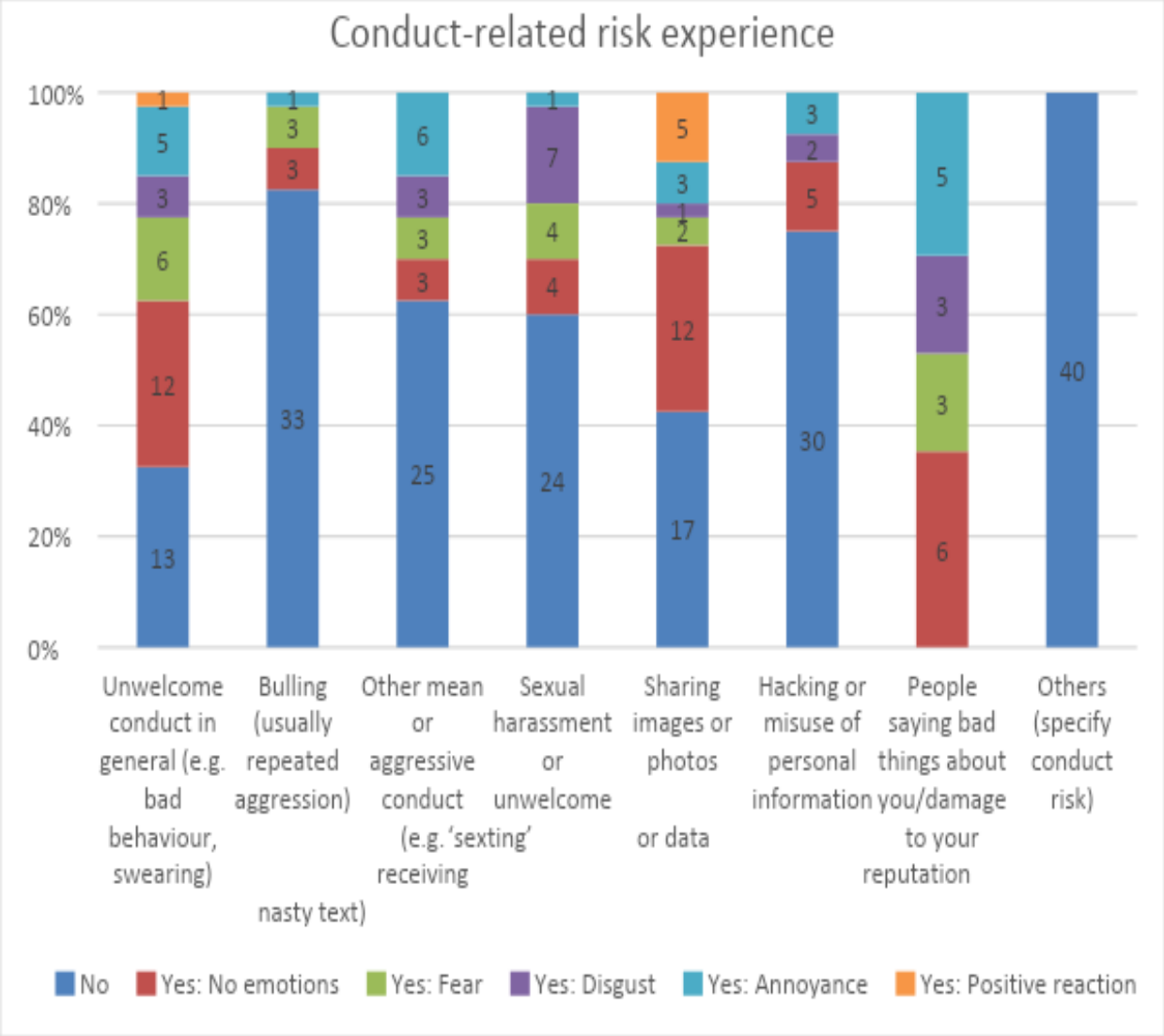


Figure 4.14: Conduct related risk experience

From the analysis, children that reported to have experienced online risks are children that reported to have spent most of their time on the Internet and reported to have shared personal information online. This means that, the more time children spend and the more information they share online on the Internet, the higher the likelihood of them being exposed to online risks.

4.8.1. Other Internet use related risks

Respondents were asked whether they had ever experienced one or more of the following other Internet use related risks. Quite a larger number of respondents indicated that they had not encountered most of the other Internet use related online risks, while only a few of respondents indicated that they had experienced other Internet use related risks and shared how they felt about the experience. These were as follows:

- Give out information to strangers: 6 respondents had no emotions, 1 respondent felt fear, another 1 respondent felt disgusted, while 2 respondents had a positive reaction,
- Gambling: 3 respondents had no emotions, 1 respondent felt fear, another 1 respondent felt annoyance while the other 1 respondent had a positive reaction,
- Spam, phishing, scams, fraud (e.g. fraudulent information): 4 respondents had no emotions, 2 respondents felt fear, 3 respondents felt disgust, while another 3 respondents felt annoyance,
- Illegal downloading: 7 respondents had no emotions, 1 respondent felt annoyance while 4 respondents had a positive reaction,
- Spending too much time online (e.g. missed homework, sleep): 17 respondents had no emotions, 3 respondents felt fear, 2 respondents felt disgust, 4 respondents felt annoyance and 3 respondents had a positive reaction,
- Health related risks (muscular, eye-sight, etc.): 7 respondents had no emotions, 9 respondents felt fear, 1 respondent felt disgust, 3 respondents felt annoyance, while another 3 respondents had a positive reaction,
- Lack of Internet safety in general: 5 respondents had no reactions, 2 respondents felt fear, 1 respondent felt disgust and 2 respondents had a positive reaction,
- Related to hardware/software (e.g. breakdown, install, etc.): 6 respondents had no emotions, 2 respondents felt fear, 5 respondents felt annoyance and 1 respondent had a positive reaction,
- Related to search (e.g. hard to find information): 3 respondents had no emotions, another 3 respondents felt fear, 1 respondent felt disgust, 10 respondents felt annoyance, while 1 respondent had a positive reaction, and
- Virus (e.g. sites that come with virus): 5 respondents had no emotions, 2 respondents felt disgust, 3 respondents felt annoyance, while 1 respondent had a positive reaction.

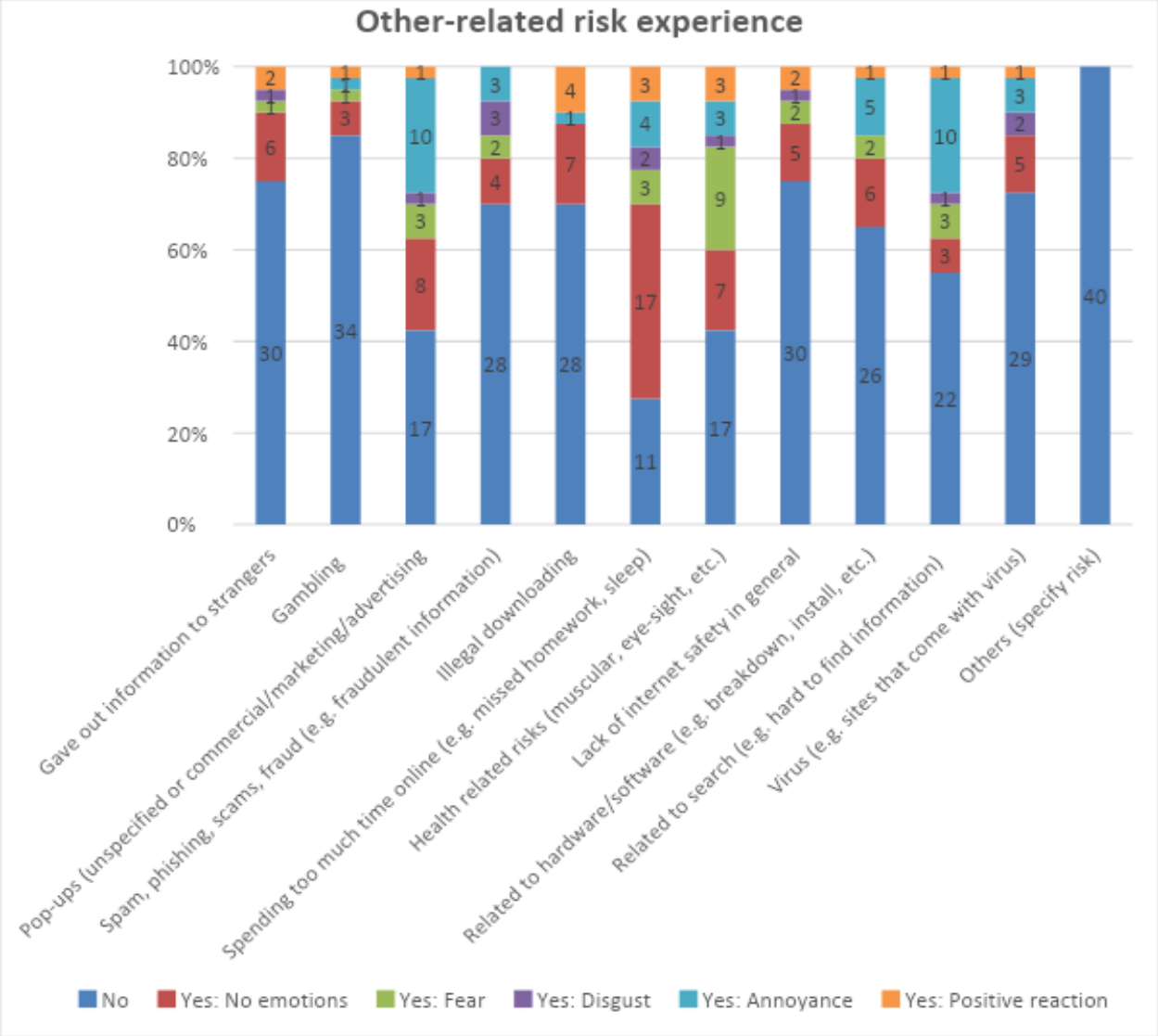


Figure 4.15: Other Internet use related risk

Looking at all the types of experiences together (content, conduct, contact and other Internet use related risk), our research paints a worrying picture of children spending too much time on the Internet where they may miss their homework or sleep.

4.8.2. Gender

With regards to gender, Livingstone et al. (2017) found that gender makes less changes in terms of Internet access and overall use of the Internet. From the participants that took part in the questionnaires, girls were more represented in the sample than boys as there were 24 girls and 16 boys.

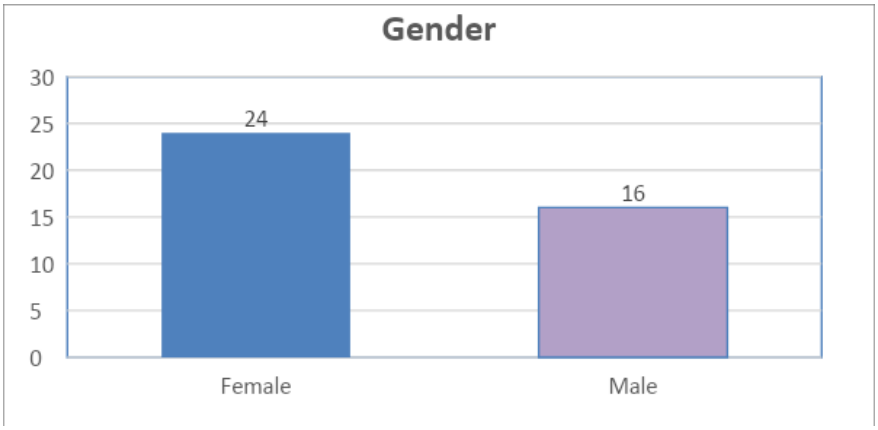


Figure 4.16: Total number of respondent based on gender

4.9. Chapter summary

In particular, from the analysis, we found that children mostly visit social networking sites, communication platforms like Skype or YouTube, and gaming platforms. The study also found out that the activities that children do on the Internet almost all the time include downloading music and posting photos, videos and music on social networking sites. Most children use smartphones to access the Internet by spending more than 6-10 hours per day and most of them access the Internet from home. The social networking sites that most of the children are frequently accessing are Facebook, WhatsApp, Snapchat and games. In addition, they share information like gender, age or date of birth, actual name, physical address and their school name with people they have never met in real life using the different social networking sites, emails, communication and gaming. A number of children also reported to have shared details about their parents or family while browsing or searching for information on the Internet. This means that when children download music or watch videos on the Internet they become more vulnerable to unwanted content, inappropriate contact and unwelcome conduct on the Internet.

Children that spend most of their time on social networking sites mostly reported to be experiencing the risk of spending too much time online where they would miss out on their homework or even miss their sleep. Additionally, they also reported to have experienced health related risks such as muscular challenges and eye-sight problems. This means that spending too much time on the Internet does not only pose Internet risk but can bring health related problems too.

From the analysis on the online risk experienced, it was found that some children reported to have negative experiences online. Although many children are aware of the risks and are taking appropriate

action in countermeasures response, the most common forms of online related risks ever experienced among respondents that completed the questionnaires are content-related risks. This report focused on the findings for the main experienced risks encountered by children and found the following:

- Content-related risk dominates children's risk experienced
- Conduct-related risk follows along with other related risk

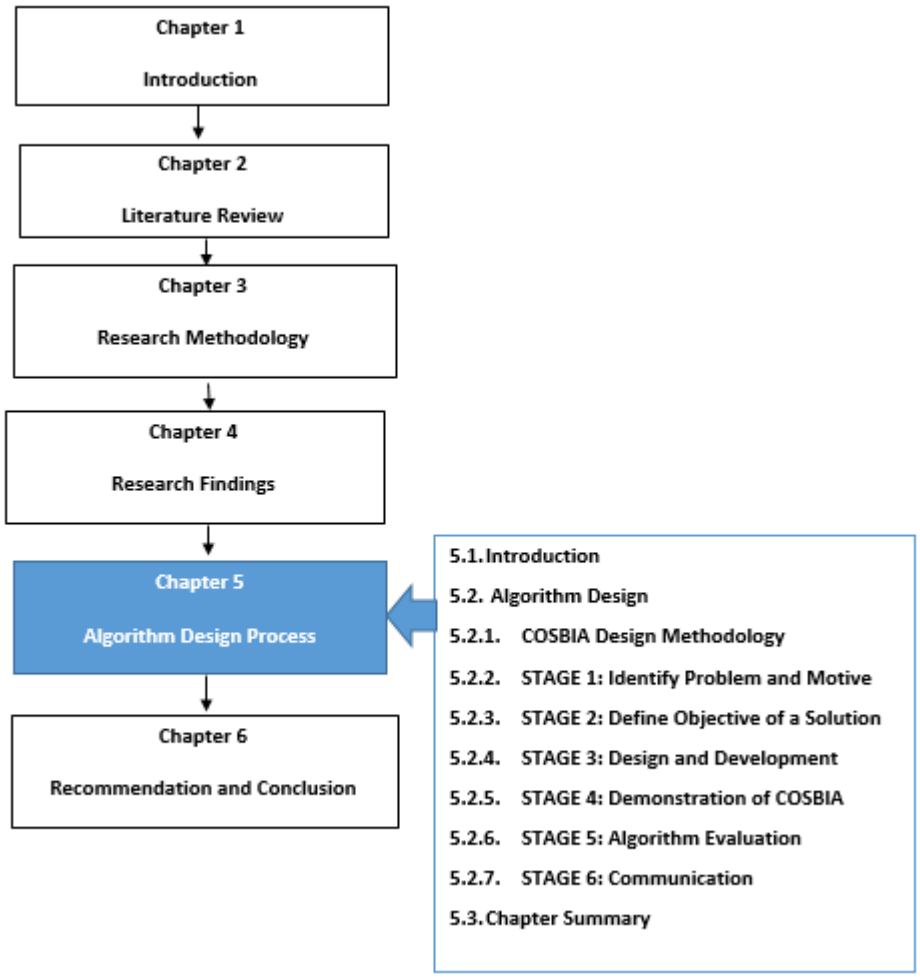
Key findings

- Children mostly visit social networking sites more frequently than other online platforms.
- Facebook is one of the social networking sites that children are mostly active on, followed by WhatsApp and Snapchat
- Children that download music or watch videos on the Internet become more vulnerable to unwanted content, inappropriate contact and unwelcome conduct on the Internet.
- Children that spend most of their time on social networking sites experience the risk of spending too much time online where they miss out on their homework or even miss their sleep and experience health related risks such as muscular challenges and eye-sight problems
- Children that spend more of their time on the Internet have more knowledge on most of the security settings that need to be configured on the Internet.
- Children can express themselves freely on the Internet more than in person and they share personal information on the Internet which could pose online risks to them.
- Most children have smartphones and have Internet at home, and this implies more opportunities for a child to obtain inappropriate Internet dangers because of the more time they spend on the Internet with little supervision.
- Children that mostly visit social networking sites watching videos online and downloading music on the Internet are the ones that mostly experience content risk.
- Children that mostly share their phone numbers on the Internet are the ones that experience inappropriate contact and face-to-face meetings after online contact with strangers.
- The more time children spend and the more information they share online on the Internet, the higher the likelihood of them being exposed to online risks.

Social media has become extremely popular and it is here to stay. The more children rely on social networking sites the more this will change their behaviours, awareness and emotional states. Therefore, it would add great value to influence children's behaviours on the Internet and raise their cyber security awareness in order to reduce online risks, although the risk is not on the majority of children as stated in Figure 4.12, Figure 4.13, Figure 4.14, and Figure 4.15. One type of activity that has been found to be a contributing factor to online risks, however, is face-to-face meetings after online contact with unknown people online by the respondents. In addition, children reported that they share personal information while on social media and through emails with people they do not know and that children pretend to be a different kind of person online from whom they really are. Amazingly, children reporting negative experiences have typically shown a higher level of knowledge about Internet activities. The next chapter discusses the approach that was used to design the algorithm.

Chapter 5: Algorithm Design

This chapter presents the design of the algorithm as outlined in the chapter map.



5.1. Introduction

The aim of this chapter is designing an algorithm that can influence the behaviour of children and raise their cyber security awareness as well as to lay a theoretical structure to guide the process of answering the fourth research question:

How can a suitable behaviour influencing algorithm be constituted to influence children's online activities?

To answer the research question as stated above, the study followed the steps of the Design Science research process proposed by Peffers, Tuunanen and Rothenberger (2020) as illustrated in the next section.

5.2. Algorithm design

An algorithm is a collection of well-defined necessary steps to accomplish a specific purpose. It often typically involves transforming a system from one state to another, probably through a series of intermediate states along the way (Harris & Ross, 2006, Erickson, 2019). This section outlines the algorithm that was designed to influence the behaviour of children and raise their cyber security awareness. This was achieved by defining the main algorithm components and relationships and applying existing knowledge on secure online behaviour for children. Figure 5.1 outlines the design of the Child Online Secure Behaviour Influencing Algorithm (COSBIA).

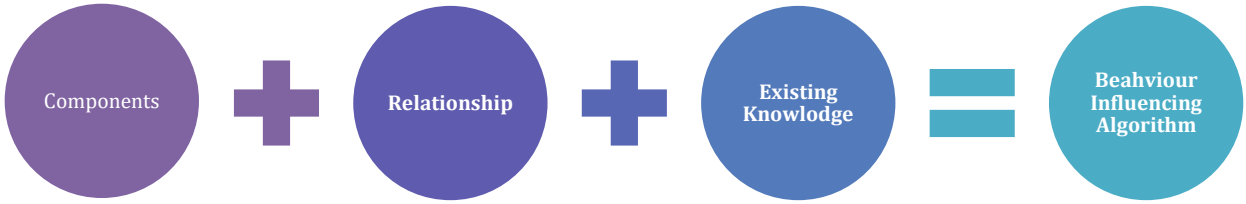


Figure 5.1: Algorithm Design

5.2.1. COSBIA design methodology

This research followed the steps of the Design Science research method suggested by Peffers, Tuunanen, and Rothenberger (2020) as outlined in the next section to address the research question mentioned in section 5.1. The process of research using design science starts with an understanding of the problem. This is achieved by analysing the literature and studying the phenomenon. Once the problem is identified and the researcher is made aware of it, the next step is to identify ideas which could solve the problem. These ideas are taken from the domains which are considered important to solve the problem. The artefacts are then generated and tested based on the recommendation, as a solution to overcome the specified problem. Figure 5.2 illustrates the algorithm design process.

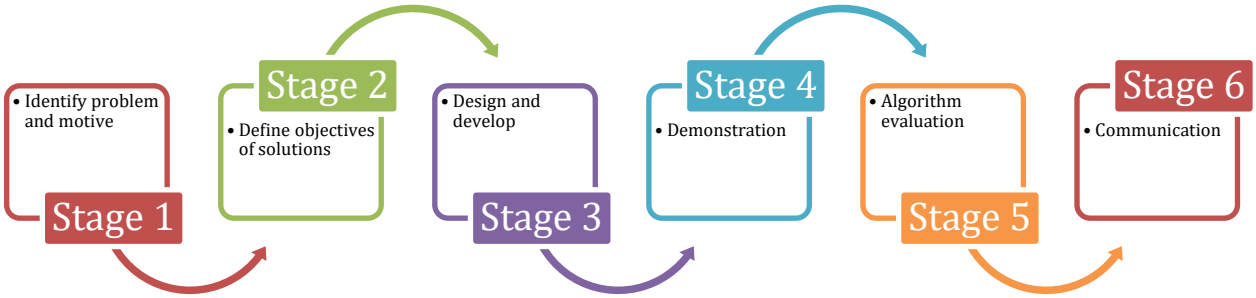


Figure 5.2: Algorithm design process (Source: Peffers, Tuunanen & Rothenberger, 2020)

5.2.2. STAGE 1: Identify problem and motive

Stage 1 involved identifying the problem, using literature and a survey, and the problem was identified as:

Out of innocence, the behaviour of children potentially exposes them to cyber criminals as they innocently share information and befriend strangers.

A child uses the Internet to visit social networking platforms, search for information, play games and to send or receive emails. Using their past experience and devices, the child shares personal information, shares emotions and feelings on their status, downloads music, and posts photos and videos on the Internet. Based on the particular online activities, online behaviours, prior knowledge, online platforms, online threats and online experience of a unique child, children's online interactions may lead to a secure experience or an insecure experience. Figure 5.3 illustrates the inputs (gadget, prior knowledge, online platforms, online activities, online behaviour, online threats and the online experience) and the output (experience).

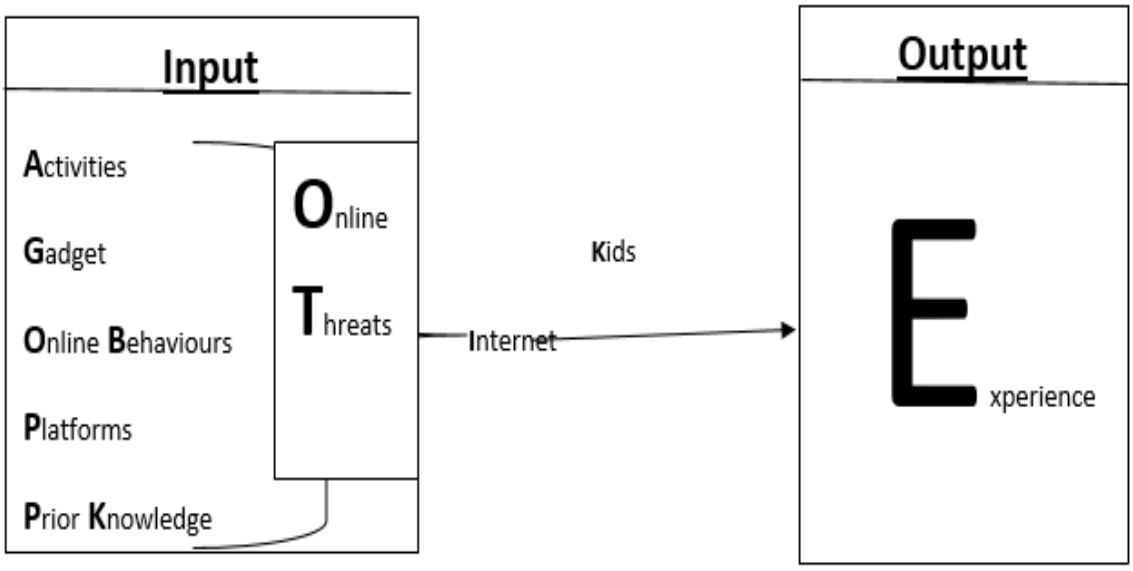


Figure 5.3: Input and output to the research problem

Children's behaviour could expose them to cyber criminals through innocently sharing information, posting photos and messages about themselves and making friendships with strangers. This led to the identification of COSBIA's objectives presented in the next section.

5.2.3. STAGE 2: Define the objective of a solution

The research objective was to **design an algorithm that can influence children's behaviour on the Internet in order to reduce cyber security risk**. To achieve this objective, the following objectives were achieved by COSBIA as outlined in Figure 5.4, which illustrates the functionality of the algorithm.

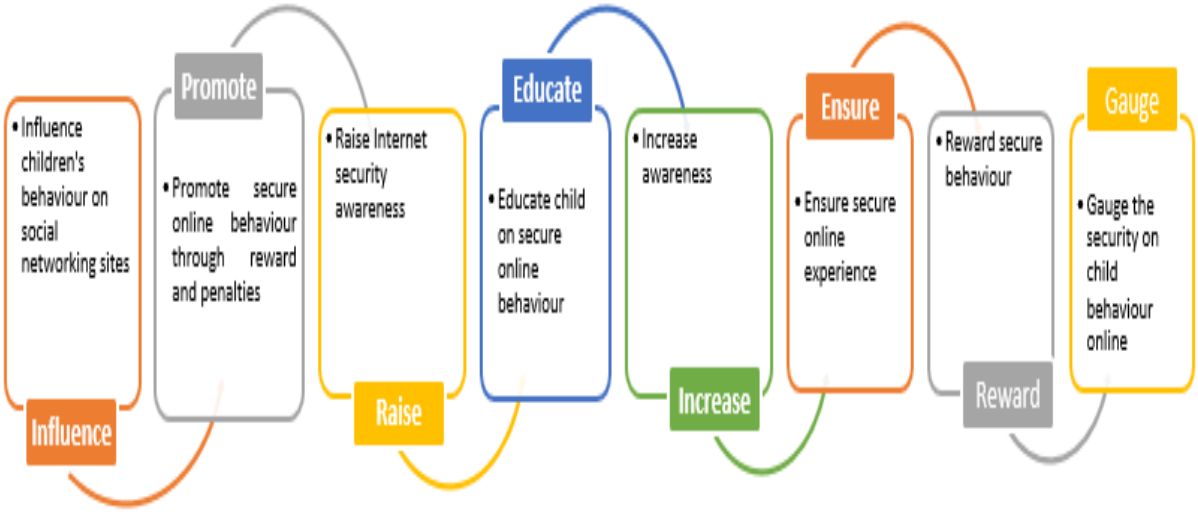


Figure 5.4: Algorithm functionality

The designed algorithm focuses on influencing children's behaviour on social networking sites by promoting secure online behaviour through rewards and penalties. It focuses on raising Internet security awareness and educating the child on secure online behaviour to achieve secure online experience. The algorithm also ensures secure online experiences by rewarding secure behaviour and finally gauges the security on the child's behaviour online. The next section outlines the design and the development of the algorithm.

5.2.4. STAGE 3: Design and development

This section presents the design and development process followed by coming up with the algorithm informed by literature in Chapter 2: and findings in Chapter 4:. Components of the algorithm, relationships and the architecture are presented.

5.2.4.1. Algorithm components identification

The study has identified from the literature and research findings a detailed list of components and their subcomponents that are key to the algorithm for influencing children's behaviour and raising their cybersecurity awareness as illustrated in the Table 5.1.

Table 5.1: Algorithm components

Set	Component	Sub-Set	Sub-components	Definition
SC	secure children online	OB	Online Behaviours	A secure child who behaves securely online Positive behaviour (PB), Negative behaviour (NB), Threatening behaviour (TB), Vulnerable behaviour (VB), Secure behaviour (SB), Online Gadget behaviour
		OE	Online Experiences	Positive online experience (POE), Negative online experience (NOE), Threatening online experience (TOE), Vulnerable online experience (VOE), Secure online experience (SOE), Happy online experience (HOE), Miserable online experience (MOE), Context of Use (COU)
		K	Knowledge	Good Internet Security knowledge (GISK), Poor Internet security knowledge (PISK), Online Platform Knowledge (OPK),Gadget Knowledge (GK), Online Activities Knowledge (OAK), Prior knowledge (PK), New knowledge (NK), Developing Knowledge (DK)
		G	Gadgets- smart gadgets used to access the Internet	Smart phone (SP), Ipad/Tablet (IP), Laptop (LP), Personal Computer (PC), School computer (SC), Game console (GC), Ipod (I)
		OP	Online platforms - used by children :	Chat (C), Tik Tok (TT), Facebook (FB), WhatsApp (WA), Instagram (I), Hangouts (HO), Twitter (T), Skype (S), MySpace (MS), Snapchat (SC), LinkedIn (LI), Gaming (G)
		OA	Online activities - children love to perform online	Watching videos (WV), Gaming (G), Information search (IS), Studying (S), Social Networks (SN), Emailing (E)
		OT	Online threats - children are exposed to online:	General Internet threats (GIT), OP specific threats (OPST), OA specific threats (OAST), G specific threats (GST), B specific threats (BST)
		E	Empowerment - is a set of interventions that will foster	Security knowledge (SK), Secure behaviour (SB), Secure experience (SE), Reduce exposure to online threats in the actors over time (RE)
		TSO	Time spend online	At least daily (LD), At least weekly (LW), At least monthly (LM), Almost all the time (AT)

5.2.4.2. Components relationship

With little knowledge and awareness, children's behaviour online potentially exposes them to cyber criminals because they innocently share information and interact with strangers. In particular, children voluntarily share personal and private information about themselves from which cybercrimes may emerge in their real world or virtual environment, if this shared information ends up in the wrong hands. A set theory was used in this study. An illustration of the relationship between the sub components from Table 5.1 is presented in the Venn diagrams in Figure 5.5, Figure 5.6 and Figure 5.7.

Relationship 1: A child (C) interacts with an Online Platform (OP) to perform Online Activities (OA) using a smart gadget (G). The Time Spent Online (TSO) and the child's Online Behaviour (OB) while performing OA on an OP using G results in a child's online experience (OE) which can either be secure or insecure. This is due to the fact that G has an influence on OB, which results in gadget specific behaviour (OGB) and OP has an influence on OB which results in platform specific behaviour (OPB). Figure 5.5 represents relationship 1. In set notation, OE(C) is a result of time spent online (TSO) over set of G, OA, OP, OB.

Equation 5.1: $OE(C) = TSO*(G+OA+OP\ (OPB)\ +OB\ (OGB))$

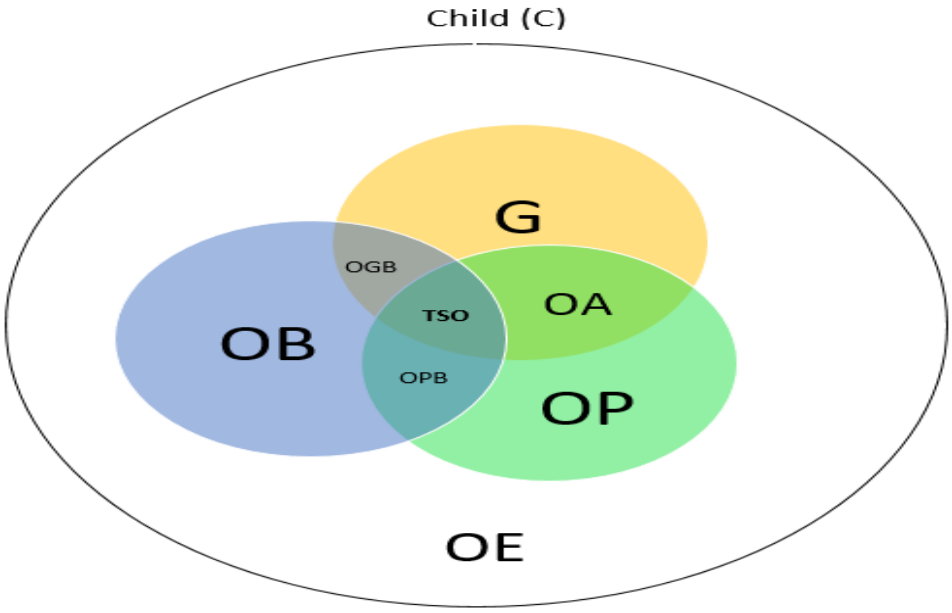


Figure 5.5: Component relationship 1

Relationship 2: The children's (C) prior knowledge (PK) and their online behaviour (OB) exposes them to online threats (OT) inherent in G, OA and OP. This results in a child's online experience (OE). If empowerment is added to this interaction, it would result in a secure online behaviour (SOB). We posit that a secure online experience (SOE) is a result of secure online behaviour and this relationship is shown in Figure 5.6 . SOE (C) is a result of applying a set of E to enhance PK and OB of/with OA, OP, and G in the presence of OT.

Equation 5.2: $OB = OP+G+OA+PK+OT+OE$

Equation 5.3: ***OE= OB*(OP+G+OA+PK+OT)***

Equation 5.4: ***SOB = OE+E*(G, OA, OP, OB)***
SOB = SOE

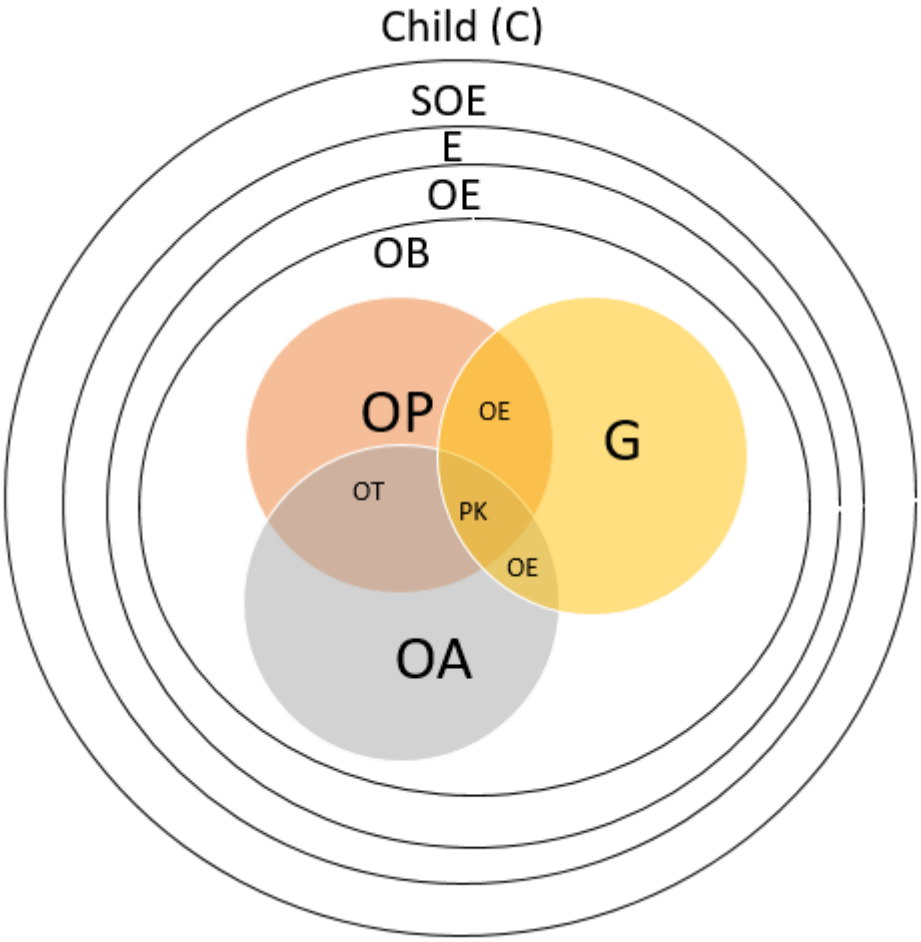


Figure 5.6: Component relationship 2

Relationship 3: A child (C) interacts with an Online Platform (OP) using a smart gadget (G) to perform Online Activities (OA). Adding prior knowledge while using the gadget (G) results in the gadget knowledge (GK). Adding prior knowledge (PK) while interacting on online platforms results in online platforms knowledge (OPK). When one adds prior knowledge to the gadget and online platform influence, online behaviour (OB) is the presence of online threats (OT). If empowerment is added then secure online experience (SOE) is the result.

Equation 5.5: ***OE= OB *(G+OP+PK)*OT)***

Equation 5.6: ***SOE= OE + E*(G+OP+PK+OT)***

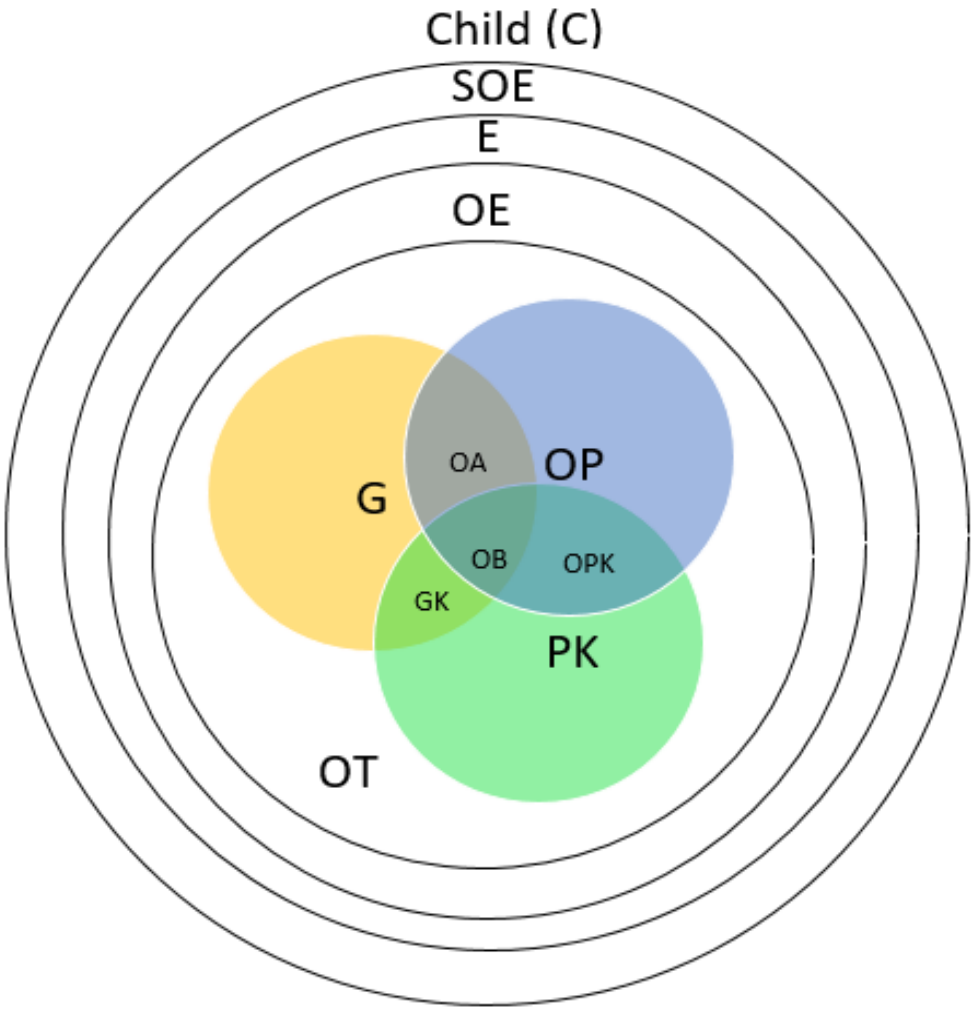


Figure 5.7: Component relationship 3

Algorithm definition

A child (C) interacts with an Online Platform (OP) to perform Online Activities (OA) using a smart gadget (G). The Time Spent Online (TSO) and the child's Online Behaviour (OB) while performing OA on an OP using G results in a child's online experience (OE) which can either be secure or insecure as depicted in Equation 5.1. This is due to the fact that G has an influence on OB as shown in Equation 5.2, which results in gadget specific behaviour (OGB) and OP has an influence on OB which results in platform specific behaviour (OPB).

The children's (C) prior knowledge (PK) and their online behaviour (OB) expose them to online threats (OT) inherent in G, OA and OP, and this results in a child's online experience (OE) shown in Equation 5.3 and Equation 5.4.

If empowerment is added to this interaction, it would result in a secure online behaviour shown in Equation 5.5 and Equation 5.6. We posit that a secure online experience (SOE) is a result of secure online behaviour.

5.2.4.3. Algorithm architecture

In this section, the architecture shown in table 5.2 and the formulation on what the COSBIA is required to accomplish is outlined.

Table 5.2: COSBIA Architecture

Set	Component
C	Secure children online (actor) is a set of (c)
PK	Prior knowledge is a set of (i)
G	Gadget is a set of (y)
OA	Online activities is a set of (n)
TSO	Time spend online is a set of (o)
SOE	Secure online experience is a set of (s)
GK	Gadget prior knowledge is the intersection of PK and G
OGB	Online Gadget Behaviour is an intersection of G and OB
OT	Online threats is a set of (t)
OP	Online platforms is a set of (m)
OB	Online behaviour is a set of (x)
OE	Online Experience is a set of (a)
E	Empowerment is a set of (e)
SOB	Secure online behaviour is a set of (b)
OPK	Online Platform Prior Knowledge is the intersection of OP and PK
OPB	Online Platform Behaviour is an intersection of OP and OB

5.2.4.4. COSBIA formulation

The algorithm is required to influence children's behaviour online and raise their cyber security awareness. A structured approach was used to describe the problem and the processing was divided into individual tasks or functions. Table 5.3 shows what is required to formulate the COSBIA.

Defining diagram of Child Online Secure Behaviour Influencing Algorithm (COSBIA)

Table 5.3: COSBIA defining table

Input	Processing	Output
unique child online • Smart Gadgets • Prior Knowledge • Time spend online • Online platforms • Online activities • Online behaviour • Online threats • Online experience	**Read** child's online experience = Time spend online *(Gadget + Online activities + Online platforms + online behaviour) **Compute** Online Behaviour = Online platform + Gadget + Online activities + Prior knowledge + online threats + online experience **Compute** Online experience = Online behaviour *(Online platforms + Gadget + Online activities+ Prior knowledge + Online threats) **Compute** secure online behaviour = Online experience + Empowerment * (Gadget, Online activities, online platforms, Online behaviour) **Compute** secure online behaviour = secure online experience **Print** online experience, online behaviour, online secure knowledge	Online experience, Online Behaviour Online security knowledge

Table 5.3 defines the algorithm, and this programme is required to read from the screen child's online experience = Time spent online * (Gadget + Online activities + online platforms + online behaviour) of the unique child's visiting the Internet. The algorithm should then compute online behaviour, online experience and secure online behaviour. In addition, print (display) online experience, online behaviour and online knowledge required to getting a secure online experience for the unique child. In the algorithm, **Read** represents the input; **Compute** represents the process and **Print** represents the output (Write or Display).

- **Problem:** Children behave insecurely online
- **Inputs:** A set **OA** of (n) online activities where n is a finite number of possible activities that can be performed by the child (C). A set **OP** of (m) online platforms where m is a finite number of possible platforms visited by the child. A set **G** of (y) smart gadgets where y is a finite number of possible gadgets that can be used to access the Internet by the child. A set **OB** of (x) online behaviours where x is a finite number of possible behaviours that can be performed by the child. A set of P**K** of (i) prior knowledge where i is a finite number of possible knowledge that a child has about the Internet, the gadget the child is using, the online platform the child is accessing and the activity the child is performing. A set of **OE** of (a) online experience where a is a finite number of possible experiences that a child has on the Internet. A set of **OT** of (t) outlines threats where t is

a finite number of possible threats that a child can be exposed to while on the Internet. A set of **TSO** of (o) time spent online where o is the finite number of possible time spent on the Internet by the child.

- **Processes:** A series of set **E** of (e) empowerment which are curried out in order to achieve a set **OB** of (x) and a set of **OE** of (a). A set of **OB** of (x) online behaviours where x is a finite number of possible behaviour that can be performed by the child resulting in secure online behaviour which is a subset of OB. A set of **OE** of (a) online experiences where a is a finite number of possible experiences that a child has on the Internet.
- **Outputs:** A set of **OE** of (a) online experiences where a is a finite number of possible experiences that a child has on the Internet, A set **OB** of (x) online behaviours where x is a finite number of possible behaviours that can be performed by the child and online secure knowledge which is a subset of knowledge (K)

5.2.4.5. COSBIA

To design the solution algorithm of COSBIA, this study adopted the set theory. Brown et al. (2011) describe a set as a collection of objects which are called the set elements that has to be well defined, meaning that it can describe and list its elements without ambiguity.

Describing the COSBIA set

- OPm = {Chat, Tik Tok, Facebook, WhatsApp, Instagram, Hangouts, Twitter, Skype, MySpace, Snapchat, LinkedIn, Gaming}
- OAn = {Watching videos, Gaming, Information search, Studying, Social Networks, Emailing}
- Gy = {Smart phone, Ipad/Tablet, Laptop, Personal Computer, School computer, Game console, Ipod}
- TSOo = {At least daily, At least weekly, At least monthly, Almost all the time}
- OBx = {positive, negative, threatening, vulnerable, secure}
- OEa= {Positive online experience, Negative online experience, Threatening online experience, Vulnerable online experience, Secure online experience, Happy online experience, Miserable online experience, Context of use}
- PKi = {Good Internet Security knowledge, Poor Internet security knowledge, Online Platform Knowledge, Gadget Knowledge, Online Activities Knowledge, Prior knowledge, New knowledge, Developing Knowledge}

- OTt = {General Internet threats, Online Platform specific threats, Online Activities specific threat, Gadget specific threats, Behaviour specific threats}
- Ee = {Security knowledge, Secure behaviour, Secure experience, Reduce exposure to online threats in the actors over time}
- SOE = {Internet security, safe behaviour, and safe interaction online to reduce exposure online threats that result in a secure child online}
- SOB = {Proper Internet etiquette}

A child (C) interacts with an Online Platform (OP) to perform Online Activities (OA) using a smart gadget (G). The Time Spent Online (TSO) and the child's Online Behaviour (OB) while performing online activities (OA) on an online platform (OP) using a gadget (G) results in a child's online experience (OE).

Equation 5.7

$$OEa^{c}\ (C) = TSOo\ *(\ Gy + OAn + OPm\ (OPB) + OBx\ (OGB))$$

This is due to the fact that the gadget (G) has an influence on online behaviour (OB), which results in gadget specific behaviour (OGB) and the online platform (OP) has an influence on online behaviour (OB) which results in platform specific behaviour such as online platform behaviour (OPB). The children's (C) prior knowledge (PK) and their online behaviour (OB) exposes them to online threats (OT) inherent in G, OA and OP, and this results in a child's online experience (OE) .

Equation 5.8

$$OBx^{c} = OPm + Gy + OAn + PKi + OTt + OEa$$

Equation 5.9

$$OEa^{c} = OBx\ *(\ OPm + Gy + OAn + PKi + OTt)$$

If empowerment is added to this interaction, it would result in a secure online behaviour. We posit that a secure online experience (SOE) is a result of secure online behaviour.

Equation 5.10

$$SOB = OE + E*(\ Gy,\ OAn,\ OPm,\ OBx)$$
$$SOB = SOE$$

COSBIA Gamification

Start

Read Gadget; online platforms; online activities

Compute online behaviour and online experience

Display online experience and online behaviour

IF Online experience = secure online experience, then
Get crown THEN
Move to next level
Else
While online experience = insecure online experience, then
DO
Get empowerment, UNTIL empowerment score = 3, THEN
Move to step 6
DONE

Compute secure online behaviour
If online behaviour = secure online behaviour, THEN
Get a crown THEN
Move to step 11
ENDIF
WHILE online behaviour! = secure online behaviour
DO
Get Empowerment
UNTIL (Empowerment score = 3) THEN
Move to step 9
DONE

Display Online secure knowledge

Return to activity

Pseudo code explanation

Step1: The child goes on the Internet, COSBIA reads the gadget the child is using, the online platform the child is visiting and the online activities the child is performing.

Step 2: COSBIA should then analyse the child's online experience and online behaviour based on step 1.

Step 3: After analysing the child's online experience and online behaviour, COSBIA should then display the child's online experience and behaviour, if the child's online experience is insecure, the child gets

empowerment until the score is 3 for them to move to the next level. If the child scores less than 3 the child has to continue to get empowerment until the score 3 then moves to the next level.

And if the child's online experience is secure the child gets a crown then moves to the next level which is analysing online behaviour. If online behaviour is secure, the child gets a crown then returns to the activity. If the child's online behaviour is insecure the child gets empowerment until the child gets a score of 3, then the child gets a crown. COSBIA then displays online secure knowledge, and the child can then return to the activity.

Score

0-2 correct answers: The child doesn't know much about the Internet, the child needs to get empowerment

3 correct answers: The child is at the beginning of the journey to become a safe Internet user and has started thinking about others online

4-6 correct answers: The child is on the way to becoming a safe Internet user and a good friend to others.

7-9 correct answers: The child is well on the way to becoming a responsible Internet user and a great online friend, and making some very sensible choices.

10 correct answers: The child is a friendly and caring Internet user who does brilliantly online.

5.2.4.6. COSBIA flowchart

Flow charts are used to represent an algorithm according to Yasseen (2013). It is a diagram that shows the data flow through data processing. A flow chart explains the operations that are required to solve a specific problem, and it can be interpreted as a blueprint of a system designed to address a problem (Yasseen, 2013). In this study, an algorithm was designed to influence children's behaviour online and raise their cyber security awareness. An online game was used to implement and evaluate the algorithm. Sălceanu's (2014) study outlined that computer game content has great potential to improve the lives of children and adolescents. Children are able to access the game on the Internet at anytime and anywhere. A flow chart for an algorithm can read the child's online experience then compute online behaviour (analyse clickstreams, interaction, activity pattern and mine browsing information), online experience and secure online behaviour. Then print the online experience and online behaviour, if online experience is equal to an insecure online experience then Get Empowerment; if the score of empowerment is equal to three, then move to next level; if empowerment is not equal to three then go back to empowerment. If online experience is not equal to insecure, then get a crown and move to the next level. Compute secure online behaviour and if online behaviour is equal to secure online behaviour, then get crown, display

online secure knowledge and stop. If online behaviour is not equal to secure online behaviour then go back to get empowerment until the empowerment score is equal to 3 then move to the next level, compute secure online behaviour. If online behaviour is equal to secure online behaviour, then get a crown displaying online secure knowledge and stop. The flow of the algorithm is presented in the flowchart in Figure 5.8.

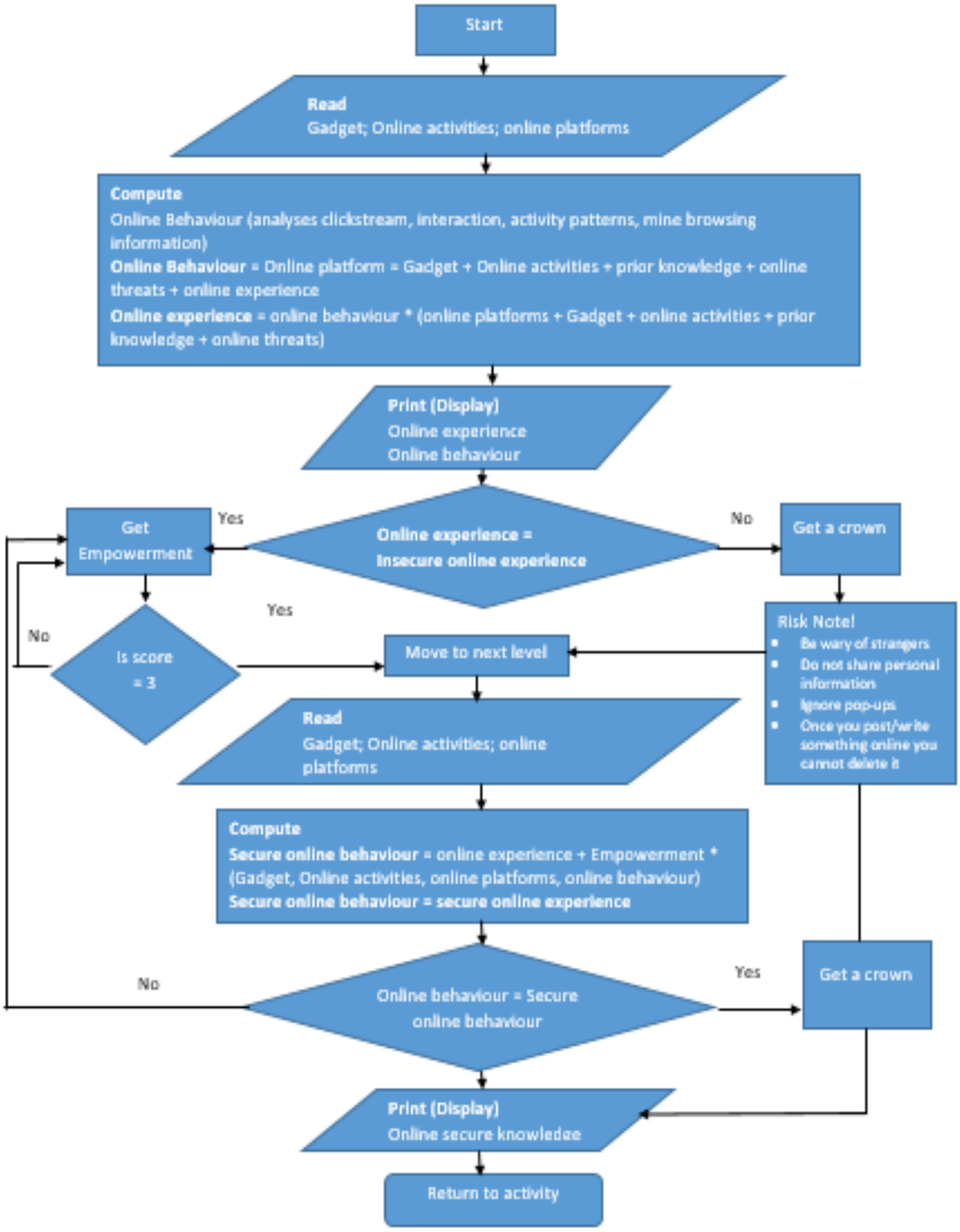


Figure 5.8: COSBIA flowchart

5.2.5. STAGE 4: Demonstration of COSBIA

Inspired by persuasion theory, gamification of COSBIA was used and the concept was fully detailed. The COSBIA game focuses on influencing children's behaviour on social networking sites by promoting secure online behaviour through rewards and penalties. It focuses on raising Internet security awareness and educating the child on secure online behaviour to achieve secure online experience. The COSBIA game also ensures secure online experiences by rewarding secure behaviour and finally gauges the security on the child's behaviour online. The COSBIA game determines the online threats based on a database of known threats, and the level of assertiveness is measured through a quiz that covers online threats on online platform specific threats, online activities specific threats, gadget specific threats and online behaviour specific threats. The main idea is for the child (player) to come and perform whatever the child wants to perform on the Internet and be empowered through a game. What the COSBIA does is that it reads information of the child's gadget being using, the platforms visited, the activities the child is performing and the way the child is behaving. When it reads the information there is a database and in the database there are identified threats for those different platforms, activities, behaviours and the gadget being used. For example, if you are preparing for an android phone, the app reads the gadget as Samsung S20, reads that the child is using Facebook (platform), and reads that the child (player) is chatting (activity). Now that is has this information, the first thing that it should do is to evaluate whether the child knows the threats inherent is these things, that's level 1 of the game. Now the child (player)'s knowledge is determined; the next thing is for the algorithm to check how the child (player) is navigating in the environment. The algorithm should read how they are clicking etc. and based on that, then it can evaluate if the child (player) is secure or insecure.

An online hackathon was hosted to demonstrate and implement the COSBIA. The game concept (Appendix H: COSBIA Game Concept) was shared on social media platforms and inviting software development students to sign up and implement it. Three teams signed up and the hackathon was open for 10 days. However, only two teams managed to submit, and one team withdrew from the hackathon. At the end, the products were evaluated using the criteria in Appendix I: COSBIA Game Evaluation Criteria by a panel of experts. The expert evaluation of the game was done manually as the developers failed to implement it online citing database complexity. Using the evaluation form, the implementations were deemed to fail, as shown in **Error! Reference source not found.**.

Table 5.4: Judges' game evaluation

	Team 1			Team 2		
Questions	Judge 1	Judge 2	Judge 3	Judge 1	Judge 2	Judge 3
1. Is the game Interactive? Can you make a choice?	Yes	Yes	Yes	Yes	Yes	Yes
2. Does the algorithm allow the child to have different options on Gadgets and platforms	No	Yes	Yes	No	No	No
3. Does the algorithm read the activities that the child is performing can it read if the child is watching Videos, playing game, searching for information, studying, social networks, emailing etc.?	No	No	No	No	No	No
4. Does the algorithm evaluate the user experience based on the answers given through the game/quiz by the child?	No	No	Yes	Yes	No	No
5. Does the algorithm have a way of outputting the online experience of the child?	No	No	No	Yes	No	No
6. Does the algorithm have a way of outputting online behaviour of the child?	No	No	No	No	No	No
7. Does the algorithm have a way of outputting secure online behaviour of the child?	No	No	No	No	No	No
8. Does the algorithm have a way of outputting secure online experience	No	No	No	No	No	No
9. Does the algorithm evaluate how knowledgeable the child is on the different threats?	Yes	Yes	Yes	No	Yes	No
10. Does it give tips on how to improve on being safe online?	Yes	No	No	Yes	No	No
11. Are there multiple exit points while playing the game?	Yes	No	No	Yes	No	No
12. Are there any empowerment messages displayed when the child decides to exit?	No	No	No	No	Yes	No
13. Are there any empowerment messages displayed after ever score?	Yes	No	No	Yes	No	No
14. Is the game doing what it is expected to?	No	No	No	No	No	Yes
15. Is the game usable?	Yes	Yes	Yes	Yes	Yes	Yes
16. Is the game appealing?	Yes	Yes	No	Yes	Yes	Yes
Mark Obtained	**23/100**	**19/100**	**15/100**	**26/100**	**23/100**	**12/100**
Total score	**57**			**61**		
General Comment	The web app provides informational CBT like interface. It requires more interactivity icons to be appeal.	The team barely solved the algorithm. They did the bare minimum and took a different direction.	The application does not really evaluate what is needed to security.			The game looks appealing but does not cover most of what is expected of it.

The judges concluded that the systems could not be availed to children due to Covid 19 restrictions and for ensuring the safety of the children hence the end user evaluation was not executed. The functional implementation was supposed to be played by the children to measure its efficacy. The children needed to experience the environment and to evaluate the user experience using the tool in Appendix K: Children's COSBIA Evaluation. Ten children were purposefully recruited, however due to the limited

capacity of the implementations, it was deferred to the future to allow for the system to be fully developed and tested. In its form, the demonstration proved that the concept can be coded and integrated on different gadgets used by children. Figure 5.9 presents the welcome screen of COSBIA.

Figure 5.9: COSBIA welcome screen

The COSBIA implementation should have a database of all the identified threats for the different gadgets, online activities, online platforms, online behaviour and the general threats online. Immediately when the child gets online, COSBIA should read the information of the child, the type of gadget they are using, the platform they are visiting, the online activities they are performing, and the way they are behaving. For example, if you are preparing for an android phone, the app reads the gadget as Samsung S20, reads that the child is using Facebook (platform), and reads that the child (player) is chatting (activity). From there, COSBIA evaluates whether the child knows the threats inherent in the gadget they are using, that's level 1 of the game. Figure 5.10 presents level 1 that is on gadget threats.

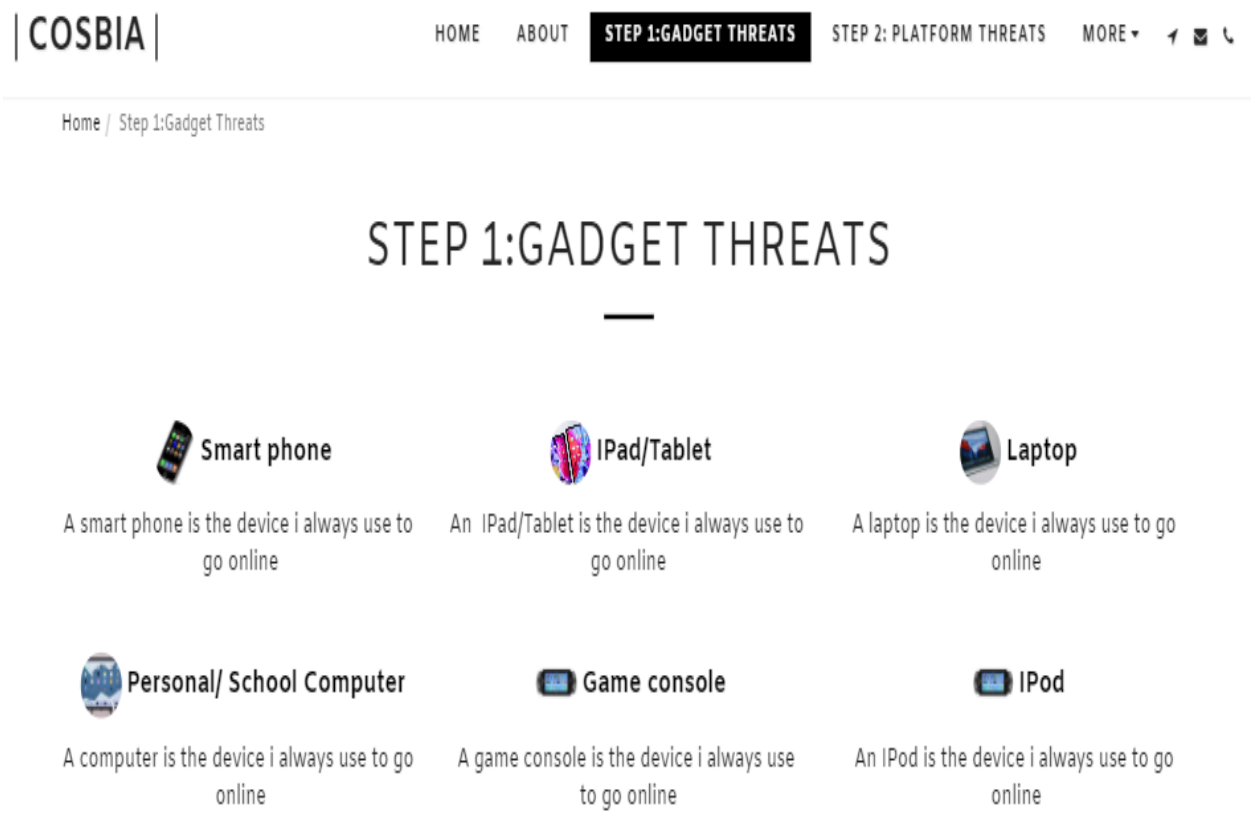


Figure 5.10: Gadget threats

For the next level, the child (player) will be evaluated on the threats inherent in the platforms they are visiting.

Figure 5.11: Platform Threats

The algorithm should have a way of reading the activities that the child (player) is doing, for example if the algorithm sees the child (player) selecting the Facebook logo, it should scan and see that it is a Facebook platform.

- So that already using the combination that it is having, it can pull out the questions that are meant for the child (player) on that specific platform.
- It asks the child (player) at level 2 generic questions about the obvious things that the child (player) is supposed to know about that platform (Facebook).
- Then if the child passes, depending on the score that is calculated, the child move to the next level.
- For example, if the score is a minimum of 1-3, then they are supposed to go through empowerment.
- When they are done with that, they are re-evaluated which is level 2 and then they get their upgrade to the next stage of the game/activity.
- However, on the other end, they could score all the questions correctly which is number 10.
- So if they score 10 they don't need empowerment, so they can just get a message that they have succeeded, they are cyber smart and that they can proceed with their activity and stay safe (so they continue to do whatever they wanted to do on Facebook, twitter, WhatsApp, Instagram, etc.).

Now that the child (player) has this knowledge determined, the next thing is for the app to check how the child (player) is navigating in the environment so that the system should read how they are clicking, etc., and based on that then it can evaluate if the child (player) is secure or insecure. The algorithm should evaluate the user experience based on their answers. There should be a way of calculating the score, for example:

- 3 equals to empowerment at first level
- 4-6 equals to empowerment at second level
- 7-9 equals to empowerment at third level
- 10 continue with your activities that means you are safe.

This should be incorporated in the entire algorithm. The scores are only enabling to give them empowerment, so if the child (player) is very unsecure you give them tips on how to improve on being safe online, then they can move to the next level of empowerment but at the same time also don't frustrate them so that they stop playing the game. There should be multiple exit points.

- For example, if the child (player) scores 7-9, this means that this is a knowledgeable person but not at the right level so they go to level 3 of the game, they earn points or lives.

- At level 3 they are given some tips and then they take another quiz and when they complete that quiz then they play their game.
- If they feel like they don't want to go on, there should be an exit point. Then a message can be displayed like "Ok you don't want to play the game however you are vulnerable to, 1, 2,3,4,5 etc. risk/ threats (so still either way they still go through empowerment). And then they can continue with their activity (whatever they wanted to do).

The evaluation of the algorithm will be on the score of the child (player) how knowledgeable are they about general Internet threats, online platform specific threats, online activity specific threats, gadget specific threats and online behaviour specific threats. If they are knowledgeable on all the threats then they are good to go but if they are not knowledgeable on a specific threat, then they need to be empowered. For example, if they don't know gadget threats, they can get a pop-up message that their gadget is vulnerable to this threats and that they need to improve by 1,2,3…If it's a combination of all threats, then you can talk about all threats. The child (player) doesn't need to be bored about things that they know, they are kids and their concentration level spin are very low. Whatever is missing, the application should be responsive enough to say this is what is missing as the child needs empowerment on the identified limitation.

COSBIA

The COSBIA is an algorithm that is designed to influence the behaviour of children between the ages of 13-17 years and raise their cyber security awareness. This section outlines the COSBIA concept that includes the story, player and player characteristics, the challenges for the player, game environment, target player, progression and principle gameplay mode.

Story

A child interacts with an online Platform to perform Online Activities using a smart gadget. The Time Spent Online and the child's Online Behaviour while performing online activities on an online platform using a gadget results in a child's online experience, which can be either secure or insecure. This is due to the fact

that gadgets have an influence on online behaviour, which results in gadget specific behaviour and the online platform has an influence on online behaviour which results in platform specific behaviour.

The child's prior knowledge and their online behaviour exposes them to online threats that are inherent in gadgets, online activities and online platforms, and this results in a child's online experience. If empowerment is added to this interaction, it would result in a secure online behaviour. We posit that a secure online experience is a result of secure online behaviour.

Player characteristics

A **child** is the main actor in the COSBIA, and the child:

- Interacts with an online platform to perform online activities using a gadget,
- Spends time online and needs to be tracked,
- Has an online behaviour while on the different environment,
- Has an online experience (secure or insecure), and
- Should be empowered while on the different environment.

Challenges for the player

- Applying prior knowledge (for initial evaluation, a quiz on their prior knowledge of risks and security around their gadgets, platforms and activities)
- Exposed to online threats based on the gadget or platform used or activity being performed
- Gets empowerment if their security levels are lower than a score of three.
- Online behaviour should be secure to move to the next level (for level 1 to level 2, a score of 3 out of should be obtained, and for level 2 to level 3, a score of 3 should be obtained, whereas for level 3 to exit back to the activity, a score of 3 should be obtained).
- Secure online experiences are attained through performing several empowerment activities.

Score

3 correct answers: You are at the beginning of your journey to become a safe Internet user and you start thinking about others online. However, you can do more! Always remember to ask an adult for support as soon as you need it, instead of trying to do it all by yourself or just go along with what others do. In addition, you should have a much better time on the Internet.

4-6 correct answers: You are on the way to becoming a safe Internet user and a good friend to others. However, you can do more! Remember always to ask an adult for help as soon as you need it, instead of trying to do some things by yourself or being caught up in what others might do. That means you and your friends can enjoy the Internet together safely.

7-9 correct answers: You are well on the way to becoming a responsible Internet user and a great online friend, and you are making some very sensible choices. It is always a good idea to ask for help from an adult if there is anything you are uncertain about, or if anything makes you feel worried or upset. In addition, you will get the most out of the Internet and all the amazing stuff that it has to offer.

10 correct answers: You are a friendly and caring Internet user who does brilliantly online. You know how important it is to ask for support when you need it, to be healthy and to look after the feelings of your friends. Share your knowledge with as many friends as possible to help everyone around you stay safe and enjoy fantastic online time.

Game environment

- **Online platforms**: Chat, Tik Tok, Facebook, WhatsApp, Instagram, Hangouts, Twitter, Skype, Myspace, Snapchat, LinkedIn, gaming
- **Gadget**: smart phone, IPad/Tablet, Laptop, Personal computer, school computer, game console, IPod
- **Online activities**: Watching Videos, Gaming, information search, studying, social networks, emailing

Table 5.5: Quiz question on the different online threats

Online Threats	Quiz	Answers
General Internet Threats	One of your classmate has sent around an embarrassing photo of another classmate. What should you do with it? A. Show your teacher, and tell them what happened B. Forward the photo to others C. Save it on your phone, so that you can embarrass them later D. Laugh at the photo with your friends	**A:** You should show the photo to your teacher and tell them what has happened. Think of how you would feel if the picture have been of you.
	One of your friends posted a video about you on the Internet and you do not like it. You asked them to take it off but they said no, because it is funny. What is it that you should do? A. Keep asking your friend until they take it down B. Speak to an adult and say why you don't like it C. Leave it – you can't do anything else about it D. Post a video of them to get back at them	**B:** You should talk to an adult about what happened and tell them you do not like it. Then, they can try to take down the video.
	Your friend tells you she is talking to a boy/girl online and on the weekend, she/he will meet him/her. What should you do? A. Volunteer to go with her/him B. Let her/him go on her/him own C. Tell an adult straight away D. Tell your other friends	C: If someone is going to meet a person they met online, you must tell an adult right away. You should never meet strangers, unless you know for sure who they are.
	A classmate tells you someone on an online game was calling him/her mean names. What should you do? A. Tell your teacher or another adult B. Tell him/her to call the person mean names back C. Tell him/her to just ignore it and let it go away D. Tell him/her to stop playing games for a while	A: Calling anyone online means names is a cyberbullying act. You should inform an adult about this and you should not neglect it.
	Whom are you allowed to share your passwords with? A. Your friends B. Nobody – you should keep them to yourself C. Your family D. Your teacher	B: You should also keep your passwords to yourself. If your password falls in the wrong hands, it could be risky.

	You need to create a Website password. What should you use? A. Your full name (e.g. Annamarie) B. Part of your name and a number (e.g. anna123) C. A random word, number and punctuation combination (e.g. 1vira8pm!) D. A nickname that your friends call you (e.g.annagirl)	**C:** The strongest passwords should include letters, numbers, and punctuation combinations. You should never use something that is connected to your name because it is very easy to guess.
	The Internet gives us access to many resources we would otherwise not be able to get in contact with. A. TRUE B. FALSE	**A:** That is probably the best thing about the Internet. It is giving us instant access to distant things, things locked away, that does not even exist yet. It is a travel agent, a guide to the museum and a play with friends from all over the world!
	Information on the Internet can always be trusted to be truthful. It would not be online if it were not true. A. TRUE B. FALSE	B: The Internet is an open forum for anyone and everyone. Bias is the rule rather than the exception. Evaluate carefully ALL information on websites, personal or public

Online Platform Specific Threats	What is the best way to use Facebook, Chat, TikTok, WhatsApp, Instagram, Hangouts, Twitter and other social networking sites? Limit the amount of information I share about myself. A. Only talk to people I know. B. Make my page private, except to the people C. I have as my friends. D. All of the above	**D:** Own Your Online Presence. When available, set the privacy and security settings on websites to your comfort level for information sharing. It is ok to limit how and with whom you share information.
	What do you do when a stranger asks you to give them a picture of yourself on social networking sites? A. Send no pictures, and tell an adult immediately B. If you think you know them, send the picture C. Send the picture, even if they're a stranger D. Ignore them	**A:** You should never give pictures of yourself to a stranger because you do not know who they are or what they may be doing. When a stranger is asking for a picture, immediately deny and tell an adult. You should never give anyone a photo that you would not want someone else to see. Even if you are comfortable with that person, it could still end up online or be shown to others
	From online, who should you accept friend request? A. Anyone B. A friend of a friend C. Someone you think you've met before D. Only people you definitely know	**D:** Only friend requests from people you definitely know, you should never accept friend request from strangers or anyone else you are uncertain.

	Others cannot see anything I send in my private email, Instant messenger or Chat (Tik Tok, Facebook, WhatsApp, Instagram, Hangouts, Twitter, Skype, Myspace, Snapchat, LinkedIn, and gaming). A. TRUE B. FALSE	**B:** There are people and programs that can "see" into your private correspondence online. NEVER send personal information unless you are positive it is a secure site
	Jessica's friend Sophie asks for Jessica's password to her Facebook account. What should Jessica do? A. Give Sophie her password. Sophie is her friend and Jessica can trust her. B. Tell Sophie her password and change it as soon as she gets home. C. Don't give her password to Sophie.	**C:** Protect your personal information. Passwords are never to be shared with anyone other than a parent or guardian. It is a good idea for parents and guardians to keep passwords to make sure you remain safe and secure. Just because you spend time with friends, doesn't mean you have to follow everything they do. If they are doing something that doesn't seem right, you should feel completely comfortable standing up for what you think is right.
	If I want to know something about a stranger that sends me an Instant Message, I can check their profile and trust that information. A. TRUE B. FALSE	**B:** Part of the Internet's wonder is its anonymity and sometimes the worst thing, too. Unlike the physical world, you cannot verify a person's age, location, etc. online so it is easier to lie and get away with it.

Online Activities Specific Threats	You have been to a gaming/video website and it is asking you to download a link before playing the game/watching the video. What should you do? A. Show the link to an adult and ask them if it's safe B. Download it anyway C. Don't download it, it must be illegal D. Ask your friends what to do	**A:** If a website asks you to download something, you should always speak to an adult. You never know what that could be
	I can always trust emails and attachments I get from friends. A. TRUE B. FALSE	**B:** New programs and viruses send out emails without their knowledge or consent to everyone in your inbox. Verify it is in fact from your friend first.
	Private browsing" is a feature in many Internet browsers that lets users access web pages without any information (like browsing history) being stored by the browser. Can Internet service providers see the online activities of their subscribers when those subscribers are using private browsing? A. Yes B. No	**B:** If you want to hide your activity from your service provider, consider a VPN.

	When it comes to information searching online, you can safely search for information from any site. A. True B. False	**B:** When searching information online, you should always search from trusted and well-known websites. Check to be sure the sites is security enabled. Look for web addresses with "https://," which means the site takes extra measures to help secure your information. "Http://" is not secure.
	You and a friend are on the computer, looking to download music and movies. You should: A. Go to a site that your friend uses and download a few files onto the computer. B. Only with your parent's permission, go to trusted websites or app stores to download music and movies.	**B:** Only with your parent's permission, go to trusted websites or app stores to download music and movies. Your friends may not know what websites are safe or unsafe for you to download. It is illegal to download music or movies from certain websites. Only purchase music and movies from established services for media distribution.
	It is okay to download FREE music/videos from music/video sharing sites, as long as no one finds out. A. True B. False	**B:** This is the same as stealing from a store and you are stealing from your favorite artists as well! Only purchase music/videos from established services for music/video distribution. Some file sharing sites are also well known sources of malware distribution. Remember, safer for me more secure for all. What you do online has the potential to affect everyone – at home, at work and around the world. Practicing good online habits benefits the global digital community.
Gadget Specific Threats	Turning off the GPS function of your gadgets prevents any tracking of your phone's location. A. True B. False	**B:** If it were only that easy. A 2018 Princeton study found that device's time zone and information from its sensors could be combined with public information like maps to estimate your location, even without GPS data.
	Installing a virus checker on my gadget will keep my gadget safe. A.TRUE B. FALSE	**B:** Just installing the program will help for a little while, but new viruses are spawning all the time. Update and run the software at least once each month.
	Tjipena unlocks his smartphone and notice he has 12 apps that need to be updated. What should he do? A. Ignore the prompt to update B. Update the apps.	**B:** It is important to keep a clean machine. Keeping machine means having the latest operating system, software, web browser, anti-virus protection and apps on your computer and mobile devices. You should also only have apps on your phone that you actually use
	You receive a chain email that tells you to pass it on to 10 of your closest friends. Do you: A. Send the email to your friends – it is so cool and you want them to see it too! B. Delete the email. You are never sure what viruses these types of chain emails can have.	**B:** When in doubt, throw it out! Links in email, tweets, posts, and online advertising are often the way cybercriminals compromise your computer. If it looks suspicious, even if you know the source, it's best to delete or if appropriate, mark as junk email.

Online Behaviour Specific Threats	You posted a picture online, but soon decided to take it down. You are worried your friend may see it, but then soon remember that person DOES NOT have a computer. Your friend will never see the photo. A. True B. False	**B:** You never know who is going to see things that are posted online. Even if your friend does not have a computer, there are many other ways he could see the photos after they have been shared with friends. Copies could be passed around and someone may have saved an image before you deleted it. Be a good online citizen. Think about images you post and whether your friends would be okay with them. Post only about others as you would have them post about you. Whenever possible, get permission before posting pictures or videos of others. Likewise, let others know they need your permission before posting pictures or videos of you.
	You don't have to worry when you visit your favorite sites, like Facebook and gaming sites, because they are safe from spyware, malware and other online threats. (True or False) **A.True** B. False	**B:** Trusted sites can be safer. However, what you do on those sites — such as clicking on posts with links or using apps — can put you at risk. The best security step you can take is to Keep a Clean Machine. Keeping a Clean Machine means having the latest operating system, software, web browser, anti-virus protection and apps on your computer and mobile devices. Remember, when in doubt, throw it out! Links in email, tweets, posts, and online advertising are often the way cybercriminals compromise your computer. If it looks suspicious, even if you know the source, it's best to delete or if appropriate,

	When online, you should be careful whenever approached by a new person or asked to provide information about yourself. A. True B. False	**A:** You always need to be on the lookout for online intruders! Be careful because they may be trying to get information from or about you. Remember to Be Web Wise and think before you act. Be wary of communications that implore you to act immediately, offer something that sounds too good to be true, or ask for personal information.
	You receive an email from a person that identifies themselves as your friend John. They want to meet you in the park after school. Do you: A.Tell your parents about the email and ignore the request. B.Ask the person a question only John would know to make sure it is John. C.Go to the park and meet your friend John.	**A:** Some people will pretend to be other people and may be impersonating someone you know. It is better to be safe than sorry! Unfamiliar email addresses and posts on social network sites should raise a red flag. Let your parents know and let them help you make the right decision about contacting John.
	You should always know whom you are talking to online. A .True B. False	**A:** The Internet can be a place to meet people and join new communities. However, just because you meet someone online, it does not mean you really know his or her identity. Use caution when interacting with new people. There is nothing wrong with being suspicious and extremely guarded about sharing any personal information.

Target player

The COSBIA was initially created in the interest of influencing children's behaviour aged 13-17 on the Internet and to raise their cyber security awareness.

Progression

The game starts with a short intro scene where the children behave insecurely online. Then they get exposed to cyber criminals through innocently sharing information, posting photos and messages about themselves and befriending strangers. Secure online experience is attained through performing several empowerment activities. Empowerment is achieved through security knowledge, secure behaviour, secure experience and reducing exposure to online threats in the player over time. The player also obtains rewards through the completion of security knowledge, secure behaviour, secure experience and reducing exposure to online threats. The game should have three (3) levels; level 1 is on security knowledge, level 2 is on secure behaviour and secure experience, and level 3 is on reducing exposure to online threats.

The first level is on cyber security knowledge; users are introduced to mechanics of information security and how to measure the security of players on information security while performing their online activities (playing games or social networking sites);

- When adding strangers
- When sharing personal information such as an address, phone number, or school name or location with strangers online
- When sharing pictures to close friends is limited
- When posting everything online such as feelings and emotions

Empowerment

- Do not add strangers
- Do not share personal information such as an address, phone number, or school name or location with strangers online
- Picture sharing to close friends should be limited
- Once you have written something you cannot delete it online

Once the player beats the first level, they get a crown and can advance to the second level. Users are introduced to secure online behaviours which result into secure online experience. How to measure the security of players on secure online behaviours;

- Not wary of stranger
- Meeting online friends without permission
- Pay attention to insulting messages and do not report to parents
- Do not pay attention to parental regulations and rules
- Do not report inappropriate web content upon finding out
- Pay attention to popups

Empowerment

- Be wary of strangers
- Get parents' permission to meet online friends
- Ignore insulting messages and report to parents
- Confirm parental regulations and rules
- Report inappropriate web content upon finding out
- Ignore popups

Once the player beats the second level, they get a crown and can advance to the third level. Users are introduced to mechanics that reduce exposure to online threats. How to measure the security of players on reducing exposure to online threats while on Internet;

- Security software outdated
- Using the same passwords for every online account
- Geolocation software is always on
- Suspicious downloads
- Clicking on clicks in emails and providing personal information

Empowerment

- Protect your computer by updating security software regularly
- Install anti-virus software

- Create unique passwords by using different passwords for every online account as this helps to prevent others from accessing your personal information
- Control privacy and security settings to control or limit access to information such as which apps have the permission to access contacts, locations and calendar
- Switch off geolocation software for sharing locations on smart devices, it can let unfriendly people know where you are
- Be careful of suspicious downloads as they could expose you to potential viruses and hacks
- Never click on links in emails asking for information of any kind as this could expose you to a phishing scam
- Once the player beats the third level, they get crowns and should return back to the activity

Principle Gameplay mode

Goals

- Overall (long term): Influence children's behaviour online and raise their cyber security awareness
- Gameplay (short term): Get empowerment, advance to the next level.

User skills

- Screen tap
- Drag and drop
- Solving a puzzle
- Rearranging pieces
- Strategize

Challenge

Difficulties will advance by making the player score more than 3 points for secure online behaviour to move to the next level. To mitigate difficulty, the user will have to play better, and level up their online behaviour.

Losing

Losing conditions are by running out of time and a score of less than three. When the player loses, there must be an image showing vulnerable online experience, negative online experience or threatening online experience depending on the player's online behaviour.

Art style

Everything should be very colourful and feel alive, with highly animated scenarios and a layered background.

Music and sounds

The music should have a Retro style, appealing to 8-bit nostalgia but with high quality. It is important that a lot of sound effects praise the user when they do something good. There should be immediate and positive feedback. When time is running low, add a sound that makes the users to be nervous. The sad scenes should be accompanied by Accordion/ Violin music and sound like a sorrowful tango. For in-game music, use a more relaxed approach with happy tunes and going up on tempo as the level progresses.

5.2.6. STAGE 5: Algorithm evaluation

Information systems design science research (DSR) consists of two main activities: building and evaluating (Herselman & Botha, 2015). Evaluation is an important prerequisite in research into design sciences (Gacenga, Cater-Steel, Toleman, & Tan, 2012). Even though the evaluation of DSR artefacts and design processes is considered "important," much of the contemporary DSR information system work focuses on the building processes (Herselman & Botha, 2015). The COSBIA was designed, as illustrated in Section 5.2.4. However, Herselman and Botha (2015) outline that to ensure rigor and improve the knowledge base and scientific relevance of artefacts, it is important to evaluate it. The artefact is evaluated against set objectives to demonstrate utility, its organisation and the environment of application. The COSBIA was evaluated using expert reviews. The expert review tool covered utility questions in line with the objectives in section 5.2.3; the environment of application in insecure online activities on online platforms using smart gadgets by children and the components were evaluated on relevancy and validity in addressing security challenges. To ensure reliability, the tool was tested for convergence against the research and artefact objectives.

5.2.6.1. Expert review

Research studies have extensively used various human-computer interaction (HCI) evaluation techniques, namely focus groups, field experiments, and expert reviews. These approaches aim to yield qualitative

results and require fewer participants than controlled experiments (Tory & Moller, 2016). In this research, we focused on expert reviews to evaluate the algorithm using a design science research process. A detailed description of how the participants in this study were selected is presented in section Chapter 1690710027: with section 5.2.6.2 presenting how the tool was designed and tested. All of the experts were neutral because they had not previously participated in this study. The criteria for the selection of expert reviewers was based on the;

- Education background in Information Security, Human Computer Interaction and Software Development (Master student, PHD students, Professors and Lecturer).
- Job position of people working in information communication and technology, Internet safety and children's digital rights (COP, MGECW, Office of the First Lady, UNICEF, MICT, ISOC, NamPol, CRAN, Lifeline/ChildLine, Telecommunication, and the Prosecutor General).
- People with a specialised knowledge in information security and children's digital rights.

5.2.6.2. Algorithm expert review tool

The experts review evaluation form was developed and then reviewed before carrying out the expert evaluations by the research supervisor and two other colleagues. The expert review evaluation form was piloted to make sure that all questions were answered and to correct any mistakes or design flaws. The expert review evaluation form comprised of four sections. The first section introduced the main objective of the tool and the demographic information of the experts. The second section evaluated the first relationship of the algorithm which is on child online experience. The third section evaluated the second relationship of the algorithm that is on children's secure online behaviour. The last section evaluated the third relationship of the algorithm that is on children's secure online experience and the overall flow of the algorithm. The study's components were measured against a 5-point scale from strongly agree, agree, neutral, disagree to strongly disagree and from not at all true, slightly true, somewhat true, moderately true to extremely true.

5.2.6.3. Data analysis

The data analysis was classified using the COSBIA components and relationship relevance. The analysed data was used as guidelines to improve the COSBIA and refine it. A total number of 29 experts were emailed the evaluation tool, and only 17 experts participated.

5.2.6.4. Evaluation of findings

Demographic information

A collection of demographic information details on the background of the experts is presented in Table 5.6.

Table 5.6: Expert reviewer demographic information

	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14	P15	P16	P17
Organization	CRAN	Internet Society	Academia	Academia	Academia	Academi	Academia	Academia	MICT	MGECW	Former Unic	Unicef	MGECW	Academia	Unicef	Prosectur General	Lifeline/Childl ine
Role in Organzation	ICT Policy and Regulation, Law		Master/Phd student	IT Lecturer	Researcher & Senior Lecturer	Lecturer	IT Specialist	Lecturer	Deputy Director	Social Worker	Communic ations Officer	Social Worker	DIRECTOR	Lecturer	Child Online Protectio n Officer	Lecturer	Coordinating the Counselling Centre
Years of Experience		3	1	4	10	6	8	10	8	16	3	9	10	4	3	25	
Understanding and experience on child online protection	Intermediate	Intermediate	Intermediate	Intermediate	Advanced	Advanced	Beginner	Advanced	Intermediate	Beginner	Advanced	Advanced	Intermediate	Intermediate	Advanced	Advanced	Advanced
Level of cyber security knowledge	Intermediate	Advanced	Advanced	Advanced	Advanced	Advanced	Intermediate	Advanced	Intermediate	Beginner	Advanced	Intermediate	Intermediate	Intermediate	Advanced	Intermediate	Intermediate

5.2.6.5. Algorithm evaluation

This section evaluates the proposed aspects for COSBIA. It presents both quantitative and qualitative results. The quantitative part are the assessment results and the qualitative results from the experts' comments and suggestions. From the analysis, most reviewers agreed on the proposed component relationships on child online experience, children's secure online behaviour, children's secure online experience and the overall assessment of the children's online secure behaviour influencing algorithm. The children's online experience evaluation and score per relationship by the experts are presented in Figure 5.12.

Child online experience evaluation

In order to evaluate the child online experience components relationship, the experts were asked to assess the relationship on child online experience on a scale of 1-5. Figure 5.12 illustrates the experts' assessments on the components relationship between relationship one that is on child online experience.

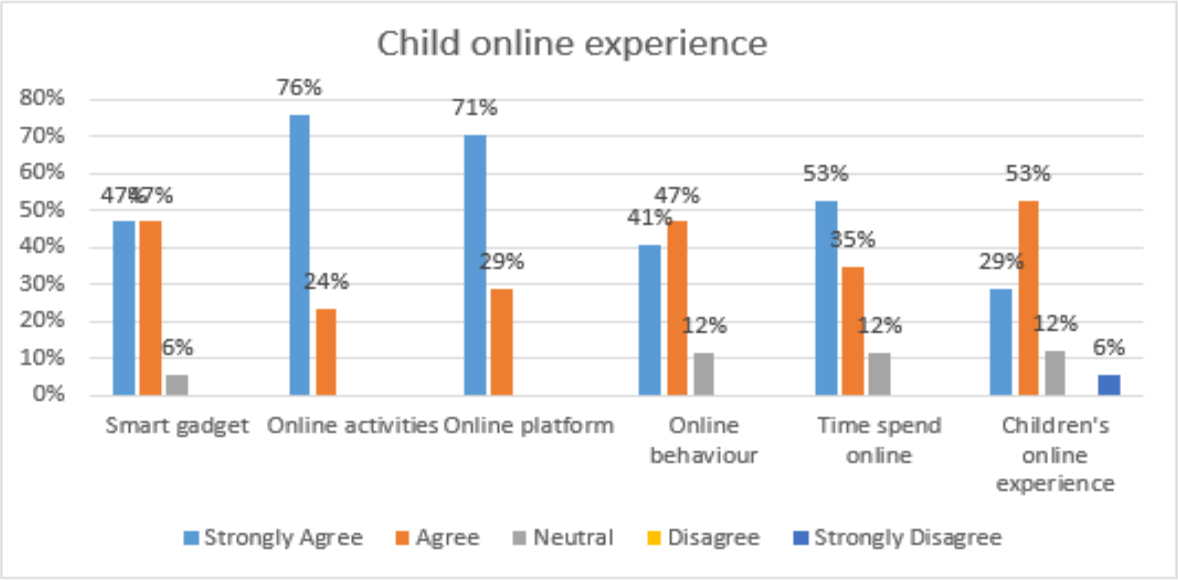


Figure 5.12: Child online experience assessment

The results highlight that the majority of the experts highlighted that they agreed with the child online experience components relationship. The component on online activities and online platform had the highest amongst all the other child online experience components relationship.

Out of the 17 experts' responses to the child online experience components relationship, most of the experts strongly agreed and agreed that the components are relevant. As shown in **Error! Reference source not found.**, all components have a direct influence on children's online experience in the order shown:

- Type of smart gadget, with 94% agreeing or strongly agreeing, and this confirms similar findings by Mascheroni and Ólafsson (2013) who outlined that the circumstances under which the children access and use the Internet could expose them to online risk which leads to their online experience
- Type of online activities, with 100% agreeing or strongly agreeing, and this confirms similar findings by Kardefelt-Winther (2017) who alludes that the children's online activities influence the child online experience by affecting their mental well-being, social relationships and physical activities which results into a child's online experience.

- Type of online platforms, with 100% agreeing or strongly agreeing, which is consistent with the findings of Atkinson, Alqahtani, Stengel, and Furnell (2017) who state that the higher the use of online platforms, the higher the exposure to risk which may result in a child's online experience.
- Type of online behaviour, with 88% agreeing or strongly agreeing, and this confirms similar findings by Livingstone et al. (2017) who outline that children's online experience differs depending on the child's online behaviour. The impact of this online exposure on children's behaviour are personal information harvests (Fire et al., 2014), that result into the child online experience.
- Time spent online, with an assessment of 88% agreeing or strongly agreeing, and this confirms similar findings as in section 4.5, which presents findings that most children spend most of their time on social networking sites, making them more likely to be exposed to cybercriminals and they are left with less time to do other potentially more rewarding activities.
- 82% of the experts agreed or strongly agreed that children's online experience is a proportion of the time spent online using a gadget, the online activities they are performing, the specific online behaviour on the online platform and their online behaviour using that specific gadget. One expert strongly disagreed however, the expert did not state the reason for disagreeing on the children's online experience components relationship.

The results are consistent with the research findings from literature and interviews as presented in Chapter 2: and Chapter 4: . It could be concluded that the type of smart gadget, online activities, online platform, online behaviour, and time spent online have a direct influence on children's online experience. Experts were then asked if they would recommend any changes to the child's online experience components relationship. Table 5.7 presents the experts' comments on the child's online experience components relationship.

Table 5.7: Experts' feedback on the child's online experience component relationship

Experts	Experts feedback and suggestions on component relationship 1	How the comments were addressed
P1	No	
P2	I would add the context of use (COU) of G to be part of the set	What makes up the Context of Use (COU) in COSBIA are the gadgets used (G), online platforms (OP) visited and online activities (OA) performed that can trigger online behaviour habits of a child and affects the child's online experience. It is a component of OE as presented in Equation 5.1. COU= G+OP+OA.
P3	No. It is well represented	
P4	None	

P5	I would rather have a separation of the enablers of child behaviours and experiences as catalyst such as the Gadgets & the Online Platform, Gadgets becomes the superset, and everything happens within the superset, hence subsets. I would also rethink the representation of OE and OB, which influences the other? That is also going to entail some modification on their representation in Figure 1.	The COSBIA reads information of the child's gadget they are using, empowerment is then presented via a quiz to evaluate them of that gadget specific threats and a score will determine their vulnerability and enable tips and further empowerment to be availed if necessary. The next step is to read the platforms the child is visiting as platforms can be gadget specific, a quiz is then provided on the online platform specific threats. Based on the score, feedback is provided and where necessary further empowerment is provided. The algorithm then reads the activities the child is performing and the way they are behaving (analyse the clicks etc.), from all that they are presented with a quiz on online activities specific threats and online behaviour specific threats. The children will get the empowerment through the score they get in the quiz. The way the child behaves online will influence their online experience. The gadget cannot be a superset as it may not support all OP and OB may be a result of aesthetics of the gadget hence they will vary from gadget to gadget.
P6	No changes required	
P7	None	
P8	I would not use equal but to say children's online experience is proportional l to the time spend online using a gadget, the online activities they are performing, the specific online behaviour on the online platform and their online behaviour using that specific gadget	Corrected: Equation 5.1, outlines that Children's online experience OE(C) is proportional to the time spend online (TSO) multiple by the gadget they are using, the online activities they are performing, the specific online behaviour on the online platform and the way they are behaving using that specific gadget.
P9	Parental guidance is required	
P10	Yes, decrease the time spend online.	
P11	Of course - more parental/security monitoring due to paedophile and online sexual abuse	
P12	No	
P13	Children to be taught earlier in school the dangers of online chatting, and search of information.	The COSBIA focus is to influence children's behaviour online and raise their cyber security awareness as early as they can be online.
P14	no	
P15	No	
P16	Yes. maybe parental guidance could also play a role	
P17	None	

From the feedback and suggestions, most of the experts had nothing to change, however, only a few had suggestions and those comments were addressed as presented in Table 5.7.

Children's secure online behaviour assessment

In order to evaluate the children's secure online behaviour components relationship, the experts were asked to assess the relationship on children's secure online behaviour on a scale of 1-5. **Error! Reference source not found.** illustrates the experts' assessment on the components relationship between relationships two that is on the children's secure online behaviour.

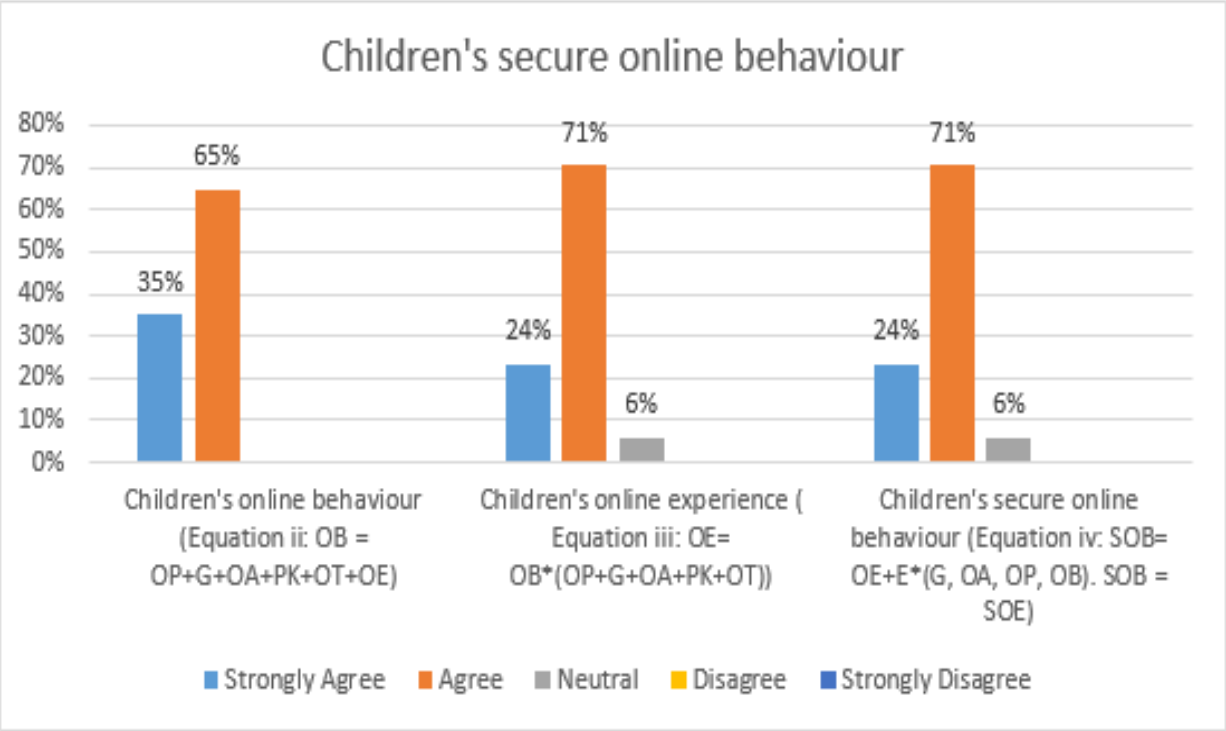


Figure 5.13: Children's secure online behaviour components relationship

Most of the experts agreed with the children's secure online behaviour components relationships, with only one expert having a neutral feeling about the relationship. However, one expert had a neutral feeling on the children's online experience components relationship and another expert also felt neutral on the components relationship on children's secure online behaviour and no feedback or suggestions were made in this regard. Hence, it could be concluded that the equation on children's online behaviour, children's online experience and children's secure online behaviour are the summation or product of the listed components. Table 5.8 presents the experts' comments on the children's secure online behaviour components relationship.

Table 5.8: Experts feedback on children's secure online behaviour components relationship

Experts	Experts Feedback and suggestions on component relationship 2	How the comments were addressed
P1	No	
P2	None	
P3	no	
P4	None	
P5	How can you capture other attributes such as peer pressure and external factors such as offline behaviours that cripple into online behaviours, which may not necessarily be represented by the current variables under consideration?	The other attributes such as peer pressure and external factors are captured under prior knowledge which is a subset of the Knowledge component in COSBIA as presented in Table 5.1.
P6	No changes required	
P7	None	
P8	no	
P9	Children should not allowed to visit site for adults	True, the COSBIA focus is to influence children's behaviour online and raise their cyber security awareness as early as they can be online. Parents will be encourage to adopt safe practices and guidelines as shared in Table 2.7.
P10	No	
P11	No	
P12	No	
P13	No	
P14	no	
P15	no	
P16	As above	
P17	None	

From the expert comments on relationship 2 most of the experts' feedback there was no changes required to the children's secure online behaviour components relationship. However, two suggested changes on how to capture other attributes such as peer pressure and external factors, and that children should not be allowed to visit site for adults as shown in Table 5.8. Other attributes could be captured through prior knowledge.

Children's secure online experience assessment

In order to evaluate the children's secure online experience components relevance, the experts were asked to assess the relationships of components constituting children's secure online experience on a scale of 1-5.**Error! Reference source not found.** illustrates the expert's assessment on the components relationships on children's secure online experience.

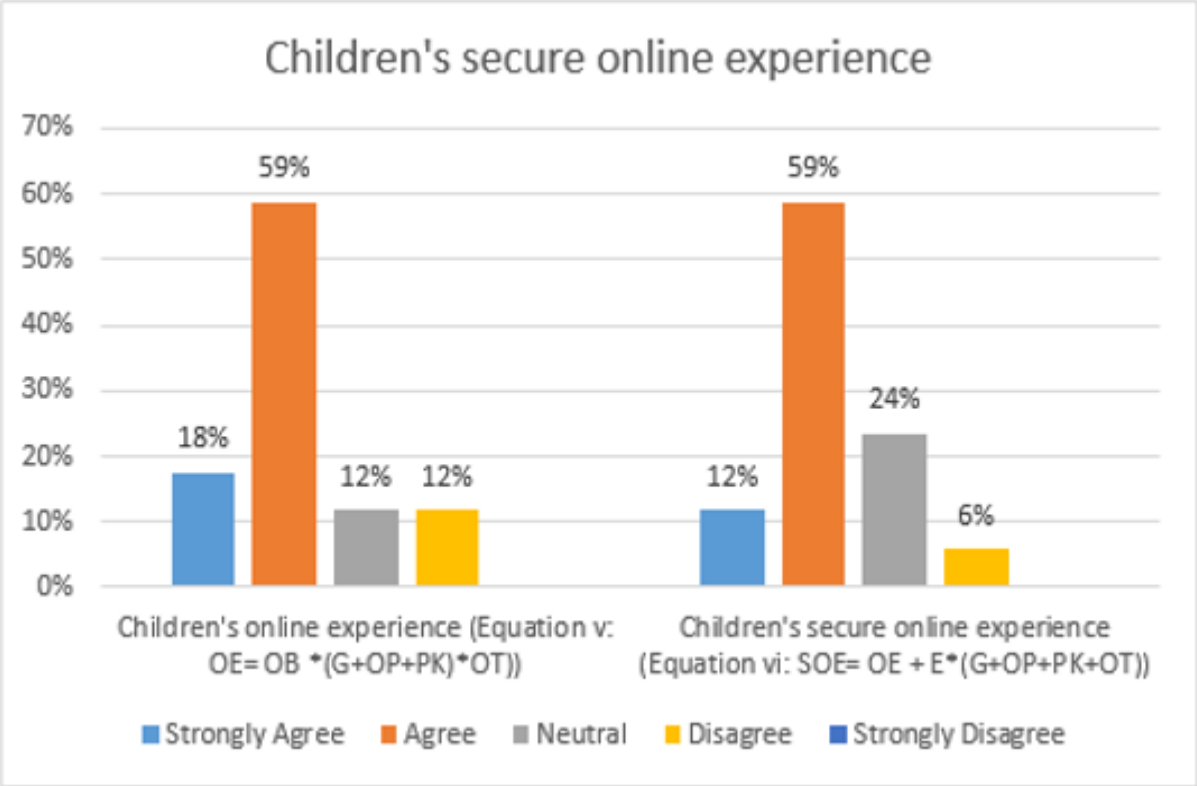


Figure 5.14: Children's secure online experience components relationship

Most of the experts agreed on the components relationship on children's online experience and the children's secure online experience. Out of 17 experts, 2 experts felt neutral and disagreed on the components relationship on children's online experience, they did not have any suggestions or feedback to the relationship. Additionally, on the children's secure online experience components relationship 1 expert disagreed with the children's secure online experience component relationship while 4 experts felt neutral, however no reasons were provided except for one suggestion to create awareness. Table 5.9 presents the comments from the experts on relationship 3.

Table 5.9: Expert feedback on children's secure online experience

Expert	Expert Feedback and Suggestions on component relationship 3	How the comments were addressed
P1	No	
P2	Empowerment has a 50/50 chance to result in either SOE or otherwise.	True
P3	No. it is well presented	
P4	SOE= OE + E*(G+OP+PK+OT) was not supposed to be: SOE= OE + E*(G+OP+PK) * OT)	SOE= OE +PK+ E*(G+OP)*OT) Children's secure online experience (SOE) is the summation of their online experience, prior knowledge and empowerment over the gadget they are using, online platform visited and inherent online threats in gadgets and online platforms.
P5	I am still battling to figure out the rationale behind the E and OE, there may be need for some explanation notes to accompany for a better understanding, otherwise I would rather have OE alone since the E is part and parcel of the OE.	E (Empowerment) - is a set of interventions that will foster. Such as Security knowledge (SK), Secure behaviour (SB), Secure experience (SE), Reduce exposure to online threats in the actors over time (RE). OE (Online Experiences) – Positive online experience (POE), Negative online experience (NOE), Threatening online experience (TOE), Vulnerable online experience (VOE), Secure online experience (SOE), Happy online experience (HOE), Miserable online experience (MOE)
P6	No changes required	
P7	None	
P8	No	
P9	To create awareness	True, the COSBIA focus is to influence children's behaviour online and raise their cyber security awareness as early as they can be online.
P10	No	
P11	No	
P12	No	
P13	No	
P14	no	
P15	No	
P16	no	
P17	No	

The experts' comments on children's secure online experience, mostly highlighted that they had no improvements on this component relationships but a suggestion was made to change the children's secure online experience. Additionally, three other suggestions were made on secure online experience, a request to differentiate between empowerment and online experiences and a suggestion was given to create awareness of which all comments were addressed in Table 5.9. Therefore, it is concluded that the equation on children's online experience components are relevant.

Child online secure behaviour influencing algorithm assessment

The experts were asked to assess the relationship on children's secure online experience on a scale of 1-5 in order to evaluate the composition of COSBIA. Figure 5.15 illustrates the experts' assessment on the overall COSBIA's components relationships.

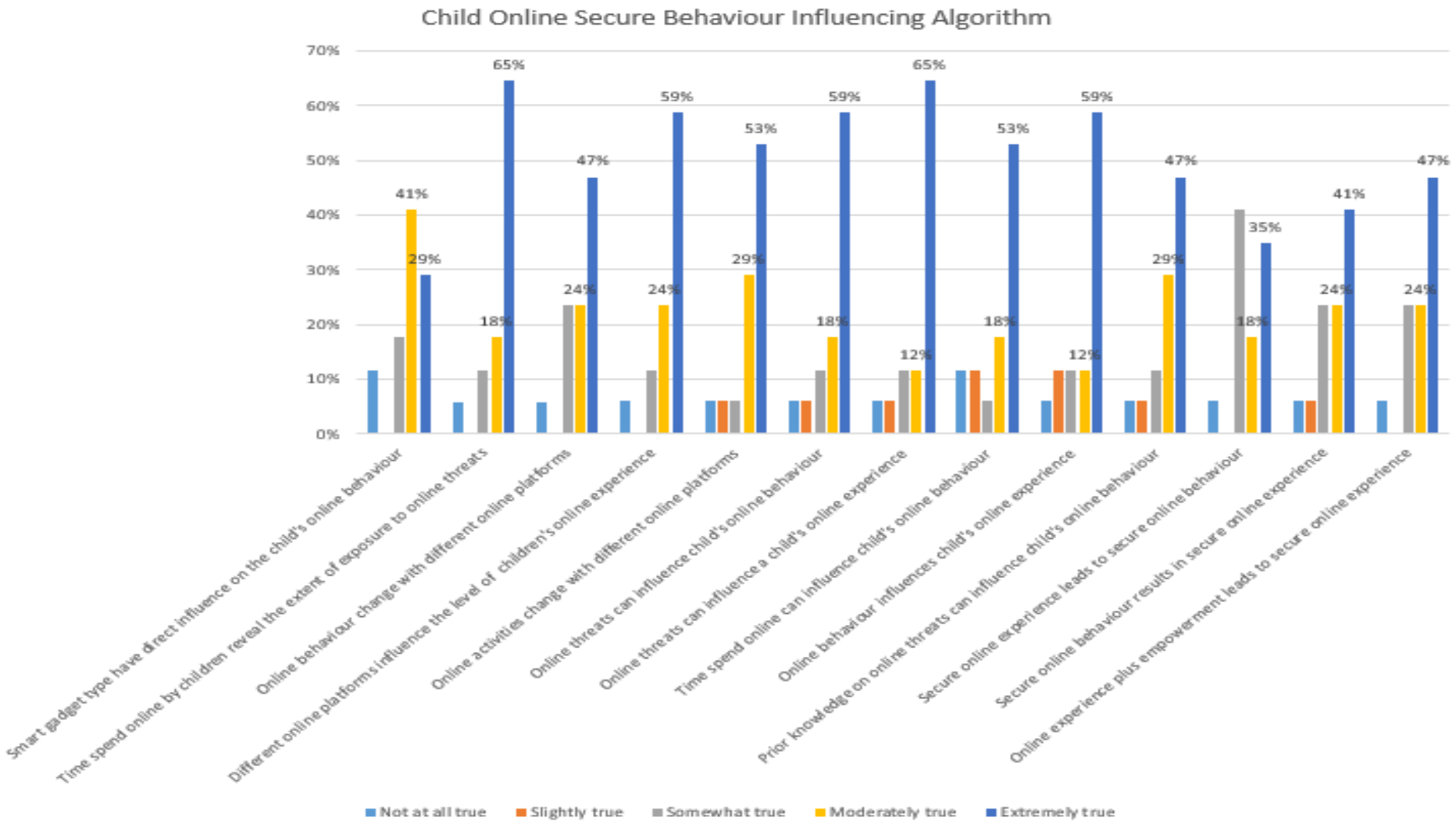


Figure 5.15: Child online secure behaviour influencing algorithm components relationship

The review on the overall components of the children's online experience were positive for most of the experts. This is in alignment with the findings in Figure 5.12 that show that the majority of experts agreed that smart gadgets, online activities, online platforms, online behaviour and time spent online have a direct influence on children's online experience. The results from **Error! Reference source not found.**, **Error! Reference source not found.** and Figure 5.15 reveal that most of the reviewers agreed on the relationship between the components of COSBIA. This means that the COSBIA components are valid and relevant in achieving secure online experiences among children. Table 5.10 presents the comments from experts on the composition of child secure behaviour influencing algorithm.

Table 5.10: Experts feedback on the overall components relationship of COSBIA

Experts	Experts feedback and suggestions on component relationship on child online secure behaviour influencing algorithm	How the comments were addressed
P1	no	
P2	Context of use. If in the presence of "friends" the Prior Knowledge of online threats or secure online behaviour may be useless if factors like peer-pressure are introduced. This may be an extension of the algorithm. The case of the Momo game and child online platform use may be an angle of category to investigate as well.	True: The Context of Use (COU) comes in place here. The gadgets used, online platforms visited and online activities performed can trigger online behaviour habits of a child and thus affects the child's online experience. It is therefore important to include the empowerment aspect, in order to get empowered if their security levels are lower in prior knowledge (e.g. peer-pressure, etc.), their online activities, online platforms and online behaviour.
P3	No. Most imminent areas are covered	
P4	None	
P5	It's unfortunate that I couldn't locate the Table 5 that was being referenced here, so there might be not fruitful inputs to that effect.	Proper alignments were made
P6	No changes required	
P7	None	
P8	not sure	
P9	Nothing to recommend is complete	
P10	No	
P11	No	
P12	No	
P13	No	
P14	no	
P15	no	
P16	No	
P17	No	

The overall experts' comments on the algorithm flowchart are presented in Table 5.11.

Table 5.11: Experts' comments on the algorithms flowchart

Experts	Experts feedback and suggestions on the algorithm flowchart	How the comments were addressed
P1	No comment	
P2	The score is not clear as to why it needs to be exactly equal to 3 empowerment(s).	The score =3 is an example of the level of score required to move to the next level. Get empowerment if their security levels are lower than a score of three. Online behaviour should be secure to move to the next level (Level 1 to level 2 a score of 3 out of should be obtained, Level 2 to level 3 score of 3 should be obtained, Level 3 to exit back to activity a score of 3 should be obtained). The scoring sheet is provided in Appendix H: COSBIA Game Concept or section 5.2.5 in full.
P3	The process "move to another level" might not be necessary	It highlights the progression of the child through the levels of empowerment.
P4	"Online Behaviour = Online platform = Gadget + Online activities..."etc. Or you mean/I think it is "Online Behaviour = Online platform + Gadget..." Based on the previous algorithm variables, the two are not the same thing... The second stage of the flowchart is read, I think it should be read Gadget; Online activities; Online platform not plus. Because you not yet computing	True: Flowchart corrected Online Behaviour = Online Platform + Gadget + Online Activities + Prior Knowledge + Online Threats + Online Experience True: Flowchart corrected Read Gadget; Online activities; online platforms
P5	Why is the time spent not part of the parameters as was being represented in the previous equations? Recheck the first equation on computing online behaviour. One main question though is, who determines the online threats? The algorithm or the child? If it's the algorithm, how do you measure the level of assertiveness of the child to the identified threats? If it's the child, how is the scoring determined if the threats vary in the degree of complexity?	Time spent is to analyse how much time the child spend online (at least daily (LD), At least weekly (LW), At least monthly (LM), Almost all the time (AT)). The Time Spent Online (TSO) and the child's Online Behaviour (OB) while performing OA on an OP using G results in a child's online experience (OE) which can either be secure or insecure. In set notation OE(C) is a result of time spent online (TSO) over set of G, OA, OP, OB. **Equation 5.1:** ***OE(C) = TSO*(G+OA+OP (OPB) +OB (OGB))*** The COSBIA determines the online threats based on a database of known threats, and the level of assertiveness is measured through a quiz that covers on online threats on online platform specific threats, online activities specific threats, gadget specific threats and online behaviour specific threats. The main idea is for the child (player) to come and perform whatever they want to perform not play a game. What the

		algorithm does is that it reads information of the child's gadget they are using, the platforms they are visiting, the activities they are performing and the way they are behaving. When it reads the information there is a database and in the database there are identified threats for those different platforms, activities, behaviour and the gadget being used.
P6	I would recommend you to provide a pseudocode of the above flowchart as well	Pseudocode provided on the flowchart in the final algorithm section 5.2.6.6.
P7	The element of online supervision and guidance effect on children's online behaviour and activities	Based on the assumption that when parents/guardians/ caregivers allow the child access to online platforms they also provide basic etiquette to the child (based on parental guidelines in table 2.7). Studies have however highlighted the challenges of these custodians mainly having less knowledge and involvement in this regard. In future we intend to educate the caregivers to empower them to take responsibility to supervise online activities. This can be through tools such as Net nanny.
P8	What is score 3?	The score =3 is an example the level of score required to move to the next level. Get empowerment if their security levels are lower than a score of three. Online behaviour should be secure to move to the next level (Level 1 to level 2 a score of 3 out of should be obtained, Level 2 to level 3 score of 3 should be obtained, Level 3 to exit back to activity a score of 3 should be obtained).
P9	The element of social influence is missing	The social influence is captured under prior knowledge which is a subset of the Knowledge component in COSBIA as presented in Table 5.1
P10	It is well outline in terms of flow of information, however it appears too busy and complicated for the untrained eye. Too complicated.	Noted, however it is meant for developers to implement, being technical, it I assumed they can handle the details.
P11	None	
P12	I see relationship with each variable	
P13	I really did not grasp the questions well	
P14	Workflow may have an error in the Get Empowerment step, is it a decision or how?	Get Empowerment is a process that the child needs to go through before moving to the next stage.
P15	Looks okay	
P16	The flowchart has all the correct information, but doesn't flow well, i.e. not easy to read	Addressed in the presentation as shown in Figure 5.19.
P17	Very well displayed and put together	

Concluding insights

The aim of this section was to evaluate the proposed child online secure behaviour influencing algorithm. The algorithm was evaluated by experts and their demographic information is presented in Table 5.6. The algorithm evaluation tool was formulated according to the objectives of the study and to determine if the designed algorithm is necessary, whether it will influence children's behaviour online and raise their cybersecurity awareness. The COSBIA evaluation tool was created using Google forms (Appendix G: Expert Review Evaluation Form

From the results on the overall child online secure behaviour influencing algorithm (COSBIA) components relationship, it showed that most reviewers agree with the relationships between most of the components except for one expert who disagreed, however, the expert did not provide feedback on the disagreement. Yet still, it could be concluded that the type of smart gadget, online activities, online platform, online behaviour and time spent online have a direct influence on the children's online experience.

5.2.6.6. Final algorithm

The analysis of the expert assessment of the components and relationships on child online secure behaviour algorithm has not suggested many changes.

Relationship 1: A child (C) interacts with an Online Platform (OP) to perform Online Activities (OA) using a smart gadget (G). The Time Spent Online (TSO) and the child's Online Behaviour (OB) while performing OA on an OP using G results in a child's online experience (OE) which can either be secure or insecure. This is due to the fact that G has an influence on OB, which results in gadget specific behaviour (OGB) and OP has an influence on OB which results in platform specific behaviour (OPB). Figure 5.5 represents relationship 1. In set notation OE(C) is a result of time spent online (TSO) over set of G, OA, OP, OB.

Equation 5.11: $OE(C) = TSO*(G+OA+OP\ (OPB) +OB\ (OGB))$

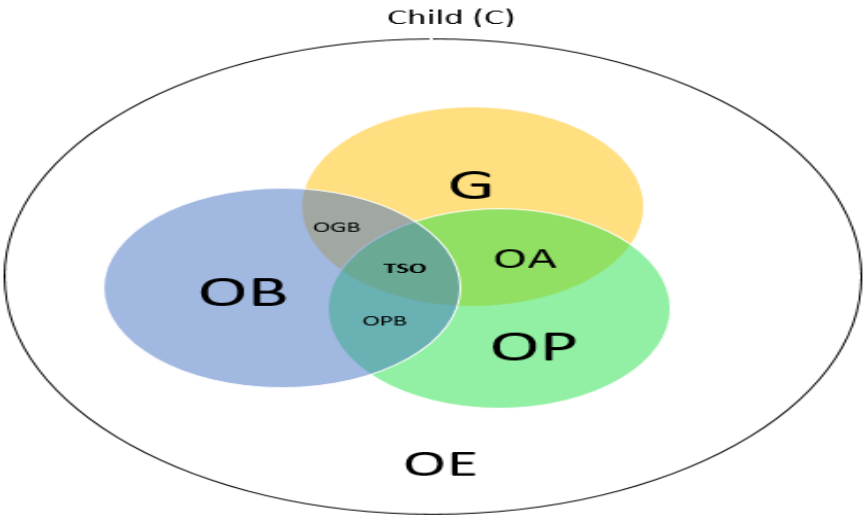


Figure 5.16: Component relationship 1

Relationship 2: The child's (C) prior knowledge (PK) and their online behaviour (OB) exposes them to online threats (OT) inherent in G, OA and OP, and this results in a child's online experience (OE). If empowerment is added to this interaction, it would result in a secure online behaviour (SOB). We posit that a secure online experience (SOE) is a result of secure online behaviour and this relationship is shown in Figure 5.6 . SOE (C) is a result of applying a set of E to enhance PK and OB of/with OA, OP, and G in the presence of OT.

Children's online behaviour is a summation of the type of online platform they are visiting, the type of gadget they are using, the types of online activities they are performing, their prior knowledge, the online threats posed to them and their online experience

Equation 5.12: $OB = OP+G+OA+PK+OT+OE$

Children's online experience is a product of their online behaviour and the combination of the online platforms they are visiting, the gadget they are using, the online activities they are performing, their prior knowledge and the online threats posed to them.

Equation 5.13: $OE = OB*(OP+G+OA+PK+OT)$

Children's secure online behaviour is the summation of their online experience and empowerment on the gadget, online activities, online platform and online behaviour, where secure online behaviour is proportional to secure online experience.

Equation 5.14: $SOB = OE + E*(G, OA, OP, OB)$

$SOB = SOE$

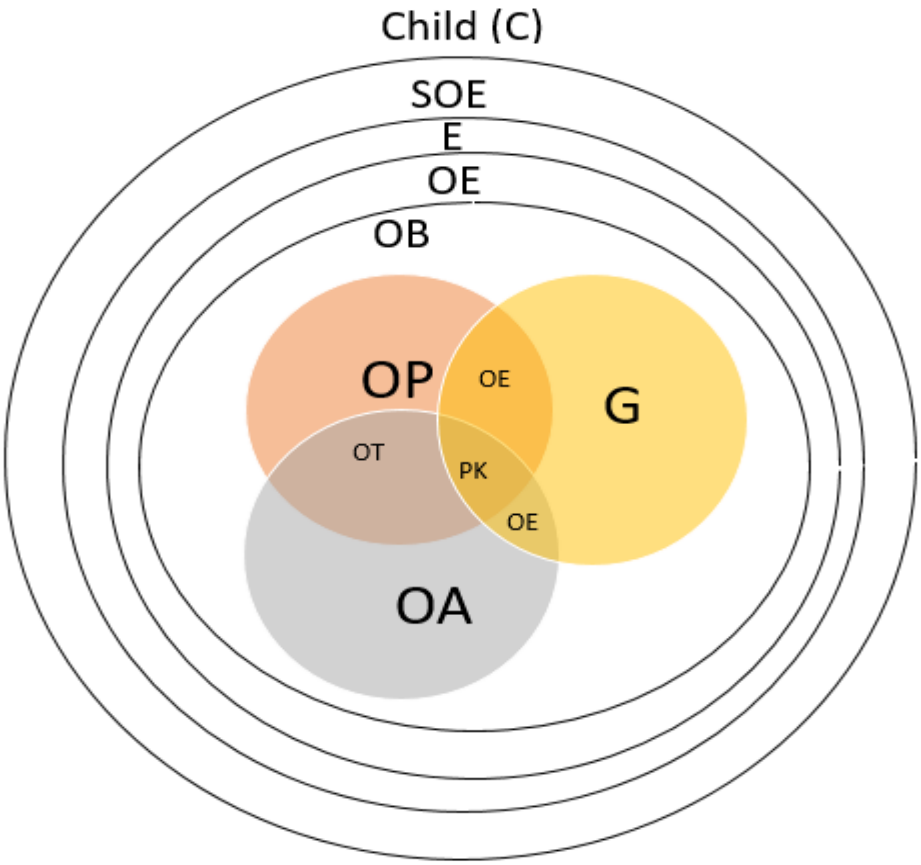


Figure 5.17: Component relationship 2

Relationship 3: A child (C) interacts with an Online Platform (OP) using a smart gadget (G) to perform Online Activities (OA). Adding prior knowledge while using the gadget (G) results in the gadget knowledge (GK). Adding prior knowledge (PK) while interacting on online platforms results in online platforms knowledge (OPK). When one adds prior knowledge while using a gadget and visiting online platform, this influences online behaviour (OB) in the presents of online threats (OT). If empowerment is added then secure online experience (SOE), is the result.

Children's online experience is a product of their online behaviour and a summation by the posed online threats on the gadgets used, the online platform visited and their prior knowledge.

Equation 5.15: $OE = OB * (G + OP + PK) * OT$

Children's secure online experience (SOE) is the summation of their online experience, prior knowledge and empowerment over the gadget they are using, the online platform visited and inherent online threats in the gadgets and online platforms.

Equation 5.16: $SOE = OE + PK + E * (G + OP) * OT$

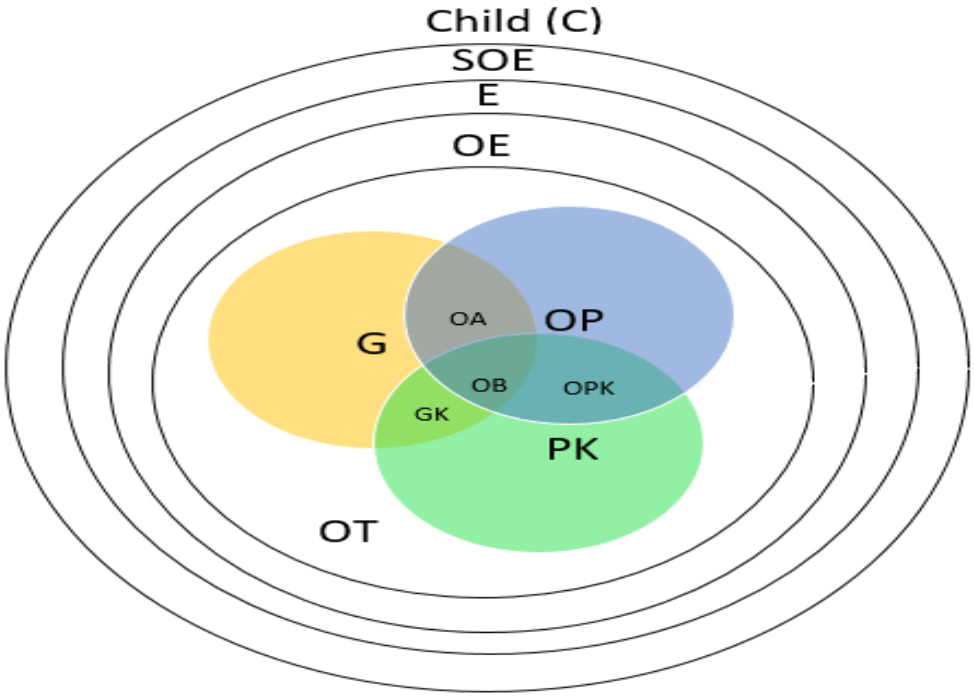
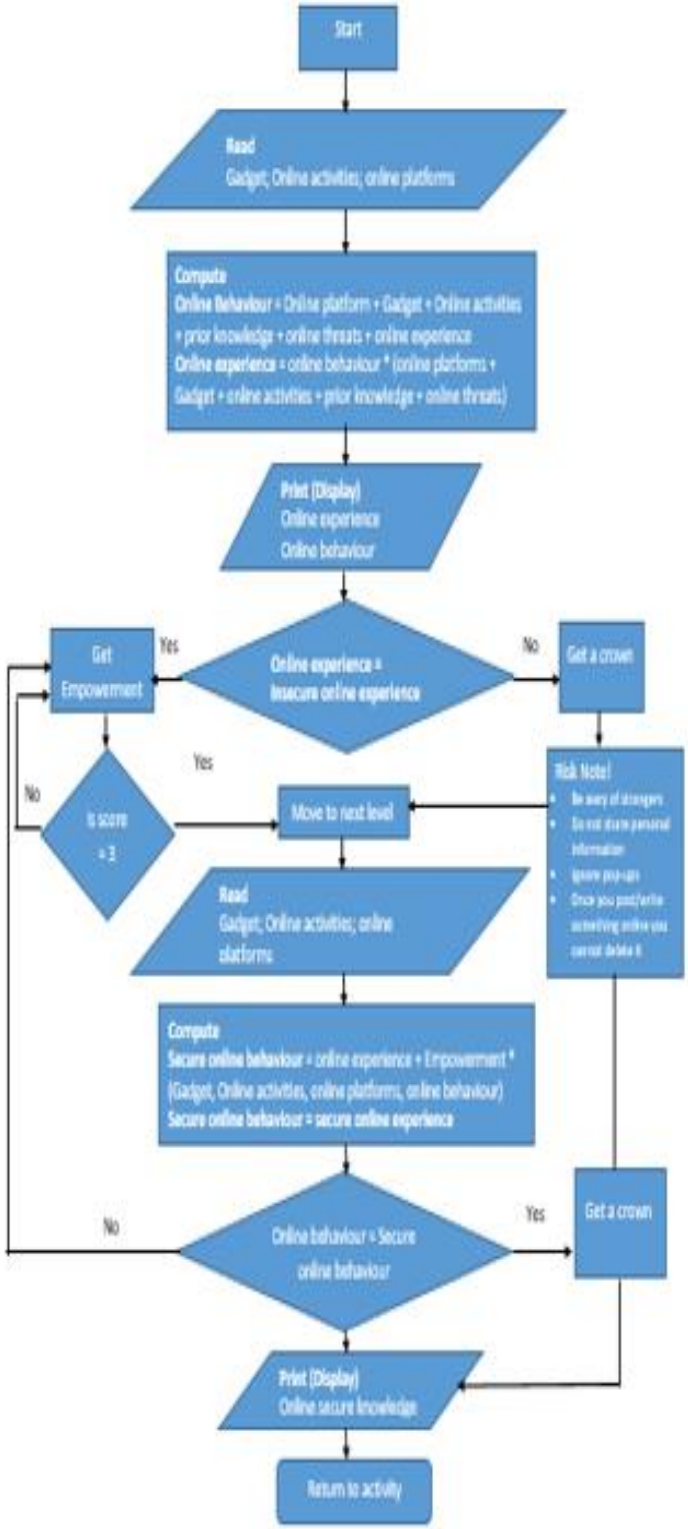


Figure 5.18: Component relationship 3

COSBIA flowchart and Pseudo code



Pseudo code
PRAGRAM COSBIA

Read Gadget; online platforms; online activities

Compute online behaviour and online experience

Display online experience and online behaviour

IF Online experience = secure online experience, then
Get crown THEN
Move to next level
Else
While online experience = insecure online experience, then
DO
Get empowerment,
UNTIL empowerment score = 3, THEN
Move to step 6
DONE

Compute secure online behaviour
If online behaviour = secure online behaviour THEN
Get a crown THEN
Move to step 11
ENDIF
WHILE online behaviour! = secure online behaviour
DO
Get Empowerment
UNTIL (Empowerment score = 3) THEN
Move to step 9
DONE

Display Online secure knowledge

Return to activity

Figure 5.19: COSBIA flowchart and Pseudo code

5.2.7. STAGE 6: Communication

This thesis will be communicated through the following:

- Raising awareness at schools in Namibia;
- Introducing the algorithm to children and raising cyber security awareness at schools in Namibia through game play;
- Providing guidelines on how to influence children's online behaviour to parents and teachers;
- Through the behaviour influencing algorithm game, which will assist children on how to securely behave online; and
- Findings will be published in scholarly publications.

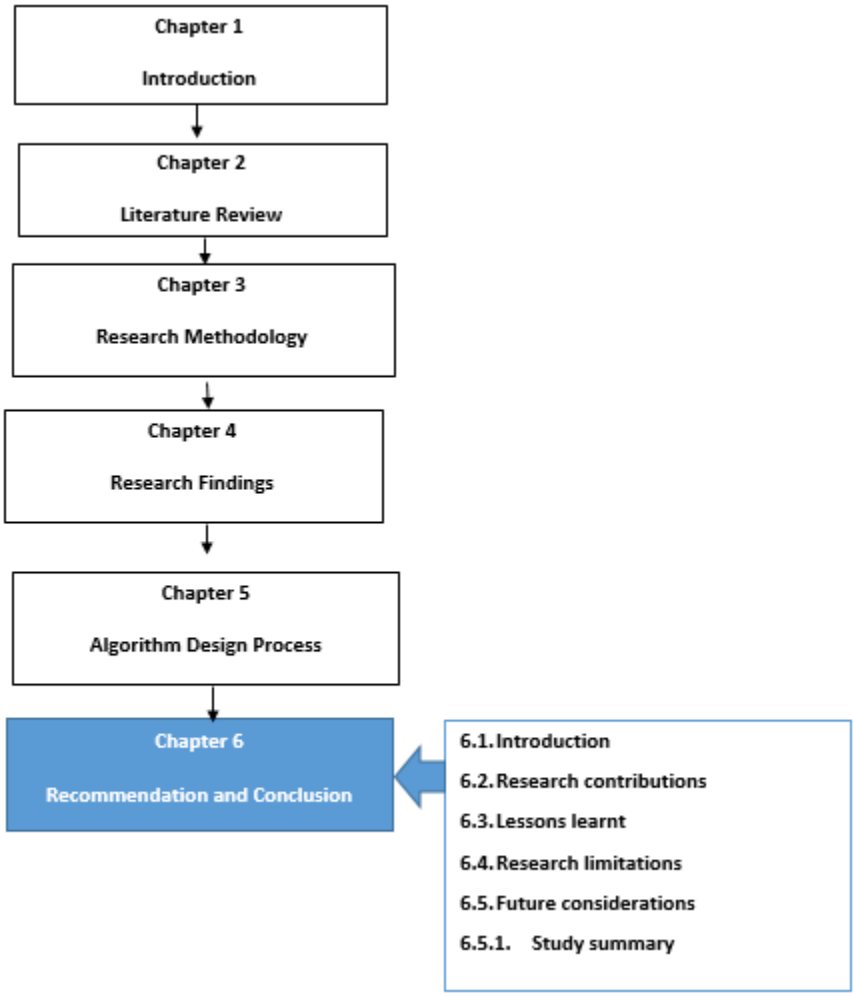
5.3. Chapter summary

This chapter presented the process that was used to design a behaviour influencing algorithm that is suitable for the security of children engaged in online activities. The algorithm was designed following the steps of the design science research method. In the first stage of the design science research method the research problem was identified and motivated. In the second stage the objective of a solution was defined. The third stage outlined the design and development of the algorithm by identifying the components of the algorithm, the relationship between the components, the definition of the algorithm, architecture and the formulation of the COSBIA integrating persuasion theories. COSBIA was presented in six equations and in a flowchart. A demonstration of how the COSBIA will work was presented in stage four. In stage five, the COSBIA was evaluated by experts that are specialists in the field of information security, cybersecurity, HCI and children's digital rights.

The results from the experts' reviews showed that most reviewers agreed with the relationship between most of the components, and generally all were positive and suggestions were made to improve. Based on the recommendations, the final equations were presented in section 5.2.6.6 and the revised flowchart was presented in Figure 5.19.

The last stage on the way the algorithm will be communicated was outlined. The next chapter (Chapter 6) presents the recommendation and conclusion of this study.

Chapter 6: Recommendations and Conclusion



6.1. Introduction

This chapter concludes the study by presenting various recommendations with respect to the objectives and aims highlighted during this study, based on the findings of the analysis outlined in Chapter 4. Additionally, the research contribution, reflection, lessons learnt, research limitations and future considerations are provided as well. The previous chapters presented the research problem, literature, methodologies, the findings and the design of the algorithm. The research problem was based on the fact that out of innocence, the behaviour of children potentially exposes them to cyber criminals as the children innocently share information and befriend strangers.

The key to influence children's behaviour online is through empowering them on the online threats that may be posed to them, namely, general Internet threats, online platform specific threats, online activities specific threats, gadget specific threats, and online behaviour specific threats.

Revisiting the objectives of this study

The main objective of this study was to design an algorithm that will influence children's behaviour online in order to reduce cyber security risks. In order to achieve the main objective, this research established the following sub-objectives:

1. Analyse how children behave online;
2. Evaluate online activities that expose children's interactions with strangers; and
3. Evaluate behaviour analysing tools that are suitable for child online activities.

All three sub-objectives were accomplished by detailed analysis of the related literature that was later evaluated in the analytical part of this study. In addressing the first sub-objective, it was found that the children's behaviour online involves risky activities such as befriending strangers, sharing of personal/private information, sending pictures or videos of themselves with strangers, meeting strangers in person, and sharing emotions and feelings online. This analysis of how children behave online is presented in Table 2.2.

The second sub-objective was addressed and the findings of the evaluation are presented in Table 2.1 and Table 2.2. It was found that the online activities that expose children's interactions with strangers were playing online games, watching/uploading videos, visiting social networking sites and searching for information. Cyberbullying, sexual exploitation, impersonation, online sexual harassment and access to inappropriate content are some of the risks associated with the various children's online activities. Children mostly perform particular risky activities on the Internet because they believe that it is easier to be themselves online and they believe that it promotes respect and kindness.

In achieving/addressing the third sub-objective, it was found that the behaviour analysing tools that are suitable for child online activities are VisMOOC, Web miner, Webalizer and E-web miner. VisMOOC is appropriate because it analyses user behaviour, what they have access to and their patterns of activity, and with this the right empowerment strategy can be designed to secure their online experiences. The Web miner searches users' information and the user's access patterns. This is important in understanding what the children access online. The Webalizer analyses online behaviour and it is better than VisMOOC

because it supports 30 languages, and it runs on THE cross-platforms operating system. Lastly the E-web miner uses an algorithm that mines web content, web layout, web logs and web content as presented in Section 2.6. Additionally, these tools analysed children's behaviour through:

- Clickstream analysis
- Interaction analysis
- Application should be easy to use, portability, transparency, efficiency and robustness
- Screen time analysis
- User patterns analysis
- Providing tips of empowerment on online topics
- Activity patterns analysis
- Mining browsing information

By analysing the different tools used online to analyse children's behaviour, this has helped to shape the design of the behaviour influencing algorithm that will be suitable for the security of children's online activities. Most of the capabilities were used in designing COSBIA such as analysing clickstream, interactions, screen time, user patterns, activity patterns, mining browsing information and providing tips of empowerment on online topics. And on the features of the application, we only adopted the ease of use and effectiveness, then we added enjoyable.

The outcome of objective 1: Analyse how children behave online, objective 2: Evaluate online activities that expose children's interaction with strangers, and objective 3: Evaluate behaviour influencing tools suitable for chid online activities, helped to identify what makes up the children's online behaviour, online experience, secure online behaviour and secure online experience that were used to achieve the main objective, that is to design a behaviour influencing algorithm that is suitable for the security of children's online activities.

6.2. Research contributions

The study contributes significantly to the Namibian children's online safety, the Ministry of Education and the research community at large in the following ways:

- This study contributes to the empirical gaps that are in the literature on child online protection specifically in developing countries through COSBIA, an algorithm that influence the security of children's behaviour online.

- COSBIA helps to raise awareness on the possible online threats that children may encounter while online, in so doing the children will be safe online.
- This study has made available activities that specifically expose children who interact with strangers to the research community through a publication (Appendix J: Publications and this thesis document.
- Guidelines (Table 2.5) are provided on how to influence children's behaviour online, which can be used elsewhere.
- COSBIA can also support the Ministry of Education and other organisations involved in childcare by:
    - Providing Cyber Security Awareness material and a platform that can be included in the school curriculum to avert online abuses.
    - Empowering children on secure online behaviour especially now that education has moved to e-learning due to the Covid-19 outbreak.

6.3. Lessons learnt

Through this study, a lot of insights were gained in the field of HCI, specifically user behaviour as an in-depth understanding of factors influencing children's online behaviours and cyber security was pursued. These insights are important because they provide the basis for supporting the value of this study. The lessons learnt are:

i. Set clear research focus and limited goals: At the start of the research, I lacked a clear purpose and the importance of the study, however as I progressed, I could set SMART goals.
ii. Criticism helps you to improve and helps your research to get better: Throughout the years of research, I've learnt a lot of things about myself based on my research criticism from my supervisor. It helped me to learn things I've never known about research and myself, and that was instrumental to my growth. Second, our response to that criticism is important. I have learnt a lot about myself based on the emotions that surfaced when I received criticisms from my supervisor and how I responded. I've learnt that my reactions usually reflect unprocessed inner problems. Working through these reactions has helped me to become a calmer and self-aware person.
iii. Use cloud tools always to back up your work
iv. There is no short cut in research

v. Time is of essential importance

6.4. Research limitations

This study was limited in several ways noted here. This study only covered four schools in Windhoek, and as such, the basis might not be reflective of the different children we have in the nation. An effort was made to include children from all socio-economic backgrounds prevalent in the nation with the exception of the actual context which can be rural, urban or peri-urban. For the algorithm evaluation, a live hackathon was scheduled so as to implement and evaluate the algorithm. However, due to the Covid-19 pandemic an online one was scheduled. A limited number of teams then signed up, and those who came on board had challenges with data and coordination. The developers found the implementation to be complex and the end product had limitations as shared in section 5.2.5. The children could not test the efficacy, utility and experience of the implementation for refinement.

6.5. Future considerations

In future, the researcher will complete the demonstration of COSBIA through gamification and have it evaluated by children in all regions and typical setups in Namibia. Feedback will be used to further refine the algorithm and implementation. Partnerships with technology influencers and children trustees will be sought to fund a full development of and facilitate the final deployment of the awareness tool on devices. Key stakeholders in child welfare will be engaged as a way to raise cyber security awareness in children in and out of schools around Namibia.

6.5.1. Study summary

This study aimed to design an algorithm for influencing online actions of children. The study was inspired by understanding the lack of guidelines to influence online behaviour in children. This has contributed to the COSBIA concept as a solution to the defined gap. Researching the nature of the problem, formulating research questions and aiming for results was carried out in Chapter 1.

Chapter 2 was used to classify literature that was important to this study. This looked at the online dangers of children, online behaviour, online behaviours that expose them to communicating with strangers and their level of activity and actions on the Internet. Then a general analysis was done on the various online

tools for analysing behaviour. Ultimately, a review of the approaches used to design a behaviour influencing algorithm was done and deep learning algorithms approaches were chosen as appropriate.

The research followed a paradigm of design science while observing a pragmatism philosophical posture. A mixed method approach was used in the study, employing an inductive mode of reasoning. The data collection strategies in the research included a literature study, expert reviews consisting of academic reviews of publications submitted to international conferences, as well as questionnaires with children. The research methodology section of the study was presented in Chapter 3.

Chapter 4 presented an analysis on the research findings on the platform mostly visited by children, their online activities, the devices they use to access the Internet, where they access the Internet from, the types of information shared online and their online experience.

Chapter 5 served to design the COSBIA, and five phrases were followed to design COSBIA. The five stages used to design COSBIA are namely: Identify the problem and motivate, define the objective to the solution, design and development, demonstration, evaluation and communication of COSBIA.

The proposed conceptual COSBIA was then evaluated for its validity through game and expert reviews. This was done in the form of a survey using experts as well as through children playing the COSBIA game. The results of the evaluation were used to refine the conceptual algorithm to the COSBIA that was presented in Chapter 6.

It can be concluded that the purpose of the research was satisfied through the identification of the components of the algorithm for influencing children online behaviours and through the design of COSBIA.

References

Agarwala, S., & Schwan, K. (2006). *SysProf: Online distributed behavior diagnosis through fine-grain system monitoring.* Proceedings - International Conference on Distributed Computing Systems. https://doi.org/10.1109/ICDCS.2006.81

Al-Badi, A. H., Al Mahrouqi, S., Ali, O., Al-Badi, A., & Khaled Hassan, M. AL. (2016). The influence of the internet on teenagers' behaviour in Oman. *Journal of Internet Social Networking & Virtual Communities*, *2016*. https://doi.org/10.5171/2016.171712

Amutan, K. I. (2014). A review of B. F. Skinner's reinforcement theory of motivation. *Journal of Advances in Chemistry*, *10*(1), 2146–2161. Retrieved from https://www.researchgate.net/publication/306091479_A_Review_of_B_F_Skinner%27s_%27Reinforcement_Theory_of_Motivation

Anderson, M. (2018). *A majority of teens have experienced some form of cyberbullying*. (September 27), 1–18. Retrieved from http://www.pewinternet.org/2018/09/27/a-majority-of-teens-have-experienced-some-form-of-cyberbullying/

Anderson, M., & Jiang, J. (2018). *Teens' social media habits and experience*. (May). Retrieved from https://www.pewresearch.org/internet/2018/11/28/teens-social-media-habits-and-experiences/

Atanasova, D., & Hristova, P. (2015). *Human computer interaction*. Retrieved from https://www.researchgate.net/publication/282278596_HUMAN_COMPUTER_INTERACTION_IN_COMPUTER_SCIENCE_EDUCATION

Atkinson, S., Alqahtani, N., Stengel, I., & Furnell, S. (2017). *Internet risks for children : Parents ' perceptions and attitudes*.. Retrieved from https://ieeexplore.ieee.org/abstract/document/8101918

Baskerville, R., Baiyere, A., Gregor, S., Hevner, A., & Rossi, M. (2018). Design science research contributions: Finding a balance between artifact and theory. *Journal of the Association of Information Systems*, *19*(5), 358–376. https://doi.org/10.17705/1jais.00495

Beaudouin-Lafon, M. (2006). Human-computer interaction. *Interactive Computation: The New Paradigm*, 227–254. Retrieved from https://doi.org/10.1007/3-540-34874-3_10

Bhunu Shava, F., Chitauro, M., Mikka, J., Nhamu, I., & Gamundani, A. (2016). *Exploratory research study on knowledge, attitudes and practices of ICT use and online safety risks by children in Namibia*. Retrieved from https://www.un.org.na/home_htm_files/na.COP_Research_Report_2016.compressed.pdf

Broughton, D. D. (2009). *Child exploitation in the 21st century*. Retrieved from https://doi.org/10.1016/j.paed.2009.08.006

Brown, P., Evans, M., Hunt, D., Mcintosh, J., Pender, B., & Ramagge, J. (2011). *Sets and venn diagrams*. Retrieved from http://amsi.org.au/teacher_modules/pdfs/Sets_and_venn_diagrams.pdf

Cacciatore, R., & Kaltiala, R. (2019). The Steps of Sexuality — A developmental , emotion-focused , child-centered model of sexual development and sexuality education from birth to adulthood. *International Journal of Sexual Health*, *31*(3), 319–338. https://doi.org/10.1080/19317611.2019.1645783

Calder, A. (2019). NIST Cybersecurity Framework - Aligning to the NIST CSF in the AWS Cloud. *NIST Cybersecurity Framework*. Retrieved from https://doi.org/10.2307/j.ctv4cbhfx

Conlan, R. M. (2005). *Human Computer Interface Security (HCISEC)*. Retrieved from https://doi.org/10.5040/9781501371738.ch-001

Cooley, R., Mobasher, B., & Srivastava, J. (1997). Web mining: information and pattern discovery on the World Wide Web. *Proceedings Ninth IEEE International Conference on Tools with Artificial Intelligence*. https://doi.org/10.1109/TAI.1997.632303

Creswell, J. W. (2007). *Qualitative inquiry and research design: Choosing among five approaches*. Retrieved from https://doi.org/10.1016/j.aenj.2008.02.005

Dawson, S., Burnett, B., & McArdle, F. (2005). *Watching learning from behind closed doors: The*

impact of surveillance on student online behaviour. Retrieved from http://www.netnanny.com/products/net_nanny_5/feature

Dix, A. (2017). Human–computer interaction, foundations and new paradigms. *Journal of Visual Languages and Computing*, *42*, 122–134. https://doi.org/10.1016/j.jvlc.2016.04.001

Eloff, M. ., & Eloff, J. H. . (2002). *Human computer interaction: An information security perspectives*. Retrieved from https://doi.org/10.1007/978-0-387-35586-3_46

Erickson, J. (2019). *Algorithms*. Retrieved from https://www.researchgate.net/publication/334233634_Algorithms

Etikan, I. (2017). *Comparison of convenience sampling and purposive sampling*. (January 2016). Retrieved from https://doi.org/10.11648/j.ajtas.20160501.11

Fahrnberger, G., & Heneis, K. (2015). *Securestring 3.0 A cryptosystem for blind computing on encrypted character strings*. Retrieved from https://www.researchgate.net/publication/269203698_SecureString_30_A_Cryptosystem_for_Blind_Computing_on_Encrypted_Character_Strings

Fire, M., Goldschmidt, R., & Elovici, Y. (2014). Online social networks: Threats and solutions. *IEEE Communications Surveys and Tutorials*. https://doi.org/10.1109/COMST.2014.2321628

Fryling, M., & Hayes, L. J. (2011). *Understanding observational learning : An interbehavioral approach understanding observational learning : An interbehavioral approach*. (April). https://doi.org/10.1007/BF03393102

Gacenga, F., Cater-Steel, A., Toleman, M., & Tan, W. G. (2012). A proposal and evaluation of a design method in design science research. *Electronic Journal of Business Research Methods*, *10*(2), 89–100.

Gardikiotis, A., & Crano, W. D. (2015). Persuasion theories. *International Encyclopedia of the social & behavioral sciences* (2nd ed.). (September 2019), 941–947. https://doi.org/10.1016/B978-0-08-097086-8.24080-4

Garfinkel, S. L. (2005). *Future work : An HCI-SEC research agenda*. 349–370. Retrieved from https://simson.net/thesis/agenda.pdf

Ghari, W. (2012). Cyber threats in social networking websites. *International Journal of Distributed and Parallel Systems*, *3*(1), 119–126. https://doi.org/10.5121/ijdps.2012.3109

González-ortega, E., & Orgaz-baz, B. (2013). *Minors ' exposure to online pornography in Spain : Prevalence , motivations , contents and effects . Minors ' exposure to online pornography : Prevalence, motivations, contents and effects*. (May 2014). Retrieved from https://www.scopus.com/inward/record.uri?eid=2-s2.0-84877140176&doi=10.6018%2Fanalesps.29.2.131381&partnerID=40&md5=bf1e0f94bc52e698957d9f724bf41cf3

Green, L., Ólafsson, K., & Hartley, J. (2011). *Risks and safety for Australian children on the internet*. https://doi.org/10.5334/csci.40

Gunawan, F. E., Ashianti, L., & Sekishita, N. (2018). A simple classifier for detecting online child grooming conversation. *Telkomnika (Telecommunication Computing Electronics and Control)*, *16*(3), 1239–1248. https://doi.org/10.12928/TELKOMNIKA.v16i3.6745

Hangtwenty. (2018). Dive into Machine Learning. *Github* (October). Retrieved from https://github.com/hangtwenty/dive-into-machine-learning

Harris, S., & Ross, J. (2006). *Beginning algorithms*. Retrieved from https://doc.lagout.org/science/0_Computer Science/2_Algorithms/Beginning Algorithms %5BHarris %26 Ross 2005-11-07%5D.pdf

Hasib, A. Al. (2009). Threats of online social networks. *Proceedings - Annual Computer Security Applications Conference, ACSAC*, *36*(11), 335–344. https://doi.org/10.1109/ACSAC.2008.36

Hendrix, M., Al-Sherbaz, A., & Bloom, V. (2016). Game based cyber security training: Are serious games suitable for cyber security training? *International Journal of Serious Games*, *3*(1). https://doi.org/10.17083/ijsg.v3i1.107

Herselman, M., & Botha, A. (2015). Evaluating an artifact in design science research. *ACM International Conference Proceeding Series*, *28-30-Sept*(September). https://doi.org/10.1145/2815782.2815806

Heyvaert, M., Maes, B., & Onghena, P. (2013). Mixed methods research synthesis: Definition, framework, and potential. *Quality and Quantity*, *47*(2), 659–676. https://doi.org/10.1007/s11135-011-9538-6

Hillman, H., Hooper, C., & Choo, K.-K. R. (2014). Online child exploitation: Challenges and future research directions. *Computer Law & Security Review*, *30*(6), 687–698. https://doi.org/10.1016/j.clsr.2014.09.007

ITU. (2010). *Child online protection statistical framework and indicators*. Retrieved from https://www.itu.int/dms_pub/itu-d/opb/ind/D-IND-COP.01-11-2010-PDF-E.pdf

ITU. (2014). *Guidelines for children on child online protection*. Retrieved from www.itu.int/cop

ITU. (2018). *Global cybersecurity index (GCI) 2018 ITU publications studies & research*. Retrieved from https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

ITU. (2019). *Global cybersecurity index, 2017*. *Measuring the digital transformation*. Retrieved from https://doi.org/10.1787/5d87fa05-en

Johnson, G. M. (2006). *A theoretical framework for organizing the effect of the Internet on cognitive development*. Retrieved from https://files.eric.ed.gov/fulltext/ED493998.pdf

Just, M. (2016). *Usability and security usable security examples exercise*. Retrieved from https://coinsrs.no/wp-content/uploads/2016/08/metochi2016-Just-1-COINS_Intro_31July2016.pdf

Kahimise, J., & Bhunu Shava, F. (2019). *An analysis of children's online activities and behaviours that expose them to cybercrimes*. *27th Telecommunications Forum, TELFOR 2019*. Retrieved from https://doi.org/10.1109/TELFOR48224.2019.8971089

Kahimise, J., & Bhunu Shava, F. (2020). *An analysis of social networking threats*. Retrieved from

https://doi.org/10.34190/ICCWS.20.127

Kainda, R., Flechais, I., & Roscoe, A. W. (2010a). Security and usability: Analysis and evaluation. *ARES 2010 - 5th International Conference on Availability, Reliability, and Security*, (February 2010), 275–282. https://doi.org/10.1109/ARES.2010.77

Kainda, R., Flechais, I., & Roscoe, A. W. (2010b). *Security and usability: Analysis and evaluation*. Retrieved from https://ora.ox.ac.uk/objects/uuid:b4b142ed-11f7-48d1-83f9-f4479ca0b84f/download_file?file_format=pdf&safe_filename=ares_main.pdf&type_of_work=Journal+article

Kangootui, N. (2019). *Internet game drives 10-year-old to suicide.* Retrieved from https://www.namibian.com.na/190714/archive-read/Internet-game-drives-10-year-old-to-suicide

Kardefelt-Winther, D. (2017). *How does the time children spend using digital technology impact their mental well-being, social relationships and physical activity? An evidence-focused literature review. I How does the time children spend using digital technology impact their mental we*. Retrieved from www.unicef-irc.org

Kemp, S. (2020, February 18). *Digital 2020: Namibia — Data reportal – Global digital insights.* Retrieved https://datareportal.com/reports/digital-2020-namibia

Khalil, I., Zahoor, K., & Amber, S. (2018). Human Computer Interaction and Security (HCI-Sec). *International Journal of Scientific & Engineering Research*, *9*(4). Retrieved from http://www.ijser.org

Kim, G. J. (2015a). *Human-computer interaction fundamentals and practice*. Retrieved from http://www.copyright.com/

Kim, G. J. (2015b). *Human – computer interaction fundamentals and practice*. Retrieved from http://www.ittoday.info/Excerpts/HCI.pdf

Kirichenko, L., Radivilova, T., & Anders, C. (2017). Detecting cyber threats through social network

analysis: short survey. *SocioEconomic Challenges*, *1*(1), 20–34. https://doi.org/10.21272/sec.2017.1-03

Kovacevicˇ, A., & Radenkovic, S. D. (2020). *Applied sciences SAWIT — Security awareness improvement Tool in the workplace*. Retrieved from https://www.mdpi.com/2076-3417/10/9/3065

Kuechler, B., & Petter, S. (2012). *Design science research in information systems*, (1), 1–66. https://doi.org/1756-0500-5-79 [pii]\r10.1186/1756-0500-5-79

Kundu, S., & Garg, L. (2017). Web log analyzer tools: A comparative study to analyze user behavior. *Proceedings of the 7th International Conference Confluence 2017 on Cloud Computing, Data Science and Engineering*, 17–24. https://doi.org/10.1109/CONFLUENCE.2017.7943117

Kuniavsky, B. Y. M. (2007). *User experience and HCI Section 1 : The boundaries of user experience*. Retrieved from https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.469.4829&rep=rep1&type=pdf

Kuss, D. J., Griffiths, M. D., Karila, L., & Billieux, J. (2014). *Send orders for reprints to reprints@benthamscience.net Internet Addiction: A systematic review of epidemiological research for the last decade*. Retrieved from https://pdfs.semanticscholar.org/1682/7c8aa80f394a5117126e1ec548fd08410860.pdf

Law, E., Roto, V., Vermeeren, A. P. O. S., Kort, J., & Hassenzahl, M. (2008). Towards a shared definition of user experience. *Conference on Human Factors in Computing Systems - Proceedings*, (January), 2395–2398. https://doi.org/10.1145/1358628.1358693

Lecun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. *Nature*, *521*(7553), 436–444. https://doi.org/10.1038/nature14539

Leela Prasad, K., Anusha, P., Srinivasa Rao, M., & Venkata Rao, K. (2019). *A machine learning based preventing the occurrence of cyber bullying messages on OSN*. Retrieved from

https://doi.org/10.35940/ijrte

Livingstone, S., Davidson, J., Batool, S., Haughton, C., & Anulekha, N. (2017). *Children's online activities, risks and safety: A literature review by the UKCCIS evidence group*. Retrieved from http://eprints.lse.ac.uk/84956/1/Literature Review Final October 2017.pdf

Livingstone, S., Kirwil, L., Ponte, C., & Staksrud, E. (2013). *In their own words: What bothers children online?* Retrieved from www.eukidsonline.net

Luk R., Cohn R., Muth, H., Patil, A., Klauser, G., Lowney, S., Wallace, V., Janapa, R. C.-K., & Hazelwood, K. (2005). *Pin: Building customized program analysis tools with dynamic instrumentation*. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.598.4587&rep=rep1&type=pdf

Luo, W., Liu, J., Liu, J., & Fan, C. (2009). An analysis of security in social networks. *8th IEEE International Symposium on Dependable, Autonomic and Secure Computing, DASC 2009*, 648–651. https://doi.org/10.1109/DASC.2009.100

Magkos, E., Kleisiari, E., Chanias, P., & Giannakouris-salalidis, V. (2014). *Parental control and children ' s internet safety : The good , the bad and the ugly*. Retrieved from https://www.google.com/search?q=Parental+Control+and+Children+'+s+Internet+Safety+%3A+The+Good+%2C+the+Bad+and+the+Ugly.+1–18.&oq=Parental+Control+and+Children+'+s+Internet+Safety %3A+The+Good+%2C+the+Bad+and+the+Ugly.+1–18.&aqs=chrome..69i57.1488j0j7&sou

Maoneke, P. B., Shava, D. F. B., Gamundani, A. M., Bere-Chitauro, M., & Nhamu, I. (2018). ICTs use and cyberspace risks faced by adolescents in Namibia. *ACM International Conference Proceeding Series*, 109–117. Retrieved from https://doi.org/10.1145/3283458.3283483

Martínez-mesa, J., & González-chica, D. A. (2016). *Special article sampling : How to select participants in my research study ?* 326–330. Retrieved from https://www.scielo.br/pdf/abd/v91n3/0365-0596-abd-91-03-0326.pdf

Mascheroni, G., & Ólafsson, K. (2013). *Mobile internet access and use among European children.*

Initial findings of the Net Children Go Mobile project. Retrieved from www.netchildrengomobile.eu

McAfee. (2013). *Digital deception: The online behaviour of teens*. Retrieved from http://boletines.prisadigital.com/rp_digital_deception_survey.pdf

McLeod Saul. (2018). B.F. Skinner: Operant conditioning. *Simply Psychology*, (1948), 1–12. Retrieved from https://s3.amazonaws.com/academia.edu.documents/44186702/Skinner.pdf?response-content-disposition=inline%3B filename%3DSkinner_-_Operant_Conditioning.pdf&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIWOWYYGZ2Y53UL3A%2F20190721%2Fus-east-1%2Fs3%2F

Melnikovas, A. (2018). Towards an explicit research methodology: Adapting research onion model for futures studies. *Journal of Futures Studies*, *23*(2), 29–44. https://doi.org/10.6531/JFS.201812_23(2).0003

Mishna, F., Cook, C., Saini, M., Wu, M. J., & MacFadden, R. (2011). *Interventions to prevent and reduce cyber abuse of youth: A systematic review.* Retrieved from https://doi.org/10.1177/1049731509351988

Muskat, M., Blackman, D., & Muskat, B. (2012). Mixed methods: Combining expert interviews, cross-impact analysis and scenario development. *Electronic Journal of Business Research Methods*, *10*(1), 9–21. Retrieved from https://doi.org/http://dx.doi.org/10.2139/ssrn.2202179

Nabavi, R. T. (2014). *Theories of developmental psychology : Bandura's social learning theory & social cognitive learning theory*. Retrieved from https://www.researchgate.net/publication/267750204_Bandura's_Social_Learning_Theory_Social_Cognitive_Learning_Theory

Nakerekanti, M., & Narasimha, V. B. (2019). Analysis on malware issues in online social networking sites (SNS). *2019 5th International Conference on Advanced Computing &*

Communication Systems (ICACCS), 335–338. https://doi.org/10.1109/ICACCS.2019.8728536

Nalinipriya, G., & Asswini, M. (2016). A survey on vulnerable attacks in online social networks. *Proceedings 2015 - IEEE International Conference on Innovation, Information in Computing Technologies, ICIICT 2015*, 1–6. https://doi.org/10.1109/ICIICT.2015.7396102

Nanny, N. (2002). *User guide for windows*. Retrieved from https://www.netnanny.com/assets/documentation/nn/nn7_guide.pdf

Nashuuta, L. (2018). *Namibia a safe haven for cybercriminals* . Retrieved from https://neweralive.na/posts/namibia-a-safe-haven-for-cybercriminals

Nuha, N., Molok, A., Chang, S., & Ahmad, A. (2010). *Information leakage through online social networking: Opening the doorway for advanced persistence threats*. Retrieved from https://doi.org/10.4225/75/57b673cf34781

OECD. (2012). The protection of children online. *OECD Council Recommendation*, 161–165. https://doi.org/10.1002/1099-0852(200005/06)9:3<161::AID-CAR629>3.0.CO;2-I

Ojose, B. (2008). *Applying Piaget 's theory of cognitive development to mathematics instruction*. Retrieved from https://files.eric.ed.gov/fulltext/EJ841568.pdf

Okoye, K., Tawil, A. R. H., Naeem, U., Bashroush, R., & Lamine, E. (2014). A semantic rule-based approach supported by process mining for personalised adaptive learning. *Procedia Computer Science*, *37*, 203–210. https://doi.org/10.1016/j.procs.2014.08.031

Olivier, F. (2018). *Cybercrime in Namibia*. Retrieved from https://www.namibian.com.na/165301/archive-read/Cybercrime-in-Namibia

Pather, S., & Remenyi, D. (2005). Some of the philosophical issues underpinning research in information systems: from positivism to critical realism. *Annual Research Conference of the South African Institute of Computer Scientists and Information Technologists on IT Research in Developing Countries*, (January 2019), 141–146. Retrieved from https://dl.acm.org/doi/10.5555/1035053.1035070

Peffers, K., Tuunanen, T., & Rothenberger, M. A. (2020). *A design science research methodology for information systems research*. Retrieved from https://doi.org/10.2753/MIS0742-1222240302

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of Management Information Systems*. Retrieved from http://www.tuunanen.fi.

Peker, Y. K., Ray, L., Silva, S. Da, & Gibson, N. (2016). *Raising cybersecurity awareness among college students*. Retrieved from https://cisse.info/journal/index.php/cisse/article/view/55

Penna, L., Clark, A., & Mohay, G. (2005). Challenges of automating the detection of paedophile activity on the internet. *Proceedings - First International Workshop on Systematic Approaches to Digital Forensic Engineering*. https://doi.org/10.1109/SADFE.2005.4

Peters, A., & Winschiers-Theophilus, H. (2017). HCI out of Namibia. *Interactions*, *24*(4), 85–85. https://doi.org/10.1145/3099120

Phyfer, J., Burton, P., & Leoschut, L. (2016). *Global kids online South Africa: Barriers, opportunities and risks: A glimpse into South African children's internet use and online activities Monograph.* Retrieved from www.cjcp.org.za

Picciano, A. G. (2017). Theories and frameworks for online education: Seeking an integrated model. *Online Learning Journal*, *21*(3), 166–190. https://doi.org/10.24059/olj.v21i3.1225

Plano Clark, V. L. (2017). Mixed methods research. *The Journal of Positive Psychology*, *12*(3), 305–306. https://doi.org/10.1080/17439760.2016.1262619

Ramos-Soler, I., López-Sánchez, C., & Torrecillas-Lacave, T. (2018). Online risk perception in young people and its effects on digital behaviour. *Comunicar*, *26*(56), 71–79. https://doi.org/10.3916/c56-2018-07

Razaque Chhachhar, A., Qureshi, B., Ahmed Maher, Z., & Ahmed, S. (2014). Influence of Internet websites on children study. *Journal of American Science J Am Sci*, *1010*(55), 40–45. Retrieved

from https://www.academia.edu/8488333/Influence_of_Internet_Websites_on_Children_Study

Rozanski, E. P., & Haake, A. R. (2003). *The many facets of HCI*. Retrieved from https://dl.acm.org/doi/10.1145/947121.947162

Rubenking, N. J., & Minor, J. (2016). *Mobicip (for Android) Review | PCMag*. Retrieved from https://www.pcmag.com/reviews/mobicip-for-android

Rubenking, N. J., & Moore, B. (2019). *Norton family premier review | PCMag.* Retrieved from https://www.pcmag.com/reviews/norton-family-premier

Rubenking, N. J., & Moore, B. (2020a). *Kaspersky safe kids review | PCMa*g. Retrieved from https://www.pcmag.com/reviews/kaspersky-safe-kids

Rubenking, N. J., & Moore, B. (2020b). *Qustodio review | PCMa*g. Retrieved from https://www.pcmag.com/reviews/qustodio

Sadeghian, A., Zamani, M., & Shanmugam, B. (2013). Security threats in online social networks. *2013 International Conference on Informatics and Creative Multimedia*, 254–258. https://doi.org/10.1109/ICICM.2013.50

Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behaviour formation in organizations. *Computers and Security*, *53*(June), 65–78. https://doi.org/10.1016/j.cose.2015.05.012

Sălceanu, C. (2014). ScienceDirect-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/3.0/). Selection and peer-review under responsibility of the Organizing Committee of The Influence of Computer Games on Children's Development. Exploratory study on the attitudes of parents. *Procedia-Social and Behavioral Sciences*, *149*, 837–841. https://doi.org/10.1016/j.sbspro.2014.08.323

Sanord. (2016). *Framework for addressing child online protection issues in namibia: Societal*

governance. Retrieved from *https://sanord.uwc.ac.za/media/publications/*

Santisarun, P., & Boonkrong, S. (2015). Social network monitoring application for parents with children under thirteen. *2015 7th International Conference on Knowledge and Smart Technology (KST)*, 75–80. https://doi.org/10.1109/KST.2015.7051456

Saunders, M., Lewis, P., & Thornhill, A. (2019). *Chapter 4: Understanding research philosophy and approaches to theory development.* Retrieved from https://www.researchgate.net/publication/330760964_Research_Methods_for_Business_Students_Chapter_4_Understanding_research_philosophy_and_approaches_to_theory_development

Saunders, M. (2009). *Understanding research philosophies and approaches*. Retrieved from https://www.researchgate.net/publication/309102603_Understanding_research_philosophies_and_approaches

Scholefield, S., & Shepherd, L. A. (2019). *Gamification techniques for raising cyber security awareness*. Retrieved from https://www.researchgate.net/publication/331916014_Gamification_Techniques_for_Raising_Cyber_Security_Awareness

Shannon-baker, P. (2016). *Making paradigms meaningful in mixed methods research*. Retrieved from https://doi.org/10.1177/1558689815575861

Sharma, S., & Advisor, S. (2016). *ITU initiatives on child online protection (COP).* Retrieved from https://www.itu.int/en/ITU-D/Regional-Presence/CIS/Documents/Events/2016/06_Odessa/5_Sharma.pdf

Sharpe, H., Rogers, Y., & Preece, J. (2019). *Interaction design*. Retrieved from http://prof.mau.ac.ir/images/Uploaded_files/Jenny Preece, Helen Sharp, Yvonne Rogers-Interaction Design_ Beyond Human-Computer Interaction-Wiley (2015)[369707].PDF

Shi, C., Fu, S., Chen, Q., & Qu, H. (2015). VisMOOC: Visualizing video clickstream data from Massive Open Online Courses. *IEEE Pacific Visualization Symposium*. Retrieved from https://doi.org/10.1109/PACIFICVIS.2015.7156373

Smailovic, V., & Podobnik, V. (2016). Mining social networks for calculation of smartsocial influence. *Journal of Universal Computer Science*, *22*(3), 394–415. https://doi.org/10.3217/jucs-022-03-0394

Sonia L. P., Davidson, J.L., Saqba B. W., Haughton, C., & Nandi, A. (2017). *Children's online activities, risks and safety: A literature review by the UKCCIS evidence group*. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/759005/Literature_Review_Final_October_2017.pdf

Soumya, T. R., & Revathy, S. (2018). Survey on threats in online social media. *Proceedings of the 2018 IEEE International Conference on Communication and Signal Processing, ICCSP 2018*, 77–81. https://doi.org/10.1109/ICCSP.2018.8524200

Sundaresan, N. (2018). *Overview of cyber security*. Retrieved from https://doi.org/10.17148/IJARCCE.2018.71127

Tarun. (2017). Impact of social media on pharmaceutical manufacturer. *Global Journal of Enterprise Information System*, *8*(4), 47. https://doi.org/10.18311/gjeis/2016/15773

Tennakoon, H., Saridakis, G., & Mohammed, A.-M. (2018). *Child online safety and parental intervention: a study of Sri Lankan internet users*. Retrieved from https://doi.org/10.1108/ITP-09-2016-0213

The International Telecommunication Union (ITU). (2009). *Guidelines for parents , guardians and educators on child online protection*. Retrieved from https://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-COP.EDUC-1-2009-PDF-E.pdf

The International Telecommunication Union (ITU). (2015). *Guidelines for Industry on Child Online Protection*. Retrieved from https://doi.org/322

Thom, B. (2011). *Safechat: Using open source software to protect minors from Internet predation*. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.303.6288&rep=rep1&type=pdf

Tory, M., & Moller, T. (2016). *Evaluating visualizations: Do expert reviews work ?* Retrieved from https://doi.org/10.1109/MCG.2005.102

Trivedi, S. D., Dave, D., & Sridaran, R. (2016). Analysis and impact of cyber threats on online social networks. *Proceedings of the 10th INDIACom; 2016 3rd International Conference on Computing for Sustainable Global Development, INDIACom 2016*, 3548–3553. Retrieved from https://ieeexplore.ieee.org/abstract/document/7724923

U.S Department of Homeland Security. (2018). *U.S . DEPARTMENT OF HOMELAND SECURITY CYBERSECURITY STRATEGY*. Retrieved from https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf

Uher, J. (2016). What is behaviour? and (when) is language behaviour? A metatheoretical definition. *Journal for the Theory of Social Behaviour*, *46*(4), 475–501. https://doi.org/10.1111/jtsb.12104

United Nations Children's Fund. (2012). *Child safety online global challenges and strategies technical report*. Retrieved from www.unicef-irc.org

Vaishnavi, V., & Kuechler, B. (2013). *Overview of design science research*. Retrieved from https://doi.org/10.1155/2012/651507

Vieira, A. (2015). *Predicting online user behaviour using deep learning algorithms*. Retrieved from http://arxiv.org/abs/1511.06247

Walliman, N. (2010). *Research methods: The basics.* Retrieved from https://doi.org/10.4324/9780203836071

Walsh, C. (2020a). *2020 Kidsguard pro review: Is it the best cell phone monitoring app*. Retrieved from https://www.clevguard.com/reviews/kidsguard-pro-review/

Walsh, C. (2020b). Net nanny review: Pros, cons and similar parental control apps. Retrieved from https://www.clevguard.com/reviews/net-nanny-review/

Wang, Y. (2015). Privacy threat modeling framework for online social networks. *2015 International Conference on Collaboration Technologies and Systems (CTS)*, 358–363. https://doi.org/10.1109/CTS.2015.7210449

Weir, G. R. S., Toolan, F., & Smeed, D. (2011). The threats of social networking: Old wine in new bottles? *Information Security Technical Report*, *16*(2), 38–43. https://doi.org/10.1016/j.istr.2011.09.008

Whiting, G. (2020). *The limitations of McAfee | Small business - Chron.com*. Retrieved from https://smallbusiness.chron.com/limitations-mcafee-71573.html

Wilson, M., Hash, J., & Division, C. S. (2003). *Building an Information*. Retrieved from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-50.pdf

Yadav, M. P. (2012). *An efficient web mining Algorithm for web log analysis : E-Web miner*. Retrieved from https://ieeexplore.ieee.org/document/6194598

Yasseen Mahdi, A. (2013). Algorithm and flow chart. Retrieved from http://qu.edu.iq/el/pluginfile.php/112115/mod_resource/content/1/Algorithm-and-Flow-Chart.pdf

Zorrilla, M. E., & Alvarez, E. (2008). MATEP: Monitoring and analysis tool for e-learning platforms. *Proceedings - The 8th IEEE International Conference on Advanced Learning Technologies, ICALT 2008*. https://doi.org/10.1109/ICALT.2008.33

Zucule De Barros, M. J., & Lazarek, H. (2018). *A cyber safety model for schools in Mozambique*. Retrieved from https://doi.org/10.5220/0006573802510258

List of Appendices

Title	Description
Appendix A	Higher degree Committee (HDC) and Faculty Postgraduate Committee Approval Letter
Appendix B	Ministry of Education Permission Letter
Appendix C	Ministry of Education Approval Letter
Appendix D	Schools Permission Letter
Appendix E	Parental Consent Letters
Appendix F	Questionnaires
Appendix G	Expert Review evaluation form
Appendix H	COSBIA Game Concept
Appendix I	COSBIA Game evaluation criteria
Appendix J	Publications
Appendix K	Editor's report

Appendix A: Faculty Postgraduate Committee Ethical Approval Letter

NAMIBIA UNIVERSITY
OF SCIENCE AND TECHNOLOGY

FACULTY RESEARCH ETHICS COMMITTEE (F-REC)

DECISION/FEEDBACK ON RESEARCH PROPOSAL

Dear Ms: Jennyphar Kahlmise

Research Topic: **Designing an algorithm that will influence children's behaviour online and raise their cyber security awareness**

Supervisor (if applicable): **Dr Fungai Bhunu Shava**

Qualification registered for (if applicable): **MASTER OF COMPUTER SCIENCE**

(Reference number of application: **FACULTY RESEARCH ETHICS COMMITTEE REGISTRATION NUMBER: 02/2019)**

Re: Ethical screening application No: **F-REC-02/2019**

The Faculty of **Computing and Informatics** Ethics Screening Committee of the Namibia University of Science and Technology reviewed your application for the above-mentioned research. The research as set out in the application has been:

Approved	X

(indicate with an X, and N/A if not applicable and procced)

We would like to point out that you, as researcher, are obliged to maintain the ethical integrity of your research, adhere to the ethical guidelines of NUST, and remain within the scope of your research proposal and supporting evidence as submitted to the F-REC. Should any aspect of your research change from the information as presented to the F-REC, which could have an effect on the possibility of harm to any research subject, you are under the obligation to report it immediately to your supervisor or F-REC as applicable in writing. Should there be any uncertainty in this regard, you have to consult with the F-REC.

We wish you success with your research, and trust that it will make a positive contribution to the quest for knowledge at NUST.

Any ethical issues that need to be highlighted?	Why are these issues important?	What must/could be done to minimise the ethical risk?
No	N/A	N/A

Recommendation: The application is approved: Recommendations of FCI/F-REC, communicated to you on the 2019, were addressed to the satisfaction of the Chairperson.

Sincerely,

Dr Fungai BHUNU SHAVA

Chair: Faculty Ethics Screening Committee

Tel: +264-61-207-2510

CC: None,

NAMIBIA UNIVERSITY OF SCIENCE AND TECHNOLOGY
Private Bag 13388 Windhoek NAMIBIA
2019 -02- 15
OFFICE OF THE DEAN
FACULTY OF COMPUTING AND INFORMATICS

Appendix B: Ministry of Education Permission Letter

NAMIBIA UNIVERSITY
OF SCIENCE AND TECHNOLOGY
Faculty of Computing and Informatics
Department of Computer Sciences

13 Jackson Kaujeua Street
Private Bag 13388
Windhoek
NAMIBIA

T: +264 61 207 2052
F: +264 61 207 9258
E: dcs@nust.na
W: www.nust.na

Mr. Gerard Vries
The Director of Education for Khomas Region
Ministry of Education, Arts and Culture
Private Bag 13186 Windhoek
Government Office Park (Luther Street),
Windhoek

25 June 2019

Dear Sir,

RE: SEEKING PERMISSION TO COLLECT CHILD ONLINE PROTECTION (COP) INFORMATION DATA FROM LEARNERS THROUGH QUETIONNAIRES AS WELL AS THROUGH A GAME TO EVALUATE THE RESULTING INTERVENTION IN PRIMARY AND SECONDARY SCHOOL WITHIN THE KHOMAS REGION

My name is Jennyphar Kahimise and I am a Master of Computer Science student (student number: 212064053) at the Namibia University of Science and Technology (NUST) under the supervision of Dr Fungai Bhunu Shava. This course is research based and the research I wish to conduct for my Master's thesis is entitled, **"Designing an algorithm that will influence children's behaviour online and raise their cyber security awareness"**. I would like to ask you for permission to involve the Namibian learners in this research. The research will involve the learners completing a survey and this survey is designed to collect basic information on children's online activities and behaviour that expose them to cybercrimes. The results will be used as the basis to design an algorithm that will influence children's behaviour online and raise their cyber security awareness through game play. We will target learner's age 13 – 17 year olds. The number of learners target is at least 60 and this will involve Five (5) of the following schools:

a) Windhoek Technical High School
b) Orban Primary School
c) Highline Secondary School
d) St Joseph's RC High School
e) Eldorado High School

Information about the Research

The main objective is to design an algorithm that will influence children's behaviour online in order to reduce cyber security risk.

The proposed sub objectives are:

- Evaluate online activities that expose children's interaction with strangers.
- Analyze how children behave online.
- Design a behaviour influencing algorithm suitable for the security of children online activities.
- Evaluate behaviour influencing tools suitable for child online activities.

Data collection Process

Data collection procedure will carefully follow to authorization given in the research consent form.

Participation and Confidentiality

For the research participants to make a free and informed consent they will be provided with a full detailed of the research study to ensure their right of self-determination and autonomy. Parental consent will be sought as minors will be involved in the study. In addition, research participants will be provided with full information on what the research is about, its purpose, how long the study will take, research procedures and the expected benefits of the research study.

Participants have the right to refuse or withdraw any time from taking the survey or partaking in the experimental study. You do not have to take part in this study if you do not wish to do so. Your school performance will not be evaluated or affected in any way. All data collected from this study will be kept confidential. No personal information will be collected and the data will be recorded generically, where need be a pseudo identifier will be used. Please note that any information gathered up to the point of withdrawal might be utilized inside the study. The research will be administered consistently by the researcher.

The findings from this study will be shared more broadly through thesis publications and conferences. The resulting game which will be designed to test the algorithm will be brought to the learners to play and evaluate.

Further Questions and Contact Details

For more information or for any questions about the research, please do not hesitate to contact me or my supervisor. Details are as follows:

a) Dr Fungai Bhunu Shava
   Senior Lecturer: Namibia University of Science and Technology
   Faculty of Computing and Informatics
   Department of Computer Science
   Email: fbshava@nust.na

b) Jennyphar Kahimise
   Student: Namibia University of Science and Technology
   Department of Computer Science
   Windhoek; Namibia
   Cell number: +264 81 2347785
   Email: kjennyphar@yahoo.com

Appendix C: Ministry of Education Approval Letter

REPUBLIC OF NAMIBIA

MINISTRY OF EDUCATION, ARTS AND CULTURE

Tel: +264 61 -2933202
Fax: +264 61- 2932922
Enquiries: G. Munene
Email: Gilson.munene@moe.gov.na

Luther Street, Govt. Office Park
Private Bag 13186
Windhoek
Namibia

File no: 11/1/1

Ms Jennyphar Kahimise
Private Bag 13388
Windhoek
Email:kjennyphar@gmail.com
Cell: 081 234 7785

Dear Ms Kahimise,

SUBJECT: PERMISSION TO CONDUCT RESEARCH IN KHOMAS REGION

Kindly be informed that permission to conduct an academic research for your Master's Degree in Educational Foundations and Management in *"Designing an Algorithm that will Influence Children's Behaviour Online and Raise their Cyber Security Awareness in the Khomas Region in Namibia,"* is here with granted. You are requested to present this letter of approval to the Regional Director to ensure that research ethics are adhered to and disruption of curriculum delivery is avoided.

Furthermore, we humbly request you to share your research findings with the Ministry. You may contact Mr G. Munene at the Directorate: Programmes and Quality Assurance (PQA) for submission of a summary of your research findings.

I wish you the best in conducting your research and I look forward to hearing from you upon completion of your study.

Sincerely yours

SANET L. STEENKAMP
EXECUTIVE DIRECTOR

All official correspondences must be addressed to the Executive Director.

Appendix D: Schools Permission Letter

NAMIBIA UNIVERSITY
OF SCIENCE AND TECHNOLOGY
Faculty of Computing and Informatics
Department of Computer Sciences

13 Jackson Kaujeua Street
Private Bag 13388
Windhoek
NAMIBIA

T: +264 61 207 2052
F: +264 61 207 9258
E: dcs@nust.na
W: www.nust.na

Mrs Mahua-Masule
The Principal
St. Joseph's R.C School Dobra
P.O Box 2115
Windhoek.

18 July 2019

Dear Sir,

RE: SEEKING PERMISSION TO COLLECT CHILD ONLINE PROTECTION (COP) INFORMATION DATA FROM LEARNERS THROUGH QUETIONNAIRES AS WELL AS THROUGH A GAME TO EVALUATE THE RESULTING INTERVENTION IN PRIMARY AND SECONDARY SCHOOL WITHIN THE KHOMAS REGION

My name is Jennyphar Kahimise and I am a Master of Computer Science student (student number: 212064053) at the Namibia University of Science and Technology (NUST) under the supervision of Dr Fungai Bhunu Shava. This course is research based and the research I wish to conduct for my Master's thesis is entitled, **"Designing an algorithm that will influence children's behaviour online and raise their cyber security awareness"**. I would like to ask you for permission to involve the Namibian learners in this research. The research will involve the learners completing a survey and this survey is designed to collect basic information on children's online activities and behaviour that expose them to cybercrimes. We have applied and received permission from the Ministry of Education which is also attached here. The results will be used as the basis to design an algorithm that will influence children's behaviour online and raise their cyber security awareness through game play. We target to involve 12 learners aged 13 – 17 from your school. Attached also is a letter of consent to the parents/guardian/caregiver of the child as well as the permission letter from the Ministry of Education and Culture.

Information about the Research

The main objective is to design a behaviour influencing algorithm suitable for the security of children's online activities.

The proposed sub objectives are:

- Evaluate online activities that expose children's interaction with strangers.
- Analyse how children behave online.
- Design a behaviour influencing algorithm suitable for the security of children online activities.
- Evaluate behaviour influencing tools suitable for child online activities.

Data collection Process

Data collection procedure will carefully follow to authorization given in the research consent form.

Participation and Confidentiality

For the research participants to make a free and informed consent they will be provided with a full detailed of the research study to ensure their right of self-determination and autonomy. Parental consent will be sought as minors will be involved in the study. In addition, research participants will be provided with full information on what the research is about, its purpose, how long the study will take, research procedures and the expected benefits of the research study.

Participants have the right to refuse or withdraw any time from taking the survey or partaking in the experimental study. You do not have to take part in this study if you do not wish to do so. Your school performance will not be evaluated or affected in any way. All data collected from this study will be kept confidential. No personal information will be collected and the data will be recorded generically, where need be a pseudo identifier will be used. Please note that any information gathered up to the point of withdrawal might be utilized inside the study. The research will be administered consistently by the researcher.

The findings from this study will be shared more broadly through thesis publications and conferences. The resulting game which will be designed to test the algorithm will be brought to the learners to play and evaluate.

Further Questions and Contact Details

For more information or for any questions about the research, please do not hesitate to contact me or my supervisor. Details are as follows:

a) Dr Fungai Bhunu Shava
Senior Lecturer: Namibia University of Science and Technology
Faculty of Computing and Informatics
Department of Computer Science
Email: fbshava@nust.na

b) Jennyphar Kahimise
Student: Namibia University of Science and Technology
Department Computer Science
Windhoek; Namibia
Cell number: +264 81 2347785
Email: kjennyphar@yahoo.com

Appendix E: Parental Consent Letters

NAMIBIA UNIVERSITY
OF SCIENCE AND TECHNOLOGY
Faculty of Computing and Informatics
Department of Computer Sciences

13 Jackson Kaujeua Street
Private Bag 13388
Windhoek
NAMIBIA

T: +264 61 207 2052
F: +264 61 207 9258
E: dcs@nust.na
W: www.nust.na

Parental Consent Form

25 July 2019

Dear Parent/ Guardian/ Caregiver

RE: SEEKING CONSENT FOR YOUR CHILD TO FILL IN A QUESTIONNAIRE AS WELL AS PLAY A GAME TO EVALUATE THE RESULTING INTERVENTION AT SCHOOL.

Name: Jennyphar Kahimise
Institution: Namibia University of Science and Technology
Contact details: +264 812347785 **email address:** kjennyphar@yahoo.com

BRIEF DESCRIPTION OF THE PROJECT
This is a Masters research in Information Security research within the Computer Science Department in the Faculty of Computing and Informatics.

This informed Consent has two parts:
1. **Information Sheet (information about the study)**
2. **Certificate of Consent (for signatures if you choose to participate)**

Part 1: Information Sheet

Introduction:
My name is Jennyphar Kahimise and I am a Master of Computer Science student (student number: 212064053) at the Namibia University of Science and Technology (NUST) under the supervision of Dr Fungai Bhunu Shava. This course is research based and the research I wish to conduct for my Master's thesis is entitled, **"Designing an algorithm that will influence children's behaviour online and raise their cyber security awareness"**. The Internet provides amazing opportunities for children by enhancing their communication, social connection and technical skills. Nevertheless, it cannot solely guarantee a secure environment for them. Having no experience and knowledge, the behaviour of children potentially exposes them to cyber criminals as they innocently share information and befriend strangers.

We hereby ask your permission for your child to complete a survey being administered to learners in school. The survey will ask questions about children's online activities and behaviours that expose them to cybercriminals. It is our hope that data from this survey will contribute to a better understanding of how children behave online in order to design an algorithm that will influence their behaviour online and raise their cyber security awareness.

You may have time to think about partaking, talk to anyone you feel comfortable with about the research before making your decision. This consent form may contain words that you might not understand, please feel free to contact researcher as you are going through the questions.

Purpose of the research

gathered up to the point of withdrawal might be utilized inside the study. The research will be administered consistently by the researcher.

Sharing the Results
The findings from this study will be shared more broadly through thesis publications and conferences. The resulting game which will be designed to test the algorithm will be brought to the learners to play and evaluate.

Right to Refuse or Withdraw
Participants have the right to refuse or withdraw any time from taking the survey or partaking in the experiment. Your child does not have to take part in this study if you or they do not wish to do so. Your child's school performance will not be evaluated or affected in any way.

Period Duration: 25 June 2019- 25 October 2019

My contact details are indicated above for any information regarding this study.

Part 2: Certificate of Consent

CONSENT FORM

Title of Project: Designing an algorithm that will influence children's behaviour online and raise their cyber security awareness.

Please initial all boxes

1. I confirm that I have read and understood the information sheet provided for the above study. I have had the opportunity to consider the information, ask questions and have had these answered satisfactorily. ☐
2. I understand that my child's participation is voluntary and that I am free to withdraw them or they can choose not to participate at any time without giving any reason. ☐
3. I agree to have my child take part in the above study. ☐

Statement by the person taking consent

I confirm that I have accurately read out the information sheet to the potential participant, and to the best of my ability made sure that the participant understands that the following will be done:

1. Audio Recordings *2. Publication of participant's responses (in coded form).*

I confirm that the participant/ guardian was given an opportunity to ask questions about the study, and all the questions asked by the participant/ guardian have been answered correctly and to the best of my ability. I confirm that the individual has not been forced into giving consent, and the consent has been given freely and voluntarily.

A copy of this Informed Consent Form has been explained and provided to the participant.

Name of Participant	Date	Signature
Name of Parent/Guardian taking consent	Date	Signature

Appendix F: Questionnaires

NAMIBIA UNIVERSITY
OF SCIENCE AND TECHNOLOGY
Faculty of Computing and Informatics
Department of Computer Sciences

13 Jackson Kaujeua Street
Private Bag 13388
Windhoek
NAMIBIA

T: +264 61 207 2052
F: +264 61 207 9258
E: dcs@nust.na
W: www.nust.na

03 October 2019

Questionnaire No:

Dear Participant

Ref: Research Questionnaire

My name is Jennyphar Kahimise and I am a Master of Computer Science student (student number: 212064053) at the Namibia University of Science and Technology (NUST) under the supervision of Dr Fungai Bhunu Shava. The research I wish to conduct for my Master's thesis is entitled, **"Designing an algorithm that will influence children's behaviour online and raise their cyber security awareness"**. This survey is designed to collect basic information of children's online activities and behaviour that expose them to cybercrimes in Namibia. The results will be used as the basis to design an algorithm that will influence children's behaviour online and raise their cyber security awareness.

I am inviting you to participate in this research study by completing the attached questionnaires. It will require approximately 20-30 minutes completing. There is no compensation for responding nor is there any known risk. Participation in this study is completely voluntary and the respondents have the right to withdraw at any time without any negative consequences. Identities or personal details will not be disclosed to others and as such do not include your name. Any data used in the report will not be linked to any respondents. Please do not include your name.

Should you require any further information, please do not hesitate to contact me. My contact details are as follows:

Email: kjennyphar@gmail.com

Cellphone number: +264 81 2347785

Thank you for taking your time to assist me in my educational endeavor

Yours Sincerely,

Jennyphar Kahimise

Children's online activities and behaviour that expose them to cybercrimes in Namibia Survey

How to fill in the survey

a. Please read each question carefully and take your time to answer.
b. Answer simply by putting a tick in the boxes next to the answer you want to give.
c. Feel free to ask if you have any questions as you fill in the survey

Online behavior

1. What type of online platform do you mostly visit on a scale of 1-5, using the following scheme: 1=Never, 2=At least daily, 3=At least weekly, 4=At least monthly and 5= Almost all the time

	1 Never	2 At least daily	3 At least weekly	4 At least monthly	5 Almost all the time
Email (creating, accessing, attach file etc.)					
Social networking(e.g. Facebook, WhatsApp, Twitter, Instagram)					
Internet (browsing and searching for information)					
Communication-video and/or voice (e.g. Skype, YouTube)					
Games/Gaming					
Others (specify)					

2. To what extent do you use the Internet for the listed activities on a scale of 1-5, using the following scheme: 1=Never, 2=At least daily, 3=At least weekly, 4=At least monthly and 5= Almost all the time?

	1 Never	2 At least daily	3 At least weekly	4 At least monthly	5 Almost all the time
Search school work					
Play Internet games on your own or against a PC					
Watch videos clips					
Visit social networking					
Use instant					
Send/receive email					
Read/watch news online					
Play games with people on the Internet					
Download music					
Post photos, videos or music to share with others					
Use webcam					
Post messages on website					
Visit a chat room					
Use file sharing sites					
Spent time in a virtual world					
Write blogs					
Others (specify)					

3. Which of the following things do you know how to do on the Internet on a scale of 1-5, using the following scheme: 1= No Idea, 2=Poor, 3=Average, 4=Good and 5= Very Good

Things you know how to do on Internet	1 No idea	2 Poor	3 Average	4 Good	5 Excellent
Bookmark a website					
Block messages from someone you don't want to hear from					
Find information on how to use the Internet safely					
Change privacy settings on a social network sites					
Compare different websites to decide if information is true					
Delete the record of which sites you have visited					
Block unwanted adverts or junk mail/spam					
Change filter preference					

4. Which of these device do you use to access the Internet?

Device	Select device by a tick in the corresponding box	On AVERAGE, how much time in hours do you spend on the device per day.
Smart phone		
Personal Computer		
School Computer		
Laptop		
Tablet		
Others (specify)		

I do not use the Internet ☐

5. How true is this of you?

	Not true	Somehow true	Very true
I know more about the Internet than my parents			
I find it easier to be myself on the Internet then I am with people face-to-face			
I talk about different things on the Internet than when I am with people face-to-face?			
On the Internet I talk about private things which I do not share with people face-to-face?			

Online Activities

6. Where do you access the Internet from? Tick all the applicable

Place	Select place below
At school	
At home	
In an internet café	
In a public Library	
Others (specify)	

7. On which of these social networks are you active on a scale of 1-5, using the following scheme: 1=Never, 2=At least daily, 3=At least weekly, 4=At least monthly and 5= Almost all the time.

Social networks	1 Never	2 At least daily	3 At least weekly	4 At least monthly	5 Almost all the time
Facebook					
Facebook messenger					
WhatsApp					
Twitter					
Skype					
Viber					
Myspace					
Snapchat					
LinkedIn					
Games/Gaming					
Others (specify)					

8. What type of information have you share online with people you have never met in real life using the different platforms?

Online Platforms	Physical address	Age/ Birth date	Gender	Phone number	Your actual name	Details about your parents/family	Your School
Email (creating, accessing, attach file etc.)							
Social networking(e.g. Facebook, WhatsApp, Twitter, Instagram)							
Internet (browsing and searching for information)							
Communication-video and/or voice (e.g. Skype, YouTube)							
Games/Gaming							

9. What type of information have you share with strangers when doing the following activities on the Internet?

	Physical address	Age/birth date	Gender	Phone number	Your actual name	Details about your parents/family	Your school
Search school work							
Play Internet games on your own or against a PC							
Watch videos clips							
Visit social networking							
Use instant							
Send/receive email							
Read/watch news online							

Play games with people on the internet							
Download music							
Post photos, videos or music to share with others							
Use webcam							
Post messages on website							
Visit a chat room							
Use file sharing sites							
Spent time in a virtual world							
Write blogs							
Others (specify)							

10. Would you do or share the following while online? On a scale of 1-4, using the following scheme: 1=Never, 2=sometimes, 3= Often and 4= Always.

	1 Never	2 Sometimes	3 Always
Look for new friends or contacts on the internet.			
Send my personal information (e.g., my full name, address or phone number) to someone I have never met face-to-face.			
Add people to my friends or contacts I have never met face to face.			
Pretend to be a different kind of person online from who I really am.			
Send a photo or video of myself to someone I have never met face-to-face.			
Delete the record of which sites you have visited.			
Block unwanted adverts or junk mail/spam.			
Change filter preference.			

11. Do you feel compelled to the following? On a scale of 1-3, using the following scheme: 1=Never, 2=Sometimes, and 3= Always.

	1 Never	2 Sometimes	3 Always
To read and pay attention to friendly request of strangers before accepting?			
To be polite to strangers online?			
To understand the request presented to you by a stranger online?			
Take advantage of the weakness of other online friends?			
To please others on the internet?			

12. Have you ever experienced one or more of the following content-related risk? If yes, how did you feel about this experience on a scale of 1-5, using the following scheme: 1=No emotions, 2= Fear, 3=Disgust (e.g. gross, nasty, and offensive), 4=Annoyance (e.g. annoying, irritating) and 5= Positive reaction (e.g. exciting, curios, cool, and funny).

Content-related risk experience	Choice Yes or No	1 No emotions	2 Fear	3 Disgust	4 Annoyance	5 Positive reaction
Unwanted content in general						
Violent/aggressive content (e.g. violence, torture, killing)						
Gory content (e.g. blood, pain, etc.)						
Scary content						
Pornographic or sexual content (e.g. see naked people, etc.)						
Violent pornography (e.g. violation, rape)						
Commercial content (e.g. advertising to make money)						
Racist content						
Hateful content						
Content about drugs						
Content about self-harm or suicide or anorexia/ bulimia						
Content harmful to self-esteem (e.g. feel badly about our body)						
Others (specify content risk)						

13. Have you ever experienced one or more of the following contact-related risk (usually from strangers)? If yes, how did you feel about this experience on a scale of 1-5, using the following scheme: 1=No emotions, 2= Fear, 3=Disgust (e.g. gross, nasty, offensive), 4=Annoyance (e.g. annoying, irritating) and 5= Positive reaction (e.g. exciting, curios, cool, funny)

Contact-related risk experience	State Yes or No	1 No emotions	2 Fear	3 Disgust	4 Annoyed	5 Positive
Possibility of inappropriate contact in general from strangers						
Possibility of inappropriate sexual contact in general						
Actual or attempted inappropriate content in general						
Face-to-face meetings following online contact						
Ideological or religious or fundamentalist influence						
Other people accessing your data/ being tracked/ cookies						
People pretending to be someone else						
Others (specify contact risk)						

14. How you ever experienced one or more of the following conduct-related risk (usually from other young people or strangers)? If yes, how did you feel about this experience on a scale of 1-5, using the following scheme: 1=No emotions, 2= Fear, 3=Disgust (e.g. gross, nasty, offensive), 4=Annoyance (e.g. annoying, irritating) and 5= Positive reaction (e.g. exciting, curios, cool, funny)

Conduct-related risk experience	State	1	2 Fear	3 Disgust	4 Annoyed	5

	Yes or No	No emotions				Positive reaction
Unwelcome conduct in general (e.g. bad behaviour, swearing)						
Bulling (usually repeated aggression)						
Other mean or aggressive conduct (e.g. receiving nasty text)						
Sexual harassment or unwelcome 'sexting'						
Sharing images or photos						
Hacking or misuse of personal information or data						
People saying bad things about you/damage to your reputation						
Others (specify conduct risk)						

15. What other risk-related experience have you had? If any, how did you feel about this experience on a scale of 1-5, using the following scheme: 1=No emotions, 2= Fear, 3=Disgust (e.g. gross, nasty, offensive), 4=Annoyance (e.g. annoying, irritating) and 5= Positive reaction (e.g. exciting, curios, cool, funny)

Other-related risk experience	State Yes or No	1 No emotions	2 Fear	3 Disgust	4 Annoyed	5 Positive reaction
Gave out information to strangers						
Gambling						
Pop-ups (unspecified or commercial/marketing/advertising						
Spam, phishing, scams, fraud (e.g. fraudulent information)						
Illegal downloading						
Spending too much time online (e.g. missed homework, sleep)						
Health related risks (muscular, eye-sight, etc.)						
Lack of internet safety in general						
Related to hardware/software (e.g. breakdown, install, etc.)						
Related to search (e.g. hard to find information)						
Virus (e.g. sites that come with virus)						
Others (specify risk)						

16. What gender are you?

Gender	Select gender
Male	
Female	

Do you have any other comments, please note them below:

_____

_____

_____

Thank you for taking the time to answer the questionnaire.

Appendix G: Expert Review Evaluation Form

Child Online Secure Behaviour Influencing Algorithm (COSBIA) Evaluation

My name is Jennyphar Kahimise and I am a Master of Computer Science student (student number: 212064053) at the Namibia University of Science and Technology (NUST) under the supervision of Prof Fungai Bhunu Shava. The research I conducted for my Master's thesis is entitled, "Designing an algorithm that will influence children's behaviour online and raise their cybersecurity awareness".

I am inviting you to participate in this research study by completing the attached questionnaires. This questionnaire aims to evaluate the COSBIA, COSBIA is an algorithm designed to influence the behaviour of children between the ages of 13-17 years and raise their cybersecurity awareness. It will require approximately 20-30 minutes to complete. There is no compensation for responding nor is there any known risk. Participation in this study is completely voluntary and the respondents have the right to withdraw at any time without any negative consequences. Identities or personal details will not be disclosed to others and as such do not include your name. Any data used in the report will not be linked to any respondents. Please do not include your name

The collected information will be used to improve the design of the algorithms. The resulting algorithm will contribute to the body of knowledge and guidelines on influencing children's online behaviour and raising their cybersecurity awareness in Namibia. Your responses are crucial in informing the design of the algorithm.

All of your responses will be handled in a confidential manner; hence you are encouraged to give truthful answers. All the information gathered will only be used for the purposes of this thesis.
Should you require any further information, please do not hesitate to contact me. My contact details are as follows:
Email: kjennyphar@gmail.com
Cellphone number: +264 81 2347785

Thank you for taking the time to assist me in my educational endeavor

Yours Sincerely,

Jennyphar Kahimise

Demographic information.

This section aims to gather biographical information about you as the subject expert.

Please indicate the organisation you work for (Choose one) *

- ◯ Academia
- ◯ CRAN
- ◯ Children's Digital Rights
- ◯ ISOC
- ◯ NamPol
- ◯ Child Online Protection Officer
- ◯ UNICEF
- ◯ Office of the First Lady
- ◯ MICT
- ◯ Lifeline/Childline
- ◯ Telecommunications
- ◯ Prosecutor General
- ◯ MGECW
- ◯ Other: _____

Please indicate your role in your organization (Choose one) *

- ◯ Information Security Specialist
- ◯ Lecturer
- ◯ Master/PHD student
- ◯ Children's Digital Rights Specialist
- ◯ Social Worker
- ◯ Cyber Security specialist
- ◯ Child Online Protection Officer
- ◯ IT Specialist
- ◯ Other: _____

Please specify your working experience in this field (the one you chose above) in years * *

Your answer

Please indicate your level of Cyber security knowledge (choose one) * *

- ◯ Beginner
- ◯ Intermediate
- ◯ Advanced

Please indicate your level of understanding and experience on Child Online Protection (Choose one) *

- ◯ Beginner
- ◯ Intermediate
- ◯ Advanced

Back Next

Evaluation Questionnaire of the Proposed Algorithm COSBIA

Section A: COSBIA Overview
A detailed list of components and their subcomponents that are key to the algorithm design are presented in Table 1.

COSBIA Components. Please refer to Table 1 to respond to the question in Table 2, Table 3, and Table 4.

Table1: COSBIA Components

Set	Component	Sub-Set	Sub-components	Definition
SC	secure children online			A secure child who behaves securely online
		OB	Online Behaviours	Positive behaviour (PB), Negative behaviour (NB), Threatening behaviour (TB), Vulnerable behaviour (VB), Secure behaviour (SB), Online Gadget behaviour
		OE	Online Experiences	Positive online experience (POE), Negative online experience (NOE), Threatening online experience (TOE), Vulnerable online experience (VOE), Secure online experience (SOE), Happy online experience (HOE), Miserable online experience (MOE)
		K	Knowledge	Good Internet Security knowledge (GISK), Poor internet security knowledge (PISK), Online Platform Knowledge (OPK),Gadget Knowledge (GK), Online Activities knowledge (OAK), Prior knowledge (PK), New knowledge (NK), Developing Knowledge (DK)
		G	Gadgets- smart gadgets used to access the internet	Smart phone (SP), Ipad/Tablet (IP), Laptop (LP), Personal Computer (PC), School computer (SC), Game console (GC), Ipod (I)
		OP	Online platforms - used by children :	Chat (C), Tik Tok (TT), Facebook (FB), Whatsup (WA), Instagram (I), Hangouts (HO), Twitter (T), Skype (S), MySpace (MS), Snapchat (SC), LinkedIn (LI), Gaming (G)
		OA	Online activities - children love to perform online	Watching videos (WV), Gaming (G), Information search (IS), Studying (S), Social Networks (SN), Emailing (E)
		OT	Online threats -children are exposed to online:	General internet threats (GIT), OP specific threats (OPST), OA specific threats (OAST), G specific threats (GST), B specific threats (BST)
		E	Empowerment - is a set of interventions that will foster	Security knowledge (SK), Secure behaviour (SB), Secure experience (SE), Reduce exposure to online threats in the actors over time (RE)
		TSO	Time spend online	At least daily (LD), At least weekly (LW), At least monthly (LM), Almost all the time (AT)

A child uses the Internet to visit social networking platforms, search for information, plays games and to send or receive emails. Using their past experience and devices the child shares personal information, share emotions and feeling on their status, download music and post photos and videos on the Internet. Based on the particular online activities, online behaviours, prior knowledge, online platforms, online threats and online experience of a unique child, children's online interaction may lead to a secure experience or an insecure experience. Section B represents the first relationship which is the Child online experience.

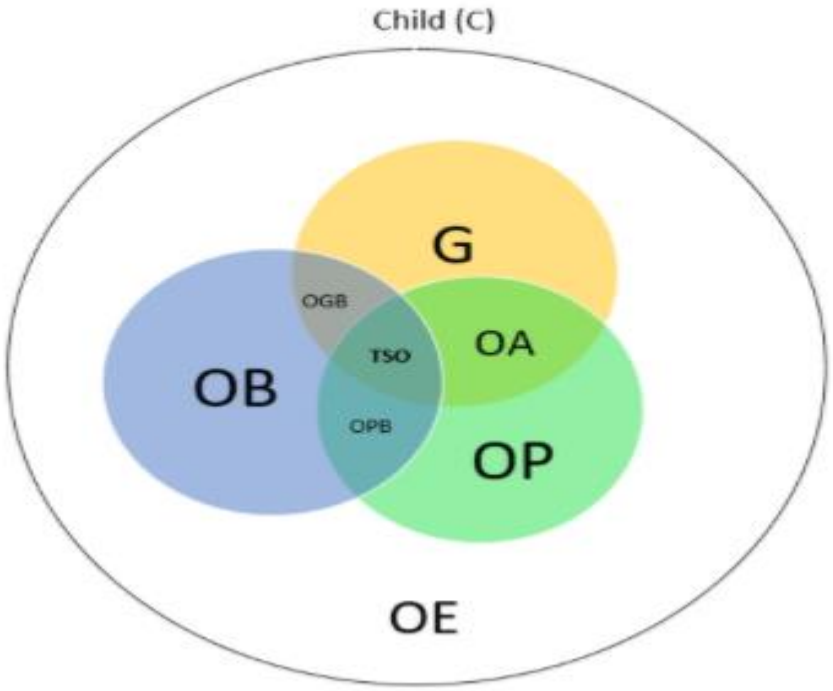
Section B: Child online experience

This section evaluates the first relationship depicted in Figure 1. This relationship of the algorithm demonstrates that a child (C) interacts with an Online Platform (OP) to perform Online Activities (OA) using a smart gadget (G). The Time Spent Online (TSO) and the child's Online Behaviour (OB) while performing OA on an OP using G results in a child's online experience (OE) which can either be secure or insecure. This is due to the fact that G has an influence on OB, which results in gadget specific behaviour (OGB) and OP has an influence on OB which results in platform specific behaviour (OPB). In set notation, OE(C) is a result of time spent online (TSO) over a set of G, OA, OP, OB.

Equation i, outlines that Children's online experience OE(C) is equal to the time spend online (TSO) multiple by the gadget they are using, the online activities they are performing, the specific online behaviour on the online platform and the way they are behaving using that specific gadget.

Equation i: $OE(C) = TSO*(G+OA+OP\ (OPB)\ +OB\ (OGB))$

Figure 1: Component Relationship 1



Please refer to Figure 1 to respond to the question in Table 2 by selecting the following scheme: 1=Strongly Agree, 2=Agree, 3= Neutral, 4=Disagree, and 5= Strongly Disagree. *

	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
The type of smart gadget used by children online have direct influence on their online experience	○	○	○	○	○
The type of online activities performed by children online have direct influence on their online experience	○	○	○	○	○
The type of online platform visited by children have direct influence to their online experience.	○	○	○	○	○
The type of online behaviour by children when using a specific gadget have	○	○	○	○	○

The time spend online by children using a gadget, performing online activities, visiting online platform and their online behaviour have direct influence to their online experience.	○	○	○	○	○
Children's online experience is equal to the time spend online using a gadget, the online activities they are performing, the specific online behaviour on the online platform and their online behaviour using that specific gadget.	○	○	○	○	○

Would you recommend any change to the child's online experience relationship in Figure 1? Please specify. *

Your answer

Back Next

Section C: Children's Secure Online Behaviour

This section evaluates the second relationship depicted in Figure 2. The child (C)'s prior knowledge (PK) and their online behaviour (OB) exposes them to online threats (OT) inherent in G, OA and OP; this results in a child's online experience (OE). If empowerment is added to this interaction, it would result in a secure online behaviour (SOB). We posit that a secure online experience (SOE) is a result of secure online behaviour this relationship. SOE (C) is a result of applying a set of E to enhance PK and OB of/with OA, OP, and G in the presence of OT.

Equation ii represents that Children's online behaviour OB is a summation of the type of online platform they are visiting, the type of gadget they are using, the types of online activities they are performing, their prior knowledge, the online threats posed to them and their online experience.

Equation ii: OB = OP+G+OA+PK+OT+OE

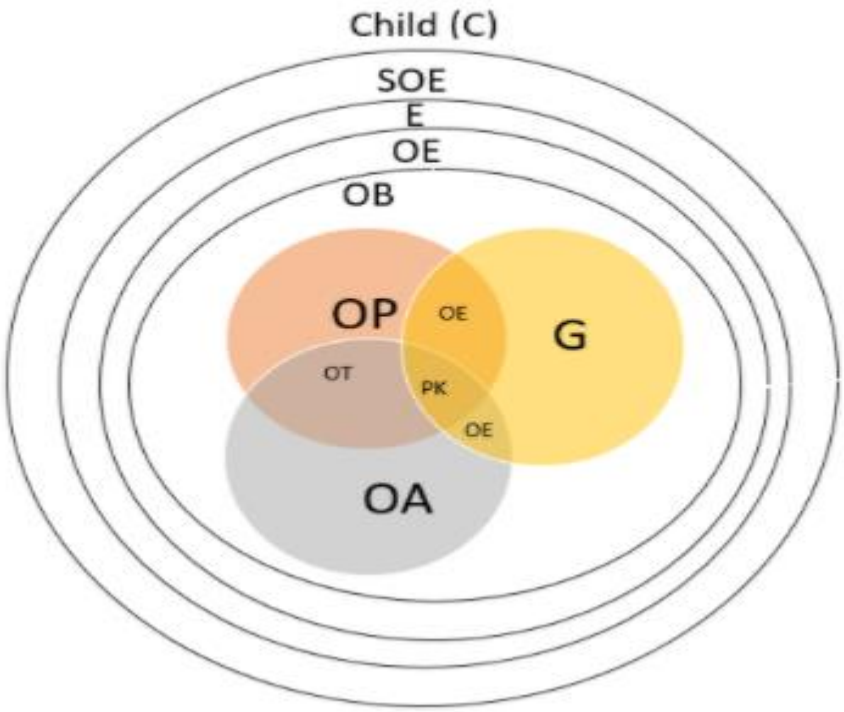
Equation iii represents that Children's online experience is a product of their online behaviour and the combination of the online platforms they are visiting, the gadget they are using, the online activities they are performing, their prior knowledge and the online threats posed to them.

Equation iii: OE= OB*(OP+G+OA+PK+OT)

Equation iv represents that Children's secure online behaviour is a summation of their online experience and Empowerment on the gadget, online activities, online platform and online behaviour. Where secure online behaviour equates to secure online experience.

Equation iv: SOB= OE+E*(G, OA, OP, OB)
SOB = SOE

Figure 2: Component Relationship 2



Please refer to Figure 2 to respond to the question in Table 3 by selecting the following scheme: 1=Strongly Agree, 2=Agree, 3= Neutral, 4=Disagree and 5= Strongly Disagree *

	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
Children's online behaviour (OB shown in equation ii) is a summation of the type of online platform they are visiting, the type of gadget they are using, the types of online activities they are performing, their prior knowledge, the online threats posed to them and their online experience. Equation ii: OB = OP+G+OA+PK+OT+OE	○	○	○	○	○
Children's online experience (OE shown in equation iii) is a product of their online behaviour and the combination of the online platforms they are visiting, the gadget they are using, the online activities they are performing, their prior knowledge and the online threats posed to them. Equation iii: OE= OB* (OP+G+OA+PK+OT)	○	○	○	○	○
Children's secure online behaviour (SOB shown in equation iv) is the summation of their online experience and Empowerment on the gadget, online activities, online platform and online behaviour. Where secure online behaviour equates to secure online experience. Equation iv: SOB= OE+E*(G, OA, OP, OB). SOB = SOE	○	○	○	○	○

Would you recommend any change to the child's secure online behaviour relationship in Figure 2? Please specify the required changes if any. *

Your answer

Back Next

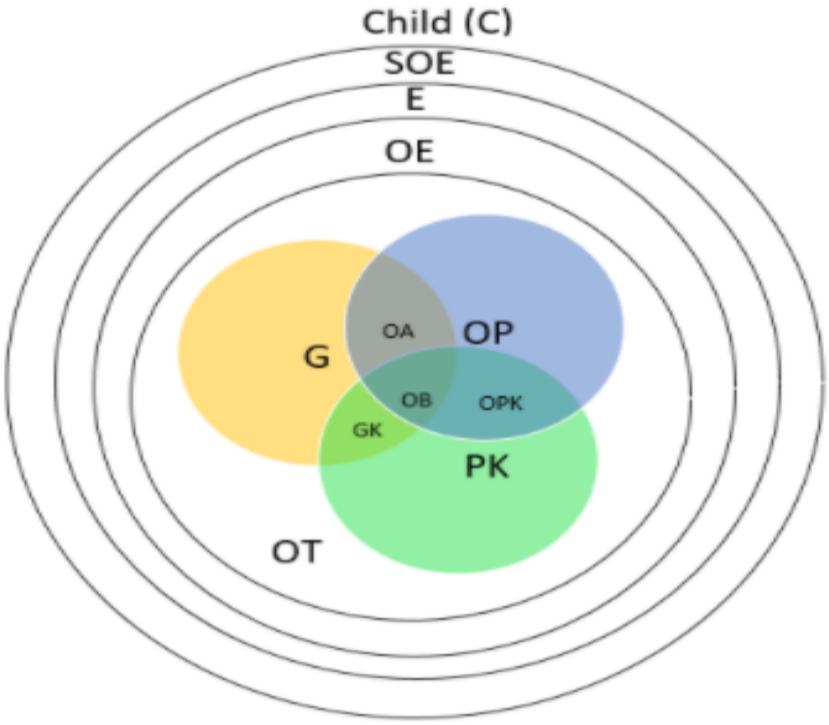
Section D: Children's Secure Online Experience

This section evaluates the third relationship depicted in Figure 3. A child (C) interacts with an Online Platform (OP) using a smart gadget (G) to perform Online Activities (OA). Adding prior knowledge while using the gadget (G) results in the gadget knowledge (GK). Adding prior knowledge (PK) while interacting on online platforms results in online platforms knowledge (OPK). When one adds prior knowledge to the gadget and online platform influence, online behaviour (OB) in the presents of online threats (OT). If empowerment is added then secure online experience (SOE), is the result.

Equation v: OE= OB *(G+OP+PK)*OT)

Equation vi: SOE= OE + E*(G+OP+PK+OT)

Figure 3: Component Relationship 3



Please refer to Figure 3 to respond to the questions in Table 4 by selecting the following scheme: 1=strongly Agree, 2=Agree, 3= Neutral, 4=Disagree, and 5= Strongly Disagree. *

	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
Children's online experience (OE shown in equation v) is a product of their online behaviour and a summation by the posed online threats on gadgets used, online platform visited and their prior knowledge. Equation v: OE= OB * (G+OP+PK)*OT)	◯	◯	◯	◯	◯
Children's secure online experience (SOE shown in equation iv) is the summation of their online experience and empowerment by the gadget they are using, online platform visited, heir prior knowledge and the online threats posed to them. Equation vi: SOE= OE + E*	◯	◯	◯	◯	◯
vi: SOE= OE + E* (G+OP+PK+OT)					

Would you recommend any change to the child's secure online experience relationship in Figure 3? Please specify. *

Your answer

In your opinion, select the extent to which you agree/disagree with the statements in Table 5 by selecting the following scheme: 1= Not at all true, 2=Slightly true, 3= Somewhat true, 4= Moderately true and 5=Extremely true. *

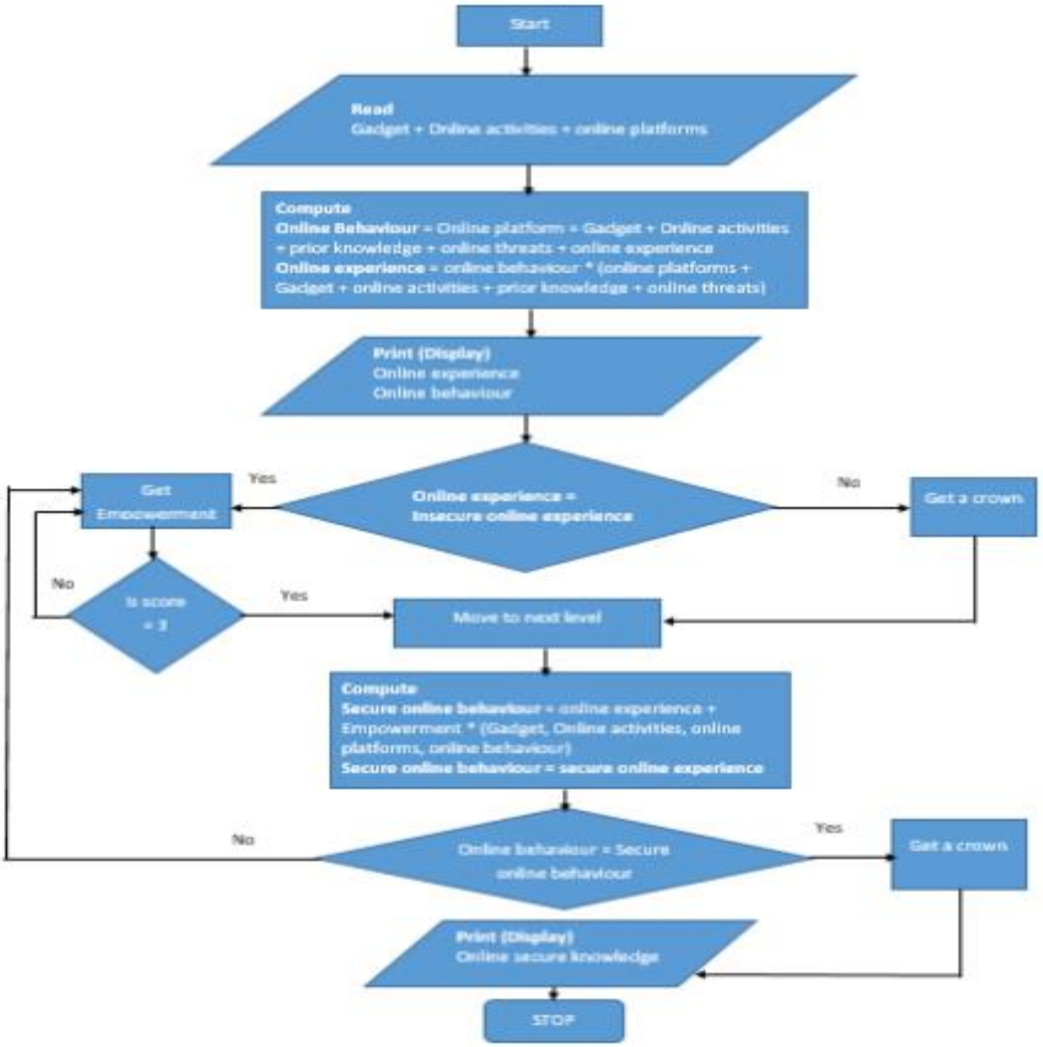
	Not at all true	Slightly true	Somewhat true	Moderately true	Extremely true
Smart gadget type have direct influence on the child's online behaviour.	◯	◯	◯	◯	◯
Time spend online by children reveal the extent of exposure to online threats.	◯	◯	◯	◯	◯
Online behaviour change with different online platforms.	◯	◯	◯	◯	◯
Different online platforms influence the level of children's online experience.	◯	◯	◯	◯	◯
Online activities change with different online platforms.	◯	◯	◯	◯	◯
Online threats can influence child's online behaviour.	◯	◯	◯	◯	◯

Online threats can influence a child's online experience.	○	○	○	○	○
Time spend online can influence child's online behaviour.	○	○	○	○	○
Online behaviour influences child's online experience.	○	○	○	○	○
Prior knowledge on online threats can influence child's online behaviour.	○	○	○	○	○
Secure online experience leads to secure online behaviour.	○	○	○	○	○
Secure online behaviour results in secure online experience.	○	○	○	○	○
Online experience plus empowerment leads to secure online experience.	○	○	○	○	○

Would you recommend any change (to add or remove) to the proposed algorithm? *

Your answer

Figure 4: COSBIA Flowchart



The overall algorithm flow is depicted in the flowchart in Figure 4, Please comment on the flowchart. *

Your answer

Thank you for taking the time to answer the questionnaire.

Back Submit

Appendix H: COSBIA Game Concept

COBSIA Game Concept

The COSBIA is an algorithm, designed to influence the behaviour of children between the ages of 13-17 years and raise their cyber security awareness. This section outline, the COSBIA concept that includes the story, player and player characteristic, challenges for the player, game environment, target player, progression and Principle gameplay mode.

Story

A child interacts with an online Platform to perform Online Activities using a smart gadget. The Time Spent Online and the child's Online Behaviour while performing online activities on an online platform using gadget results in a child's online experience, which can be either secure or insecure. This is due to the fact that gadgets has an influence on online behaviour, which results in gadget specific behaviour and online platforms has an influence on online behaviour which results in platform specific behaviour.

The child prior knowledge and their online behaviour exposes them to online threats inherent in gadgets, online activities and online platforms, this results in a child's online experience. If empowerment is added to this interaction, it would result in a secure online behaviour. We posit that a secure online experience is a result of secure online behaviour. The flowchart is presented in Figure 1.

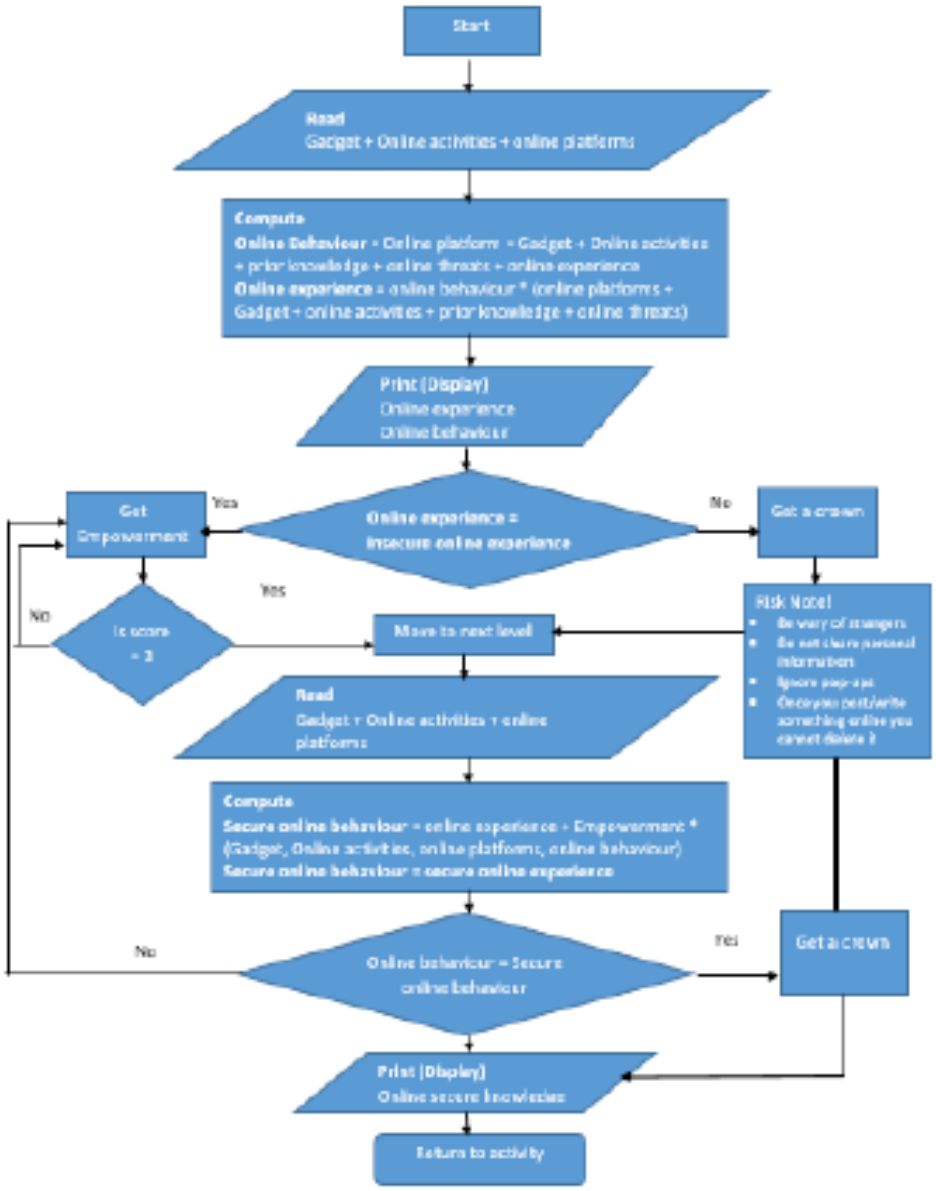


Figure 1: COSBIA flowchart

Below are the six equation for computing the different outputs in the algorithm:

Equation i: Online Experience (Child) = Time Spend Online *(Gadget + Online Activities + Online Platform (Online Platform Behaviour) + Online Behaviour (Online Gadget Behaviour))

Equation ii: Online Behaviour = Online Platform + Gadget + Online Activities + Prior Knowledge + Online Threats + Online Experience

Equation iii: Online Experience = Online Behaviour *(Online Platform + Gadget + Online Activities + Prior Knowledge + Online Threats)

Equation iv: Secure Online Behaviour = Online Experience + Empowerment *(Gadget, Online Activities, Online Platforms, Online Behaviour)
Secure Online Behaviour = Secure Online Experience

Equation v: Online Experience = Online Behaviour *(Gadget + Online Platforms + Prior Knowledge) *Online Threats)

Equation vi: Secure Online Experience = Online Experience + Empowerment *(Gadget + Online Platform + Prior Knowledge + Online Threats)

Player characteristics

A **child** is the main actor in the COSBIA, they:

- Interact with an online platform to perform online activities using a gadget.
- Spend time online and needs to be tracked
- Have an online Behaviour while on the different environment
- Have an online experience (secure or insecure)
- Should be empowered while on the different environment.

Challenges for the player

- Apply prior knowledge (for initial evaluation, a quiz on their prior knowledge of risks and security around their gadgets, platforms and activities)
- Exposed to online threats based on gadget or platform used or activity being performed
- Get empowerment if their security levels are lower than a score of three.
- Online behaviour should be secure to move to the next level (Level 1 to level 2 a score of 3 out of should be obtained, Level 2 to level 3 score of 3 should be obtained, Level 3 to exit back to activity a score of 3 should be obtained).
- Secure online experience attained through performing several empowerment activities.

Score

- **1-3 correct answers:** You are at the beginning of your journey to become a safe internet user and you start thinking about others online. However, you can do more! Always remember to ask an adult for support as soon as you need it, instead of trying to do it all by yourself or just go along with what others do. In addition, you should have a much better time on the internet.
- **4-6 correct answers:** You are on the way to becoming a safe internet user and a good friend to others. However, you can do more! Remember always to ask an adult for help as soon as you need it, instead of trying to do some things by yourself or being caught up in what others might do. That means you and your friends can enjoy the internet together safely.
- **7-9 correct answers:** You are well on the way to becoming a responsible internet user and a great online friend, and you are making some very sensible choices. It is always a good idea to ask for help from an adult if there is anything you are uncertain about, or if anything makes you feel worried or upset. In addition, you will get the most out of the internet and all the amazing stuff that it has to offer.
- **10 correct answers:** You are a friendly and caring internet user who does brilliantly online. You know how important it is to ask for support when you need it, to be healthy and to look after the feelings of your friends. Share your knowledge with as many friends as possible to help everyone around you stay safe and enjoy fantastic online time

Game environment

- **Online platforms:** Chat, Tik Tok, Facebook, WhatsApp, Instagram, Hangouts, Twitter, Skype, Myspace, Snapchat, LinkedIn, gaming
- **Gadget:** smart phone, IPad/Tablet, Laptop, Personal computer, school computer, game console, IPod
- **Online activities:** Watching Videos, Gaming, information search, studying, social networks, emailing

Quiz question

Online Threats	Quiz	Answers
General Internet Threats	1. One of your classmate has sent around an embarrassing photo of another classmate. What should you do with it?	A: You should show the photo to your teacher and tell them what has happened. Think of how you would feel if the picture have been of you.

	A. Show your teacher, and tell them what happened B. Forward the photo to others C. Save it on your phone, so that you can embarrass them later D. Laugh at the photo with your friends	
	2. One of your friends posted a video about you on the internet and you do not like it. You asked them to take it off but they said no, because it is funny. What is it that you should do? A. Keep asking your friend until they take it down B. Speak to an adult and say why you don't like it C. Leave it – you can't do anything else about it D. Post a video of them to get back at them	B: You should talk to an adult about what happened and tell them you do not like it. Then, they can try to take down the video.
	3. Your friend tells you she is talking to a boy/girl online and on the weekend, she/he will meet him/her. What should you do? A. Volunteer to go with her/him B. Let her/him go on her/him own C. Tell an adult straight away D. Tell your other friends	C: If someone is going to meet a person they met online, you must tell an adult right away. You should never meet strangers, unless you know for sure who they are.
	4. A classmate tells you someone on an online game was calling him/her mean names. What should you do? A. Tell your teacher or another adult B. Tell him/her to call the person mean names back C. Tell him/her to just ignore it and let it go away D. Tell him/her to stop playing games for a while	A: Calling anyone online means names is a cyberbullying act. You should inform an adult about this and you should not neglect it.
	5. Whom are you allowed to share your passwords with? A. Your friends B. Nobody – you should keep them to yourself C. Your family D. Your teacher	B: You should also keep your passwords to yourself. If your password falls in the wrong hands, it could be risky.
	6. You need to create a Website password. What should you use? A. Your full name (e.g. annamarie) B. Part of your name and a number (e.g. anna123) C. A random word, number and punctuation combination (e.g. 1vira8pm!) D. A nickname that your friends call you (e.g.annagirl)	C: The strongest passwords should include letters, numbers, and punctuation combinations. You should never use something that is connected to your name because it is very easy to guess.

	7. The Internet gives us access to many resources we would otherwise not be able to get in contact with. A. TRUE B. FALSE	A: That is probably the best thing about the Internet. It is giving us instant access to distant things, things locked away, that does not even exist yet. It is a travel agent, a guide to the museum and a play with friends from all over the world!
	8. Information on the Internet can always be trusted to be truthful. It would not be online if it were not true. A. TRUE B. FALSE	B: The Internet is an open forum for anyone and everyone. Bias is the rule rather than the exception. Evaluate carefully ALL information on websites, personal or public
Online Platform Specific Threats	1. What is the best way to use Facebook, Chat, TikTok, WhatApp, Instagram,Hangouts, Twitter and other social networking sites? A. Limit the amount of information I share about myself. B. Only talk to people I know. C. Make my page private, except to the people I have as my friends. D. All of the above	D: Own Your Online Presence. When available, set the privacy and security settings on websites to your comfort level for information sharing. It is ok to limit how and with whom you share information.
	2. What do you do when a stranger asks you to give them a picture of yourself on social networking sites? A. Send no pictures, and tell an adult immediately B. If you think you know them, send the picture C. Send the picture, even if they're a stranger D. Ignore them	A: You should never give pictures of yourself to a stranger because you do not know who they are or what they may be doing. When a stranger is asking for a picture, immediately deny and tell an adult. You should never give anyone a photo that you would not want someone else to see. Even if you are comfortable with that person, it could still end up online or be shown to others
	3. From online, who should you accept friend request? A. Anyone B. A friend of a friend C. Someone you think you've met before D. Only people you definitely know	D: Only friend requests from people you definitely know, you should never accept friend request from strangers or anyone else you are uncertain.
	4. Others cannot see anything I send in my private email, Instant messenger or Chat (Tik Tok, Facebook, WhatsApp, Instagram, Hangouts, Twitter, Skype, Myspace, Snapchat, LinkedIn, and gaming). A. TRUE B. FALSE	B: There are people and programs that can "see" into your private correspondence online. NEVER send personal information unless you are positive it is a secure site
	5. Jessica's friend Sophie asks for Jessica's password to her Facebook account. What should Jessica do? A. Give Sophie her password. Sophie is her friend and Jessica can trust her. B. Tell Sophie her password and change it as soon as she gets home. C. Don't give her password to Sophie.	C: Protect your personal information. Passwords are never to be shared with anyone other than a parent or guardian. It is a good idea for parents and guardians to keep passwords to make sure you remain safe and secure. Just because you spend time with friends, doesn't mean you have to follow everything they do. If they are doing something that doesn't seem right, you should feel

		completely comfortable standing up for what you think is right.
	6. If I want to know something about a stranger that sends me an Instant Message, I can check their profile and trust that information. A. TRUE B. FALSE	B: Part of the Internet's wonder is its anonymity and sometimes the worst thing, too. Unlike the physical world, you cannot verify a person's age, location, etc. online so it is easier to lie and get away with it.
Online Activities Specific Threats	1. You have been to a gaming/video website and it is asking you to download a link before playing the game/watching the video. What should you do? A. Show the link to an adult and ask them if it's safe B. Download it anyway C. Don't download it, it must be illegal D. Ask your friends what to do	A: If a website asks you to download something, you should always speak to an adult. You never know what that could be
	2. I can always trust emails and attachments I get from friends. A. TRUE B. FALSE	B: New programs and viruses send out emails without their knowledge or consent to everyone in your inbox. Verify it is in fact from your friend first.
	3. Private browsing" is a feature in many internet browsers that lets users access web pages without any information (like browsing history) being stored by the browser. Can internet service providers see the online activities of their subscribers when those subscribers are using private browsing? A. Yes B. No	B: If you want to hide your activity from your service provider, consider a VPN.
	4. When it comes to information searching online, you can safely search for information from any site. A. True B. False	B: When searching information online, you should always search from trusted and well-known websites. Check to be sure the sites is security enabled. Look for web addresses with "https://," which means the site takes extra measures to help secure your information. "http://" is not secure.
	5. You and a friend are on the computer, looking to download music and movies. You should: A. Go to a site that your friend uses and download a few files onto the computer. B. Only with your parent's permission, go to trusted websites or app stores to download music and movies.	B: Only with your parent's permission, go to trusted websites or app stores to download music and movies. Your friends may not know what websites are safe or unsafe for you to download. It is illegal to download music or movies from certain websites. Only purchase music and movies from established services for media distribution.
	6. It is okay to download FREE music/videos from music/video sharing sites, as long as no one finds out. A. True B. False	B: This is the same as stealing from a store and you are stealing from your favorite artists as well! Only purchase music/videos from established services for music/video distribution. Some file sharing sites are also well known sources of malware distribution. Remember, safer for me more secure for all. What you do online has the potential to affect everyone – at home, at work and around the

		world. Practicing good online habits benefits the global digital community.
	7. You are playing or watching videos, gaming, information searching, studying, social networking, emailing on a gadget and the app asks for your current location. It's okay to enable location services because all of your friends do the same thing and if they do it, it must be okay. A. True B. False	B: Think before you app. Many apps do not need geo-location services enabled in order to provide the service. Make sure you decline or opt out of the location service feature on your phone. If you do not know how to do this, ask your parents. Protect your personal information by reading the privacy policy of an app before you download it to understand what information the app accesses and how it uses your information.
Gadget Specific Threats	1. Turning off the GPS function of your gadgets prevents any tracking of your phone's location. A. True B. False	B: If it were only that easy. A 2018 Princeton study found that device's time zone and information from its sensors could be combined with public information like maps to estimate your location, even without GPS data.
	2. Installing a virus checker on my gadget will keep my gadget safe. A. TRUE B. FALSE	B: Just installing the program will help for a little while, but new viruses are spawning all the time. Update and run the software at least once each month.
	3. Tjipena unlocks his smartphone and notice he has 12 apps that need to be updated. What should he do? A. Ignore the prompt to update B. Update the apps.	B: It is important to keep a clean machine. Keeping machine means having the latest operating system, software, web browser, anti-virus protection and apps on your computer and mobile devices. You should also only have apps on your phone that you actually use
	4. You receive a chain email that tells you to pass it on to 10 of your closest friends. Do you: A. Send the email to your friends – it is so cool and you want them to see it too! B. Delete the email. You are never sure what viruses these types of chain emails can have.	B: When in doubt, throw it out! Links in email, tweets, posts, and online advertising are often the way cybercriminals compromise your computer. If it looks suspicious, even if you know the source, it's best to delete or if appropriate, mark as junk email.
Online Behaviour Specific Threats	1. You posted a picture online, but soon decided to take it down. You are worried your friend may see it, but then soon remember that person DOES NOT have a computer. Your friend will never see the photo. A. True B. False	B: You never know who is going to see things that are posted online. Even if your friend does not have a computer, there are many other ways he could see the photos after they have been shared with friends. Copies could be passed around and someone may have saved an image before you deleted it. Be a good online citizen. Think about images you post and whether your friends would be okay with them. Post only about others as you would have them post about you. Whenever possible, get permission before posting pictures or videos of others. Likewise, let others know they need your permission before posting pictures or videos of you.
	2. You don't have to worry when you visit your favorite sites, like Facebook and gaming sites,	B: Trusted sites can be safer. However, what you do on those sites – such as clicking on posts with links or using apps – can put you at risk. The best security

	because they are safe from spyware, malware and other online threats. (True or False) A. True B. False	step you can take is to Keep a Clean Machine. Keeping a Clean Machine means having the latest operating system, software, web browser, anti-virus protection and apps on your computer and mobile devices. Remember, when in doubt, throw it out! Links in email, tweets, posts, and online advertising are often the way cybercriminals compromise your computer. If it looks suspicious, even if you know the source, it's best to delete or if appropriate, mark as junk email.
	3. When online, you should be careful whenever approached by a new person or asked to provide information about yourself. A. True B. False	A: You always need to be on the lookout for online intruders! Be careful because they may be trying to get information from or about you. Remember to Be Web Wise and think before you act. Be wary of communications that implore you to act immediately, offer something that sounds too good to be true, or ask for personal information.
	4. You receive an email from a person that identifies themselves as your friend John. They want to meet you in the park after school. Do you: A. Tell your parents about the email and ignore the request. B. Ask the person a question only John would know to make sure it is John. C. Go to the park and meet your friend John.	A: Some people will pretend to be other people and may be impersonating someone you know. It is better to be safe than sorry! Unfamiliar email addresses and posts on social network sites should raise a red flag. Let your parents know and let them help you make the right decision about contacting John.
	5. You should always know whom you are talking to online. A. True B. False	A: The Internet can be a place to meet people and join new communities. However, just because you meet someone online, it does not mean you really know his or her identity. Use caution when interacting with new people. There is nothing wrong with being suspicious and extremely guarded about sharing any personal information.
	6. The great thing about the cyber world is that you can say things you might not always say directly to someone's face. A. True B. False	B: Statements you make online about people can be just as hurtful as saying them face-to-face. Being nice in the cyber world is equally as important as when you talk face to face. If you do not want it done to you, do not do it to someone else! Be a good online citizen. Post only about others as you have them post about you.
	7. The pictures you decide to post online today can affect your future reputation. A. True B. False	A: The photos you post online may never go away! In the digital age, you need to pay attention to your reputation from the moment you start going online. Your online reputation can be both positive and negative; depending on the choices, you make and can affect the future when you apply for colleges or jobs. You can manage your online reputation by remembering to Own Your Online Presence and setting privacy and security settings to your comfort level for information sharing.

	8. Stealing other people's work online – from sites like Wikipedia and Google – is a crime. A. True B. False	A: Stealing other people's work is considered theft. If you cut and paste content into your homework without citing the source, it is cheating and plagiarism.
	9. You are deciding on what personal information to post about yourself in an online profile. You decide to: A. Review the information carefully before you post it because you do not want to post too much information about yourself. B. In order to prevent misuse of your information, don't post too much information about yourself on Facebook, personal websites, your blog, or in chat rooms. C. Go ahead and post information about yourself online, because you can always choose to edit it later if you don't want people viewing certain information. D. BOTH A & B	D: Own your online presence. When available, take the time to understand and set privacy and security settings on websites to your comfort level for information sharing. You should know who would see the content before you post it.
	10. Post only about others as you would have them post about you. A. True B. False	A: You should always practice digital respect. Treat others as nicely as you would like to be treated. Remember, safer for me more secure for all. What you do online has the potential to affect everyone – at home, at work and around the world. Practicing good online habits benefits the global digital community.
	11. After a disagreement at school, a group of kids sends Jaydon threatening messages on Facebook. What should he do? A. Block them from his page. B. Keep the emails and comments he receives. C. Tell his parents. D. All of the above	D: If someone is bullying or harassing you online, you should tell your parents or a trusted adult. Ignore and block the person and save all messages. Many websites, including Facebook, have ways to report the abuse and/or help you respond to messages that make you uncomfortable.

Target player

The COSBIA was initially created in the interest of influencing children behaviour aged 13-17 on the Internet and raise their cyber security awareness.

Progression

The game starts with a short intro scene where the children behave insecurely online. Then they get exposed to cyber criminals through innocently sharing information, posting photos and messages about themselves and befriending strangers. Secure online experience attainment through performing several

empowerment activities. Empowerment is achieved through security knowledge, secure behaviour, secure experience and reduce exposure to online threats in the player over time. The player also obtains rewards through completion of security knowledge, secure behaviour, secure experience and reduce exposure to online threats. The game should have three (3) levels, level 1 is on security knowledge, level 2 is on secure behaviour and secure experience and level 3 is on reducing exposure to online threats.

- The first level is on cyber security knowledge; users are introduced to mechanics of information security. How to measure the security of players on information security while performing their online activities (playing games or social networking sites);

    - When adding strangers
    - When share personal information such as address, phone number, or school name or location with strangers online.
    - When sharing picture to close friends is limited
    - When posting everything online such as feelings and emotions

    Empowerment

    - Do not add strangers
    - Do not share personal information such as address, phone number, or school name or location with strangers online.
    - Picture sharing to close friends should be limited
    - Once you have written something you cannot delete it online.

- Once the player beats the first level, they get a crown and can advance into the second level. Users are introduced to secure online behaviours which results into secure online experience. How to measure the security of players on secure online behaviours;

    - Not wary of stranger
    - Meeting online friends without permission
    - Pay attention to insulting messages and do not report to parents
    - Do not pay attention to parental regulations and rules
    - Do not report inappropriate web content upon finding out
    - Pay attention to popups

    Empowerment

    - Be wary of stranger
    - Get parents' permission to meet online friends
    - Ignore insulting messages and report to parents
    - Confirm parental regulations and rules
    - Report inappropriate web content upon finding out
    - Ignore popups

- Once the player beats the second level, they get a crown and can advance into the third level, users are introduced to mechanics that Reduce exposure to online threats. How to measure the security of players on reducing exposure to online threats while on Internet;
    - Security software out dated
    - Use same passwords for every online account
    - Geolocation software is always on
    - Suspicious downloads
    - Clicking on clicks in emails and providing personal information.

  Empowerment

    - Protect your computer by updating security software regularly
    - Install anti-virus software
    - Create unique passwords by using different passwords for every online account this helps to prevent others from accessing your personal information
    - Control privacy and security settings to control or limit access to information such as which apps have permission to access contacts, location, calendar
    - Switch off geolocation software for sharing locations on smart devices, it can let unfriendly know where you are.
    - Be careful of suspicious download, they could expose you to potential viruses and hacks
    - Never click on links in emails asking for information of any kind this could expose you to a phishing scam.

- Once the player beats the third level, they get crowns and should return back to activity.

Principle Gameplay mode

i. **Goals**

Overall (long term): Influence children's behaviour online and raise their cyber security awareness

Gameplay (short term): Get empowerment, advance to the next level.

ii. **User Skills**

Tap on the screen

Drag and drop

Puzzle solving

Rearranging pieces

Strategize

iii. **Challenge**

Difficulty will advance by making the player score more than 3 points for secure online behaviour, to move to the next level. To mitigate difficulty, the user will have to play better, level up their online behaviour.

iv. **Losing**

Losing conditions are by running out of time, and a score of less than three. When the player loses, there must be an image showing vulnerable online experience, negative online experience or threatening online experience depending on the player's online behaviour.

v. **Art style**

Everything should be very colourful and feel alive, with highly animated scenarios and layered background.

vi. **Music and sounds**

The music should have a Retro style, appealing to 8-bit nostalgia but high quality. It is important that a lot of sound effects praise the user when they do something good. There should be immediate and positive feedback. When time is running low, add a sound that makes the users nervous. The sad scenes should be accompanied by Accordion/ Violin music and sound like a sorrowful tango. For in-game music, use a more relaxed approach with happy tunes and going up on tempo as the level progresses.

Appendix I: COSBIA Game Evaluation Criteria

COSBIA MARKSHEET					
COSBIA					
Judge name:					
DATE:					
Please indicate with an X if Yes or No					JUDGE COMMENTS
Questions	Yes	No	MARK	FULL MARKS	
1. Is the game Interactive? Can you make a choice?				5	
2. Does the game allow the child to have different options on Gadgets and platforms				5	
watching Videos, playing game, searching for information, studying, social networks, emailing etc.?				10	
4. Does the game evaluate the user experience based on the answers given through the game/quiz by the child?				10	
5. Does the game have a way of outputting the online experience of the child?				5	
6. Does the game have a way of outputting online behaviour of the child?				10	
7. Does the game have a way of outputting secure online behaviour of the child?				10	
8. Does the game have a way of outputting secure online experience				5	
9. Does the game evaluate how knowledgeable the child is on the different threats?				5	
10. Does it give tips on how to improve on being safe online?				5	
11. Are there multiple exit points while playing the game?				5	
12. Are there any empowerment messages displayed when the child decides to exit?				5	
13. Are there any empowerment messages displayed after ever score?				5	
14. Is the game doing what it is expected to?				5	
15. Is the game usable?				5	
16. Is the game appealing?				5	
MARK OBTAINED			0	100	

General Comment

Appendix J: Publications

An analysis of children's online activities and behaviours that expose them to cybercrimes

[1]Jennyphar Kahimise, [2]Dr. Fungai Bhunu Shava
[1]*Tel: +264 812347785, Email: kjennyphar@gmail.com*
[2]*Tel: +264 61 207 2510, Fax: +264 61 207 9510, Email: fbshava@nust.na*
[1, 2] *Namibia University of Science and Technology, 13 Jackson Kaujeua Street Private Bag 13388, Windhoek, 9000, Namibia*

***Abstract* — In this paper an analysis of children's online activities and behaviour that expose them to cybercrimes was done. Children nowadays are constantly online and as such they are exposed to cybercrimes. This research used a systematic literature review to analyse literature on online activities and the behaviour of children that exposes them to cybercriminals. The results indicate that children mostly visit social networking sites and the greatest online risk to them is sexual exploitation. However, online threats such as cyber harassment and exposure to violent Internet content can also be faced. The findings of the reviews provide guidelines for Internet child protection policy makers as well as feed into further research on how to develop child online protection (COP) solutions which educate children on safe and secure online behaviour.**

***Keywords*: — Child online activities; child online behaviour; online exposure; cybercrimes**

I. Introduction

THE Internet provides amazing opportunities by improving communication, social connections and technical abilities for children. Nevertheless, it cannot solely guarantee a secure environment for them. According to [1], many children and young people are unaware of the many safety hazards that most Internet platforms pose. Having no experience and knowledge, the behaviour of children potentially exposes them to cyber criminals as the children can innocently share information and befriend strangers. Children in particular willingly expose personal and private details about themselves from which cybercrimes may arise either in their real world or virtual world if this shared information ends up in the wrong hands [1].

As most things in life have dual aspects, there are concerns of potentially inappropriate material in the digital world. A number of researches have shown that most young Internet users are still at a low level of understanding and awareness on Internet safety [1]-[12]. Some young children are involved in dangerous Internet operations such as providing private data and pictures to strangers and surfing inappropriate websites. Reference [2] shows that children and young people's use of the Internet is changing fast, where societal, market and the technological revolution plays a big role. Internet usage by children varies according to the child's gender, age and socioeconomic status and it differs based on the location, devices and rate at which they access it [2]. In addition, the better the Internet access for children, the more their Internet activities become deeper and diversified [2]. Children and young people use the Internet for different reasons like social networking, uploading pictures and homework, which is broadly used by older children compared to younger children who use the Internet for particular purposes such as gaming and watching online videos [2]. According to a study conducted by [9] in South Africa, 86.3% of most children had a social networking website account, where WhatsApp had the highest percentage, followed by Facebook and then Instagram. They further state that from the interviews, the Internet was mostly used by the older children than by the younger children. Reference [9] shows that, overall, more than a half of the participants used the Internet for educational and social activities, nonetheless business, civic and community involvement was much less frequent.

The impact of this expose on children's behaviour and livelihood are personal information harvests such as collecting personal information to customize online advertising to a user's profile or even sharing personal information online by online social networks or companies [1], teenage bulling and harassment in the United States of America [13], and online luring and grooming of young teenagers for the prostitution business [14]. Moreover, [15] further outlines the online lurking dangers such as child online exploitation and victimisation. Reference [16] outlines that the use of digital technology affects children's mental well-being, social relationships and physical activities. These factors then set us to further investigate on the Internet activities and the behaviours of children that expose them to cybercrimes.

II. OBJECTIVE

This study's primary goal was to analyse children's Internet activities and behaviours that expose them to cybercrimes. To achieve this objective, the following sub-objectives were aimed at being achieved.

Sub-objectives;

1. To analyse how children behave online.
2. To evaluate online activities that expose children to online interactions with strangers.

978-1-7281-4790-1/19/$31.00 ©2019 IEEE

The following questions were formulated to achieve the above mentioned objectives;

1. How do children behave online?
2. Which activities specifically expose children to online interactions with strangers?

III. Methodology

This paper used a systematic review of the literature to provide a wider overview of prospective research on online children's activities, online children's behaviour, online children's exposure, and cybercrimes. The year of the article is limited to 2008 until 2018. To complete our paper list, we used relevant keywords to search in multiple computer science research paper repositories, and this included ProQuest, Sage, Science Direct and Google scholar. The search parameters included several keywords which should be mentioned in articles such as child online activities, child online behaviour, online exposure, and cybercrimes. Forty-three academic papers were reviewed but only twenty-four papers were selected for this review.

IV. Results

In this section, we present the outcome of the explanatory variables of interest which are online child activities, online child behaviour, online exposure and cybercrimes which are listed in columns in the table below.

Table 1: Reviewed papers on child online activities, child online behaviour, exposure and cybercrimes

Author (Year)	Child online activities	Child online behaviour	Exposure	Cybercrimes
[2]	Watch videos 94%, 56% Listen to music, 54%, Play games 67% ,Complete homework 47%, interact with family and friends 40%, Social networking 38%, look up information 27%, and upload videos, photos and music 27%	Children use the Internet to support and promote respect and kindness.	Add contacts they don't know on social networking sites, or send pictures they regret later, or disclose private data to strangers online	Self-harm, violence, bullying and sexual abuse, digital identity theft
[1]	Children visit social networks online, including Facebook, Google+, LinkedIn, Bebo, Weibo, Twitter, Tumblr and YouTube	On Facebook, children have been shown to accept requests for friendship from people they don't know but just have several friends with	Many children expose personal and intimate details about themselves, their friends and their relationships	The information exposes them to theft of identity, malware, fake profiles and sexual harassment
[11]	Watching Internet videos, films, or TV, school work, social networking sites, and seeking data about health	Sharing data on the following: hobbies (81%), school details (80%), real name (58%), and significant of birth (51%), with the least likely to be shared being details of parents' bank details (2%) and other details of parents (4%), home details (11%)	Lie on the Internet about their age (e.g. when establishing an account), accessing certain websites, or meeting someone online). This leads to Internet harassment and abuse	Victims' account that they didn't want to see, had someone stalked them, hacked data and asked for sexual pictures. Pornography, phishing and sexual intercourse
[9]	Social networking sites (WhatsApp, Facebook and Instagram)	Children are subjected to online meeting strangers and have been subjected to	Most children were confident to their technical abilities, saying they	Cyberbullying and unstoppable material access. Exposed to pictures of hate speech and gory
		seeing Internet sexual pictures. Send a signal to Xtended websites that they did not want with advertisements or links	have a lot of stuff online and they knew more about the Internet than their parents did.	images.
[17]	Social media	Children communicate and share their life anecdotally through pictures, videos and status updates on the Internet.	Post about their achievements, their family, share their emotions and feelings, post about their dating life, and share their private issues or religious political views.	The vast majority of teens (in the case 90 percent) believe that online harassment is an issue that affects their age children. Drama and intimidation or pressure to present themselves in some way.
[16]	Social networking sites, chatting and playing games.	Children spending too much time on the Internet could adversely affect their well-being.		digital technology could re-shape or hijack the brains of children
[18]	The first thing children do is to check the comeback of their social network (Facebook) every time they turn on the computer or smart phone.	About 32.5% of children shared their online mobile phone number, 10% shared their real home address. In addition, it was found that 1.9% of those sharing their home address out of 35 percent were actually primary school students who did not know that their posted images or photographs were automatically geo-located.	School children admitted accepting strangers into their friend list and sharing into their friend list and sharing private information at all times.	An opponent can use it to impersonate that specific user by sharing or revealing personal data and geo-tagging may result in the user being followed, i.e., paedophile instances, impersonation and stalking are possible.
[10]	In Kenya, 60% of kids have Facebook and Myspace accounts	Downloading movies or music. Online viewing of video clips (e.g. on YouTube). Sharing your own profile of social networking. Uploading to share pictures, videos or music with others. Uploading photos, videos, or music to share with others.	Lack of consciousness by parents may imply that their exposure to the Internet has an unwanted adverse impact on children. If no protective policies are implemented, children may face severe hazards and become Internet victims.	Online racial hateful content in child pornography, as well as improper or possibly detrimental sexual talk as harassment and online predator grooming.
[12]	Websites for social networking like Myspace and Facebook	In the relative 'safety' of the Internet, children with poor self-esteem, poor relationships with family members or who feel unpopular can be particularly at risk of forging such relationships. Young individuals sometimes take provocative pictures or even videos of themselves or friends, or create videogenic statements for just a few	Children often place very private data on their web pages or share important data as video communicatio n.	Predators frequently use chat rooms as a mechanism for meeting vulnerable young people for sexual exploitation of children.
[14]	Visit Websites for Social networking	Empowerment between the ages of 13 and 18 recorded sending or posting their own nude or semi-nude pictures showing they did so to	Children may also participate in illegal conduct, such as talking or explicitly sending pictures or	Cyber criminals survey through social networking sites and then lure and groom victim into their prostitution company (sexual molestation of

		someone they know only online	videos of videos of themselves before transmitting pictures or videos to others (an activity also known as 'sexting')	children)
[9]	YouTube video sharing sites, blogs, social networking sites, and games	Sharing private data online, behind their parents and purchasing stuff back online. Visit the website of the game and click on the action games to see the trailer for Alien vs Predator. It's been a lot of blood and grey and disturbing. Children are spending too much Internet time.	Many children are worried about Internet content that is violent, aggressive or gory. They show shock and disgust at seeing cruelty, murders, sexual abuse and even on the news on much in greater online than fictional violence, which adds to the depth of responses of children.	Collect children's data to share online violent and aggressive content. Cyberbullying, sexting, pornography, gory Internet content.
[19]	Social Networking sites	Posting of clips and pictures, online games and interactions with both known and unknown individuals	Sexual exploitation, cyberbullying and exposure to violent online contents.	The enhanced interaction online and the heavy use of online media expose vulnerable people and young kids to hazards such as cyberstalking.
[20]	Online Social Networking (OSN)	Befriending strangers, sharing information and meeting them offline. Exchanging sexually related messages or other content (e.g. photo, videos).	Inadequate content and contacts, Internet addictions, psychosocial deviation, loss of personal or sensitive information.	Theft of malware, phishing, identity and information, hate, violence, racism, gambling, excessive/violence, alcohol and cannabis.
[21]	Social networking	Children accessing websites that provide harmful content	Child receiving messages such as content that is violent or gory, pornographic content, racist, hateful and misguided marketing. Child involved in cyberbullying.	Cyberbullying, child pornography and robbery of identity.
[15]	Social Networking, watching films, playing games, investigating health problems and, among other operations, doing school work.	Online friendship with strangers and exchanging content information with strangers.	Online fighting, requesting private data from customers, and then exchanging that data electronically with others without permission, impersonation, cyber-stalking, and sexting from the individual.	Pornography, cyberbullying, sexual violence online and bullying or Adress stay unavailable.

All sources indicate that children use the Internet for social networks, three of the reviewed articles indicate that children use the Internet for schoolwork and four of the reviewed article indicate that children use the Internet to play online games.

In particular, from the analysis we found that most children spend most of their time on social networking sites, making them more likely to be exposed to cybercriminals and they are left with less time to do other potentially more rewarding activities. We also found strong evidence that children tend to share personal information and accept contacts they don't know without having to know that this could expose them to cyber threats just by a look at their profile by a total stranger. The risks associated with the different activities are cyberbullying, sexual exploitation, impersonation, online sexual harassment and access to inappropriate content. Children reported that they can be online themselves and use the Internet to encourage and promote respect and kindness [2]. However, reference [12] states that the magnitude of the problem is that children with bad self-esteem and bad interactions with family members may pose a particular danger of forging such relationships through Internet convenience. Sometimes children place offensive pictures or videos of themselves or friends just to get the feeling of acceptance or appreciation on the Internet [12]. Reference [17], further outlines that children post about their achievements and their family, share their emotions and feelings, post about their dating life and personal issues or religious or political beliefs on social media. Hence, we found that the typical exposure on the Internet by children is sexual exploitation, cyberbullying and exposure to violent content. In a report by reference [14] it is stated that cybercriminals go through social networking sites and lure and groom children into their prostitution organisations. In reality, cyberporn is now accessible in a variety of forms such as pop-ups ads, websites, Internet searches and emails [22].

More importantly, this Internet exposure to children may lead to Internet addiction, which in turn will alter the developing brain structure of adolescents, leading to poor academic performance, involvement in dangerous activities, unhealthy nutritional habits, poor personal relationships and self-injurious activities [23]. Reference [24] characterises the main profile of a cautious individual online by a strong perception of danger such as not spending too much time on the Internet, avoiding unsafe behaviour, talking to parents about Internet issues, obtaining advice and having clear rules on Internet usage.

V. Conclusions

Most children spend most of their time on social networking sites, making them more likely to be exposed to cybercriminals according to this study. We also found strong evidence that children prefer to share personal information and accept contacts they don't know without knowing that this could expose them to cyber threats. This calls for an increase in educating and sharing awareness with children on different internet risks and ways to stay safe on the Internet, mostly on social networking sites. There is therefore a need to train parents and teachers on how to educate children on staying safe online and the different risks associated with their online activities. To build on to these findings, future work can be on how to minimize the time that children spend on social networking sites and how to build a safer Internet environment for children.

References

[1] M. Fire, R. Goldschmidt, and Y. Elovici, "Online social networks: Threats and solutions," *IEEE Commun. Surv. Tutorials*, 2014.

[2] S. Livingstone, J. Davidson, S. Bansool, C. Haughton, and N. Anulekha, "Children's online activities, risks and safety A literature review by the UKCCIS Evidence Group," 2017.

[3] OECD, "The protection of children online," *OECD Counc. Recomm.*, pp. 161–165, 2012.

[4] S. Livingstone, L. Haddon, A. Görzig, and K. Ólafsson, *Risks and safety on the internet: The perspective of European children. Full Findings*. 2011.

[5] S. Livingstone, L. Kirwil, C. Ponte, and E. Staksrud, "In their own words: What bothers children online?," Eu kids online.net 2013.

[6] K. E. Soeters and K. Van Schaik, "Children's experience on the internet," 2006.

[7] United Nations Children's Fund, *Child Safety Online Global challenges and strategies Technical Report*. 2012.

[8] ITU, "Child Online Protection Statistical Framework and Indicators," 2010.

[9] J. Phyfer, P. Burton, and L. Leoschut, *Global Kids Online South Africa: barriers, opportunities and risks. A glimpse into South African children's internet use and online activities Monograph (Technical Report) (Published version)*. 2016.

[10] S. Atkinson, N. Alqahtani, I. Stengel, and S. Furnell, "Internet Risks for Children : Parents ' Perceptions and Attitudes," IEEE pp. 98–103, 2017.

[11] F. Bhunu Shava, M. Chitauro, J. Mikka, I. Nhamu, and A. Gamundani, "Exploratory research study on knowledge, attitudes and practices of ICT use and online safety risks by children in Namibia," 2016.

[12] D. D. Broughton, "Child exploitation in the 21st century," Elsevier Ltd Paediatrics and child health, 2009.

[13] M. Anderson, "A Majority of Teens Have Experienced Some Form of Cyberbullying," By Pew Research Center no. September 27,2018, pp. 1–18.

[14] H. Hillman, C. Hooper, and K.-K. R. Choo, "Online child exploitation: Challenges and future research directions," *Comput. Law Secur. Rev.*, vol. 30, no. 6, Dec 2014, pp. 687–698.

[15] P. Maoneke Blessings, F. Bhunu Shava, A. Gamundani Munyaradzi, M. Bere-chitauro, and I. Nhamu, "ICTs Use and Cyberspace Risks Faced By Adolescents in," AfriCHI, 2018.

[16] D. Kardefelt-Winther, "How does the time children spend using digital technology impact their mental well-being, social relationships and physical activity? An evidence-focused literature review. I How does the time children spend using digital technology impact their mental we," 2017.

[17] M. Anderson and J. Jiang, "Teens' Social Media Habits and Experience," Pew Research Center no. May, 2018.

[18] P. Santisarun and S. Boonkrong, "Social Network Monitoring Application for Parents with Children Under Thirteen," *2015 7th Int. Conf. Knowl. Smart Technol.*, 2015, pp. 75–80.

[19] H. Tennakoon, G. Sandakis, and A.-M. Mohammed, "Child online safety and parental intervention: a study of Sri Lankan internet users," 2018.

[20] E. Magkos, E. Kleisiari, P. Chanias, and V. Giannakouris-salalidis, "Parental Control and Children ' s Internet Safety : The Good , the Bad and the Ugly," 2014, pp. 1–18.

[21] M. J. Zacule De Barros and H. Lazarek, "A Cyber Safety Model for Schools in Mozambique," 2018.

[22] E. González-ortega and B. Orgaz-baz, "Minors ' exposure to online pornography in Spain : Prevalence , motivations , contents and effects . Minors ' exposure to online pornography : Prevalence , motivations , contents and effects," no. May 2014, 2013.

[23] A. H. Al-Badi, S. Al Mahrouqi, O. Ali, A. Al-Badi, and M. AL Khaled Hassan, "The Influence of the Internet on Teenagers' Behaviour in Oman," *J. Internet Soc. Netw. Virtual Communities*, vol. 2016, 2016.

[24] I. Ramos-Soler, C. López-Sánchez, and T. Torrecillas-Lacave, "Online risk perception in young people and its effects on digital behaviour," *Comunicar*, vol. 26, no. 56, pp. 71–79, 2018.

Jennyphar Kahimise and Fungai Bhunu Shava
Namibia University of Science and Technology, Windhoek, Namibia
jkennyphar@yahoo.com
fbshava@nust.na
DOI: 10.34190/ICCWS.20.127

Abstract. In this paper, an analysis of social networking threats was done. Websites for social networking are not just common to the youth of today, but it can be used by all parts of society to meet their daily needs and helps to keep in touch with old friends. Some of the sites of social networking including Facebook, Skype, Instagram, etc. have grown in popularity at an impressive level. Social networking sites could be used by individuals or organizations to create platforms through which users can share information or access it. According to the latest studies, threats in the social environment are mostly caused by social networking users that openly sharing private and personal information regarding themselves. The indicated shared information could be, relationship status, birth date, home address, telephone number, email address, and even the name of the school. Whether social networking users' behaviour is accidental or deliberate, this can provide an opportunity for perpetrators to figure out a method to exploit threats on social networking sites. This research uses a systematic literature review to analyse literature on social networking threats and different social networking sites. A diagram presenting the effects of social networking threats has been presented in this study as well. The results indicate that the most common social networking threats are phishing, spamming, cyberbullying and malware attacks. Children are more vulnerable to social networking threats because of less experience and lack of knowledge. The findings of the reviews provide knowledge to educate social networking users on the different social networking threats that they may come across while on social sites. As well as, feed into further research on developing guidelines for social networking users on how to protect themselves against social networking threats which can build awareness about potential threats to social networking.

Keywords: social networking threats, social sites, social threats protection

1. Introduction

In today's digital world, people are constantly looking at their smartphones, reading the newest updates and comments on social network sites about their connections. Rathore *et al* (2017) state that networking on social sites is a type of service on the web that establishes a virtual link between people of similar interest, experience and activities. It allows users to find new friends, expand the circle of friends and share information (Rathore et al., 2017). Kirichenko, Radivilova, and Anders (2017) added that the connectivity of the Global Internet is one of today's key phenomena that reshape the world as we know it. Moreover, the World Wide Web's love child is social networks, which comes in many ways, this includes photo sharing sites, microblogs, forums, social gaming, blogs, business networks, chat apps, and other social networks. The digital technology allows data to be sent simultaneously to a large number of receivers without starting the process again manually. It allows content to be shared instantly with a wide range of peers or even with the entire world via the World Wide Web (Davidekova and Gregus, 2017). Worldwide, the number of users on social networks is 2.34 billion, and in 2014 1.91 billion (Clement, 2019). In addition, Clement (2019) estimated 2.65 billion people used social networking sites in 2018 around the globe, a figure projected to rise to approximately 3.1 billion in 2021. The increasing popularity among internet users of social networking sites require self-reflection of human beings' personal and social behaviour. In a study by Zephoria Digital Marketing (2019), based on statistics, as of September 2019, there are more than 2.45 billion monthly active Facebook users worldwide, representing a 9 percent increase in year-over-year Facebook monthly active users. In another study by Sadeghian, Zamani, and Shanmugam (2013), based on StatisBrain statistics, Facebook currently has about 1.2 billion users and the maximum number of young people between the age of 18 and 24 who use social networks is 98 percent. Such statistics are evidence of how much time the young generation spends on social networking.

According to Murray (2011), 1.5 billion individuals around the globe have their profiles on social networking sites. When you build an account on the social networking website, everything looks great, but how you feel when someone uses your private information to start blackmailing. Social networking in today's societies has changed the way we communicate and share data with each other. Murray (2011) further stated that social networking utilizes software to create online social networks for individuals who share interests and events.

Social networking provides fresh possibilities for private expression, for cooperation and sharing. The development of the Internet has resulted in many types of Internet social behaviour including email, newsgroups, instant messaging, writing a blog, and internet dating services. The most popular technology concept in the 21st century is social networking sites. The number of respondents on these social networking websites has grown incredibly (Al Hasib, 2009). Such websites of social networks are networks where people are allowed to express their ideas, thoughts, and imagination as well as form social groups. These websites for social networks offer significant benefits for both individuals and businesses.

The success of social networking sites, however, create a high threat for its users. There is a risk with all new technologies, and the risk assessment is based on threats (Watters, 2011). A large number of personal data shared by users on social networking sites makes them a desirable target where attackers can get personal sensitive *personal information* (Rathore *et al.*, 2017). Large online social networks have become an important tool for the distribution of different information. Sadly, huge web-based risks and vulnerabilities may erupt in shared and large networks in a very short time (Wu *et al.*, 2019). Users commonly make several risks and errors when using social networking websites such as misuse of corporate computers, unauthorized software, misuse of passwords, unauthorized physical or network access and transmission of sensitive information while working at home between their work and personal computers. These risks keep escalating when users are youths or younger children who are naturally more vulnerable than adults (Fire, Goldschmidt and Elovici, 2014). Research has shown that young social networking users are still at a low level of knowledge and understanding of the security of the Internet (Anderson and Jiang, 2018; Sonia Livingstone, Professor Julia Davidson, Sagba Bataol, Haughton and Nandi, 2017; Anderson and Jiang, 2018; Fire et al., 2014; (OECD, 2012); United Nations Children's Fund, 2012). In an analysis by (Braimlan, 2017), respondents were required to show which Social Networking sites (SNSs) they had accounts with. Facebook was the most common, with 92% of the total sample, followed by Instagram with 77%.

Whether the behaviour of social networking users is accidental or deliberate, it provides an opportunity for perpetrators to figure out a method to exploit threats on social networking sites. In this paper, we present a thorough analysis of the various threats to social networking, affecting the safety of users of social networking in general and children in specific.

1.1 Key Objective and Research Questions

The study's primary goal is to review social networking threats. To achieve this objective, the following questions were formulated to achieve the above mentioned objectives;

1. What are the different social network sites?
2. What are social networking threats?
3. What are the solutions to social networking threats?

2. Methodology

This paper uses a systematic literature review to provide a wider overview of potential research on social networking sites, social networking threats and solutions on social networking threats. The year of the articles is limited to 2009 until 2019. To complete our paper list, we used relevant keywords to search in multiple computer science research paper repositories, this included ProQuest, IEEE, Science Direct, Google and Google scholar. The search strictures included several keywords, such as which should be mentioned in the article's social networking sites, social networking threats, and social networking threats protection. Thirty-seven academic papers where reviewed which only twenty five papers were selected for this review. Below is Figure 1 presenting the approached used by the researchers to complete this paper.

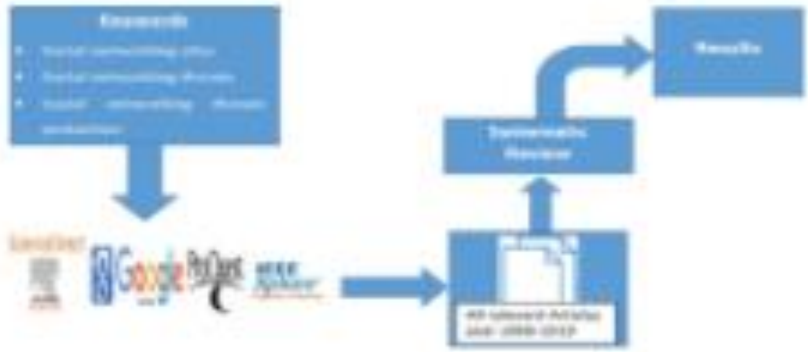


Figure 1: Researcher's approach process

3. Results

In this section, we present the results of the value explanatory variables as follows; social networking sites, social networking threats and solutions on social networking threats which is listed in columns in the table below.

Table 1: Reviewed papers on Social networking sites, social networking threats and solutions on social networking threats

No	Author (Year)	Social networking sites	Social networking threats	Solutions on Social networking threats
1	(Pilakulakosarti and Narasimha, 2013)	LinkedIn, Facebook and Twitter	• Viruses/worms/Trojan horse • Spam • Adware and Spyware • Keyloggers • Ransomware • Browser Hijacker • Crimeware	• Ordinary Data Backup • Client mindfulness • Principles in Intrusion Prevention Software (IPS) • Rogue security software
2	(Sowmya and Revathy, 2018)	Facebook, Twitter, Instagram and YouTube	• Phishing attacks • Spamming • Stalking • Fake attack on profile • Attack on Location Leakage • Attack on Account Compromise • Click jacking • Cross Site Scripting • Applications of malicious codes	• Guard against spams • Use websites that are trusted • Pop ups alert • Spam filters and Firewall • Bot unfriendly questions and use of CAPTCHA • Unwanted contacts block • Avoid auto follow • Profile privacy and Disable geo tagging • Avoid strangers and report stalkers • Social account auditing • Analyze red flag words
3	(Tarun, 2017)	Facebook, Twitter, Pinterest, Reddit and Instagram	• Facebook depression • Social anxiety of stress • Catfish • Cyber bullying • Cyber terrorism • Human trafficking • Cyber Drug dealing	• Ensure social media understanding and evaluation of what's happening in the world Awareness constantly.
4	(Kirichenko, Radivilova and Anders, 2017)	Facebook, YouTube, Twitter, Vine Camera, Ask.fm, Pinterest, Tumblr.	• Social engineering • Possibility of substitution of person or masquerade • Stealing passwords and	• Special software to monitor and analyse the social networks

No	Author (Year)	Social networking sites	Social networking threats	Solutions on Social networking threats
			• Attacks de-anonymization attacks • Spam & Attacks on Spit	
8	[Fire, Goldschmidt and Elovici, 2014]	Facebook, Google+, LinkedIn, Sina Weibo, Twitter, Tuenti and Xiaonei, MySpace	• Privacy risks • Identity theft • Malware • Attacks on Phishing • Spammer • Cross Site Scripting (XSS) • Web fraud • Clickjacking • De-Anonymization • False profiles/ socialbots • password Clone Attacks • Inference Attacks • Information Leakage • Location Leakage • Sexware • Sexual harassment	• Solutions on Internet Security • AVG privacyFix • Fill phishing defender • Norton secure web • McAfee Social security • MyPermissions • NoScript safety Suite • Facebook Privacy scanner • Defensio • ZoneAlarms privacy scanner • Net Nanny • MinorMonitor • Enhanced privacy interfaces settings • Phishing Detection • Clone profile detection • Fake profile detection • Sociware detection • Preventing information and location leakage
9	[Sudaghian, Zarsani and Mowlaei, 2013]	Facebook	• Phishing • Scam URLs • identity theft • Malicious third application • Spam • False Users • Redirects Legitimate look	• URL security tools • Privacy adjustment • Application access level adjustment • Limited sharing • Thinking twice before performing any action in social networking environment
10	[Ghani, 2012]	FriendSkin, MySpace, Facebook, Twitter, Hi5, Youtube, Flickr, Ning, Orkut, Xanga, Bing, Misc, Badoo, Delfi, Skyrock, Prophoto, Odnoklassniki.ru, V Kontakte, Digg	• Social engineering • Spammers, phishing and malicious attacks • Theft of identities • Defamation • Stalking • Personal dignity injuries and cyber harassment • Impersonation	• Encouraging awareness • Modifying existing legislation • Enable authentication • Using the most powerful antivirus tools • Providing appropriate security tool
11	[Baiku et al., 2010]	Facebook, Twitter	• Risk of malware • Net Reconnaissance • Spear phishing • Aurora attacks • Advanced persistent threat or cyber industrial espionage	• Information Security Police • Safety Education, Training and knowledge • Preventive Security Systems
12	[Al Hasib, 2009]	MySpace, Facebook and others	• Digital personal information dossier • Face Recognition • Content-based Image Retrieval • Image Tagging and cross-profiling • Complete Account Deletion difficulty • Spamming • Cross Site Scripting, Viruses and worms	• Encourage awareness-raising and education programs • Reviewing and reinterpreting the regulatory framework • Promoting better encryption and access control where appropriate • Setting acceptable defaults • Providing appropriate

No	Author (Year)	Social networking sites	Social networking threats	Solutions on Social networking threats
			• Mit Aggregators • Phishing • Information Leakage • Identity theft profile squatting • Stalking • Corporate Espionage	security tools
13	Gua et al., 2009)	Myspace, Facebook, Bebo, Orkut and friendster	• Spam attack • Worm attack • XSS attack • Plug-in attack • Phishing	• Personal information protection • Install patches • Classify users • Spam block • Filter suspicious links • Notify security alerts • Detection of vulnerability • Anti-virus detections • Transmission encrypted

In particular, from the analysis we found that most of the common threats on social networking sites are phishing, social engineering, spamming, cyberbullying/cyberstalking, Data leakage and malware attacks. Phishing is a major internet problem and social networking (and malware) distributed phishing links are becoming increasingly common (Watters, 2011). Sadeghian, Zamani, and Shanmugam (2013) outlined that, a phishing attack can happen when a user clicks on a URL that forwards the user to a phishing webpage which could be a fake facebook account. So the user assumes that his session has ended and he wants to log in to see that they've been watching, but then sign in to the false page, and his username and password will be sent to the hacker (Sadeghian, Zamani and Shanmugam, 2013). Weiss (2008) stated that the major privacy concern using social networking sites is when privacy is affected by the inability of users to control perception and maintain social context. Increasingly, social network websites are also being used for phishing attacks designed to obtain bank or credit card details (Pfeiffer, 2008). Because the number of social networking sites is increasing, spammers use different techniques of spamming to gain benefits. Spam on social networking is more effective than spam that is distributed over the email due to social connections in social networking sites that generate trust (Soumya and Revathy, 2018). Malware developers use many common social networking sites to infect worms with huge user data networks (Nakeeketani and Narasimha, 2018). Apart from all the short come social networking sites may have, there are few advantages it may have, organizations may engage in social media intelligence to control the spread of fake news, identify the sources that spread the information and, if appropriate fight back with legal action (Bilici and Lubben, 2019). Schools are a promising place for the use of social networking sites, and some learners at school have used social networking sites to target specific pupils or to spread gossip and speculations against these pupils (Weir, Toolan and Smeed, 2011). The solutions will mitigate the threats of phishing, spamming, cyberbullying and malware in social networking platforms. Table 2 illustrates the solution against common threats in social networking sites.

Table 2: Common Social Networking Threats and Solutions

Common Social Networking threats	Solutions on Social Networking Threats
Phishing	Firewall and spam filters, Using trusted websites, URL safety tools, Limited sharing, Building self-awareness about social networking threats, Profile privacy settings, FB phishing protector, phishing detection
Spamming	Firewall and spam filters, Prevent unwanted contacts, Mass auto-follow, Privacy settings on profiles, Spam protection, Use of trusted websites, Attention to pop ups, URL safety tools, Limit sharing, Building self-awareness on social networking threats, social spam detector, block spam
Cyberbullying/ cyberstalking	Geo tagging disable, Limited sharing, Privacy settings on profiles, Avoid strangers, Report stalkers, Social account audit, Red flag words analysis, Block unwanted contacts, Proxy-based protection, Watch dog and social enabler, Building self-awareness about information disclosure, protect personal information
Malware	URL safety tools, Firewall and spam filters, Awareness, Mechanisms on cyber defence, anti-virus detection, vulnerability detection, notify security alerts

According to Fire, Goldschmidt, and Elovici (2014), the most well-utilized sexual crimes actually begin by creating an adult and a child relationship by using instant messaging, emails, chats, etc. The picture of a social media predator is that of an adult man who pretends to be friends of an innocent young boy or girl by which a predator collect private information, hiding his sexual intentions until the actual meeting, which probably involves rape or kidnapping (Fire, Goldschmidt and Elovici, 2014). In addition, social networking sites have become the most successful target of identity theft attackers, for instance, the attacker uses confidential data of the victim, such as his or her social security number, full name, telephone number, and email without his or her consent, for the conduct of cybercrimes, such as theft or fraud. (Rathore *et al.*, 2017). Fire, Goldschmidt, and Elovici (2014) further stated that, terrifyingly, cyberbullying can result in major consequences in some situations such as victims committing suicide after being cyberbullied on Facebook. It can also affect legitimate users and associate them with crimes they have not actually committed such as, a picture with hidden malicious user inside social networking sites, and a legitimate user inside social networking sites, and a legitimate user could access this picture without realizing that it contains an artifacts that are maliciously embedded (Rathore *et al.*, 2017). Another example is identity theft, in a previous case an over protective mother had a fake Mylpace identity in order to threaten her daughter's competitor (Wirt, Toolan and Sinnott, 2011). Hence, it is very important to be aware of social networking threats that social media may pose to you. The diagram below presents the effect of social networking threats.

Figure 2: Effects of social networking threats

4. Conclusion

Social networking sites can provide users with active and enjoyable services to express their interests and connect with friends without meeting face to face. At the same time, these networks could place users at serious risk of cybersecurity. Lately, the number of social network users is growing very fast, attracting an attacker's attention. A clear understanding of issues relating to social network security will help the users learn how to best minimize safety risks on social networks.

We analysed the various social networking sites and the various threats associated with them in this paper. We have proposed solutions to common threats to social networking, which could help users mitigate the security risks in social networking sites. To build to these findings the future work would be on how does social networking threats affect our behaviour and are we heading for a prosperous future or a darker social networking site.

References

Fire, M., Goldschmidt, R. and Elovici, Y. (2014) 'Online social networks: Threats and solutions', *IEEE Communications Surveys and Tutorials*. doi: 10.1109/COMST.2014.2321628.

Ghuri, W. (2011) 'Cyber Threats in Social Networking Websites', *International Journal of Distributed and Parallel systems, Academy and Industry Research Collaboration Center (AIRCC)*, 3(1), pp. 319–326. doi: 10.5121/ijdps.2012.3309.

Al Hasib, A. (2009) 'Threats of Online Social Networks', *IJCSNS International Journal of Computer Science and Network Security*.

Appendix K: Children's COSBIA Evaluation

COSBIA GAME EVALUATION BY CHILD

Child name: _____ **Date:** _____

Age range

- 13 ☐
- 13-14 ☐
- 14-15 ☐
- 15-16 ☐
- 16-17 ☐
- 17 ☐

Gender

- Male ☐
- Female ☐

Questions

Please place an X in you preferred selection of answer (yes or no) for each question in the table.

Question	Yes	No	Comments
1.The game is interactive?			
2.The game allows me to make a choice to exit at any time and perform my intended activity?			
3.The game is easy to use?			
4. I like the game			

5.The game is appealing			
6.The game is interesting			
7.The game does not delay my intended activity			
8.The game is challenging			
9.The game is educating			
10.The game is easy to understand			
11.The game is easy to play			
12.I felt secure while performing my activity			

1. Why did you find the game being easy/hard to play? Please give your reasons

   _____

   _____

   _____

2. What platform were you accessing?
   a. Facebook ☐
   b. WhatsApp ☐
   c. Instagram ☐
   d. Twitter ☐
   e. Snapchat ☐
   f. Browser ☐
3. What activity are you performing?
   a. Watching videos ☐
   b. Gaming ☐
   c. Information search ☐
   d. Studying ☐
   e. Social Networking sites ☐
   f. Emailing ☐
4. Which device are you using?
   a. Samsung tablet ☐
   b. Samsung phone ☐
   c. IPhone ☐
   d. IPad/Tablet ☐
   e. Laptop ☐
   f. Personal computer ☐
   g. Others (please specify):_____

5. What percentage did you get to?
   a. 0-25 ☐
   b. 25- 50 ☐
   c. 50-75 ☐
   d. 75-100 ☐

6. What have you learnt from the game? Explain your answer
   a. _____
   b. _____
   c. _____
   d. _____
   e. _____
   f. _____
   g. _____
   h. _____
   i. _____
   j. _____

Thank you for taking the time to play the COSBIA game and for answering this questionnaire.

Appendix L: Editor's Report

ACET Consultancy
Anenyasha Communication, Editing and Training
Box 50453 Bachbrecht, Windhoek, Namibia
Cell: +264814218613
Email: mlambons@yahoo.co.uk / nelsonmlambo@icloud.com

29 October 2020

To whom it may concern

LANGUAGE EDITING – JENNYPHAR KAVIKAIRIUA

This letter serves to confirm that a **Master of Computer Science** thesis entitled **DESIGNING AN ALGORITHM THAT CAN INFLUENCE CHILDREN'S BEHAVIOUR ONLINE AND RAISE THEIR CYBER SECURITY AWARENESS** by Jennyphar Kavikairiua was submitted to me for language editing.

The thesis was professionally edited and track changes and suggestions were made in the document. The research content or the author's intentions were not altered during the editing process and the author has the authority to accept or reject my suggestions.

Yours faithfully

DR NELSON MLAMBO
PhD in English
M.A. in Intercultural Communication
M.A. in English
B. A. Special Honours in English – First class
B. A. English & Linguistics