Journal of Advanced Research in Applied Sciences and Engineering Technology

Journal homepage:
https://semarakilmu.com.my/journals/index.php/applied_sciences_eng_tech/index
ISSN: 2462-1943

Cyber Security Awareness Model Based on NIST (National Institute of Standards and Technology) for Secondary School Students in Malaysia

Zahidah Zulkifli[1,*], Ahsiah Ismail[2], Ely Salwana Mat Surin[3], Okfalisa Okfalisa[4]

[1] Department of Information Systems, Kulliyyah of Information and Communication Technology, International Islamic University Malaysia, 53100 Kuala Lumpur, Malaysia
[2] Department of Computer Science, Kulliyyah of Information and Communication Technology, International Islamic University Malaysia, 53100 Kuala Lumpur, Malaysia
[3] Institute IR4.0, Universiti Kebangsaan Malaysia, 43600 Bangi, Selangor, Malaysia
[4] Informatics Enginering Department, Faculty Science and Technology, Universitas Islam Negeri Sultan Syarif Kasim Riau, Kota Pekanbaru, Riau 28293, Indonesia

ABSTRACT

As cybersecurity issues surge, it highlights the pressing need for increased awareness. In our digitally interconnected world, where information technology underpins the lives of individuals, businesses, and even national security, the threat of cyberattacks looms large. To enhance national cybersecurity preparedness, there is a critical call to action: we must promote public awareness of cybersecurity issues and bolster the ranks of trained cybersecurity professionals. This research introduces a novel cybersecurity awareness model based on the National Institute of Standards and Technology (NIST). Its primary goal is to make NIST accessible to secondary school students pursuing ICT courses and their invaluable resource, the school counselling units. The model aims to instil cybersecurity awareness in secondary school students and guide them in choosing the most suitable higher education paths, particularly in the ICT and cybersecurity fields. The study comprises three phases. In the first phase, a systematic literature review (SLR) examines globally applicable cybersecurity education models. The second phase investigates the implementation of cybersecurity education for secondary school students in Malaysia. This includes interviews with school counselling units responsible for guiding students toward higher education and surveys of students in grades four and five enrolled in ICT courses. The third and pivotal phase focuses on developing the proposed model. It involves analysing and implementing the results of the SLR, mapping them to the NIST framework, and incorporating themes from interviews and surveys. As a tangible representation of the model, a mobile application prototype has been developed. The Cybersecurity Awareness Model empowers school counselling units to seamlessly integrate career exploration with career decision-making for secondary students at any stage of their development. Moreover, it offers a means to create strategies for after-school programs, particularly in the dynamic field of cybersecurity. This model is expected to guide students in exploring academic majors and careers, preparing for higher education post-high school, initiating internships or job searches, and adapting to a world in constant flux.

Keywords:
Cybersecurity; Cyber awareness; Secondary schools

[*] *Corresponding author.*
E-mail address: zahidahz@iium.edu.my

https://doi.org/10.37934/araset.61.2.5868

In doing so, it not only empowers individuals but also strengthens the nation's resilience in the face of cybersecurity challenges.

1. Introduction

In contemporary society, cybersecurity has emerged as a paramount concern necessitating widespread awareness. This is primarily attributed to the rapid proliferation of internet usage. A particularly alarming trend is the surge in remote work and increased internet browsing. A study finds that the longer hours spent on Internet or technology related activities promote negative behaviours such as cybercrime, behaviour problems, sexual activities and truancy [1]. Inadequate awareness about online activities can potentially expose individuals to the risks of cybercrimes. Research conducted has unveiled a concerning uptick in cybercrime incidents, correlating with heightened internet usage. A contributing factor is individuals' proclivity to share personal information, including their whereabouts, on social media platforms, rendering them vulnerable to potential data breaches. From a recent study, the security awareness among Malaysian is moderate. The most popular information security countermeasure practiced is scan PC. This is different from user's preferred countermeasure and knowledge which reveal that password and never reveal password as the most efficient countermeasure. This phenomenon shows that although education on security awareness is important, convenient and easy to use tool is comparatively important in encouraging users to practice what they have learnt [2].

As the capabilities of generative AI progress, the difficulties presented by disinformation and deep fakes are expected to change. Possible avenues for further study may encompass by creating detection technologies that are more resilient and flexible to keep up with the progress in generative AI, investigating the psychological and social consequences of continuous exposure to AI-generated disinformation and deep fakes, exploring novel approaches to verifying material and establishing trust in digital contexts and evaluating the efficacy of different educational and policy measures encountering the dissemination of false information [3].

Furthermore, the current secondary school curriculum in Malaysia lacks comprehensive cybersecurity education. This deficiency hampers students' understanding of this critical subject matter. Equally important is the need for Information Technology instructors in schools to possess cybersecurity expertise. This knowledge is indispensable in enabling them to effectively convey the significance of cybersecurity to their students.

With the problems mentioned, this paper aims to increase the awareness of cybersecurity among users. This is to achieve a higher awareness about cyber-crimes and inculcate self-regulatory attitude among netizens that can avoid from falling into cyber-crime traps [4]. Thus, this paper studies the current existing success models for cybersecurity education worldwide, then investigates the evidence related to the effectiveness of the current Cyber Security Education Models in the context of secondary school education. Based on that, we developed a cybersecurity awareness model based on the NIST model.

As a representative of the proposed model, a mobile application has been developed. The mobile application prototype derived from the users' requirements that have been obtained from the data collection phase that has been conducted earlier. It can help the internet users to know more about the security of their data and information, and the types of malware attacks that they can face when using the internet. They are also able to know steps on how to protect the data from being breached or stolen by the data theft that can lead to misusing it for other things. It also can be a reference for teachers on their teaching and learning in class. In addition, this mobile application has an attractive feature that provides knowledge on cybersecurity as a career that brings initial exposures for school

students to be more interested in cybersecurity careers. This application has been developed using Android Studio Code, Node.js, flutter, HTML5 and CSS with System Development Life Cycle method [5,6].

The research presented in this paper represents the development of a comprehensive and practical model for cybersecurity awareness using NIST. The Previous Studies Section introduces and motivates the problem of cybersecurity awareness. Fundamental research and development questions of importance to this area are discussed with a focus on the topic of cybersecurity awareness and career development in the area of cybersecurity among secondary students. The following section introduces the detailed development of the model based on the NIST. We demonstrate how the model can be applied to an example system. The subsequent section contains the findings.

2. Previous Studies

The secondary school students are chosen as they are more exposed to be one of the victims of cyber threats. The content in the current textbook used by secondary students in Malaysia contains only one chapter (chapter 1) that discusses the cyber laws, cybersecurity, and careers in ICT. It is in *Buku Teks Sains Komputer Tingkatan 4* [7] and *Buku Teks Sains Komputer Tingkatan 5* [8] for secondary four five syllabus. The rest of the courses are mainly focusing on development, programming, and database. School administration should consider the existing gender and school management roles of the present scenario to make effective policies for the students and providing them effective cybercrime prevention programs and activities [9]. From the context of IR4.0 readiness, there is a positive trend in the students' motivation to learn more about IR4.0, with many recognizing its importance for their academic and future career prospects. These findings underscore the importance of providing clearer guidance and support to help students navigate the complexities of IR4.0 education and opportunities [10].

Cybersecurity education is essential in preparing computer users with cybersecurity knowledge and skills, which will significantly improve security and lower the risk of digital ecosystems starting at an early age. Young people should have definite competences to be able to manage their own security on the Internet as well as evaluate the sources and develop a responsible Internet conversation. According to their age, children fall into the category of groups vulnerable to cybercrime. Children can easily access the internet anywhere and anytime [17]. Cases of Malaysian youth being the victims and perpetrators of cybersecurity threats such as cyberbullying and pornography are increasing. Recently, there was a viral clip that has been said using deepfake for threatening purposes. Deepfake is a type of artificial intelligence new deep learning-based method that is capable of creating convincing fake images, audio and videos, [9,12]. This technology can also lead the cyber-criminal to use deepfake to create fake videos as the risk is lower if compared to the physical criminals. For these reasons, cybersecurity education is essential in preparing computer users with cybersecurity knowledge and skills, which will significantly improve security and lower the risk of digital ecosystems starting at an early age.

This paper aims to develop a Cybersecurity Awareness Model using NIST (National Institute of Standards and Technology) [14]. NIST, a nonregulatory agency of the Department of Commerce, has developed a "cybersecurity framework" to help regulators and industry participants identify and mitigate cyber risks that could potentially affect national and economic security. The main objective of the framework is to manage cyber security risks within the organizations that implement it [15]. Organizations can use the Framework as a guideline to assess their existing cybersecurity program or to build one from scratch [14].

3. Methodology

The proposed Cybersecurity Awareness Model consists of four main phases, phase 1, phase 2, phase 3 and phase four. The proposed Cybersecurity Awareness Model process flow that comprises four phases, will be discussed in the following subsections. This paper mainly will be discussed on the Phase 3 as indicated in the red box in the Figure 1.

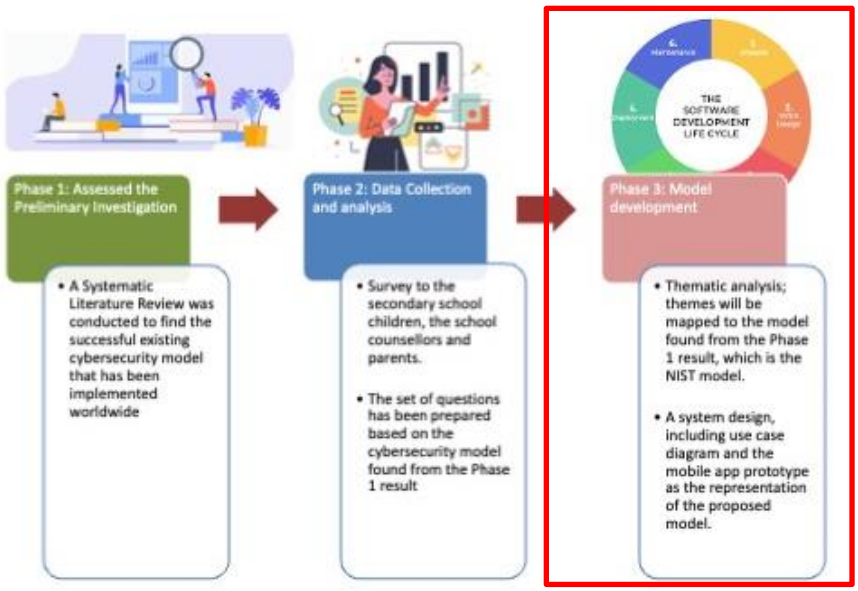

Fig. 1. The proposed cybersecurity awareness model process flow

3.1 Phase 1: Assessed the Preliminary Investigation

The phase 1 of the proposed Cybersecurity Awareness Model is to investigate the evidence related to the implementation of the current Cyber Security Education Models in the context of Secondary School Education. The study opted for a systematic literature review (SLR) procedures by Kitchenham and Charters [16] to investigate the effectiveness of current Cyber Security Education Models.

3.2 Phase 2: Data Collection

To achieve our objectives, data collection involved two primary methods: interviews with and surveys administered to students. The survey questions were distributed to students via Google Forms, encompassing a combination of open-ended and closed-ended inquiries. The total respondent for the survey is 100. This survey aimed to assess the students' level of awareness and knowledge regarding cybersecurity. The respondents in our study were students aged between 15 and 17 years old.

For the interviews, we conducted virtual sessions with two counsellors from the same school using the Zoom platform. Each interview lasted approximately 30 minutes [20]. The outcomes from this phase will be used as an input to the development of cyber security mobile application education modules that will be carried out on the next phase of this research.

3.3 Phase 3: Data Analysis and Model Development

Microsoft Excel version 2013 [18] is used for the analysis and tabulation of the percentages from all collected responses. The analysed information was presented in the tables and graphs using the "filter" function. Pivot table analysis was also carried out in order to obtain the result for the relationship pattern between the concept of knowledge and the related behaviours. The data was then presented in the graph format based on the analysis done. From the analysis of the respondent, a mobile application prototype has been developed. The contents of the mobile application prototype represent the proposed cybersecurity model.

4. Results

To demonstrate the reliability of our proposed model, the population of respondents were selected from secondary schools and cybersecurity event. The Klang Valley area includes districts in Selangor and Federal Territory of Kuala Lumpur. There are three secondary schools involved at Klang Valley area and two cybersecurity events. There are three categories of respondents which are students, teachers and parents. Each of the respondent categories have different sets of questions and all set of questions is design to understand their knowledge in cybersecurity. The details of the findings are described in the subsection below.

4.1 Phase 1: Systematic Literature Review

From the phase 1, 8 models that relates to cybersecurity education have been identified. These 8 models identified serve the different purpose, the purpose of the phase 1 is not to choose the best model to be implemented but to look at each benefit, their success stories and how each of the models can potentially contribute to the cybersecurity education in Malaysia specifically for secondary school students. Each of them serves different purpose and play their own roles. The study includes a set of six papers from among 152 retrieved papers published in SCOPUS-indexed journals [19]. Based on the review conducted, the results shows that eight commonly used and established Frameworks in Cybersecurity Awareness Model namely NIST Cyber Physical Systems Framework, Cybersecurity Capability Maturity Model (C2M2), Cyber Science Curriculum, Cyber Safety Education (CSE), Cyber-Routine Activities Theory (Cyber-RAT), Cyber Awareness Program, Attention, Relevance, Confidence, and Satisfaction (ARCS) motivational model and ADDIE model.

Among the 8 models, as shown in the Figure 2, NIST provides activities applied to awareness, education and training. As mentioned before, some of these issues stem from the lack of cybersecurity understanding of the teachers. Therefore, by training more high-quality teachers, the project will directly drive results for students. Various campaigns of security education, training and awareness programs also can be conducted to educate stakeholders about the potential threats and risks [20].

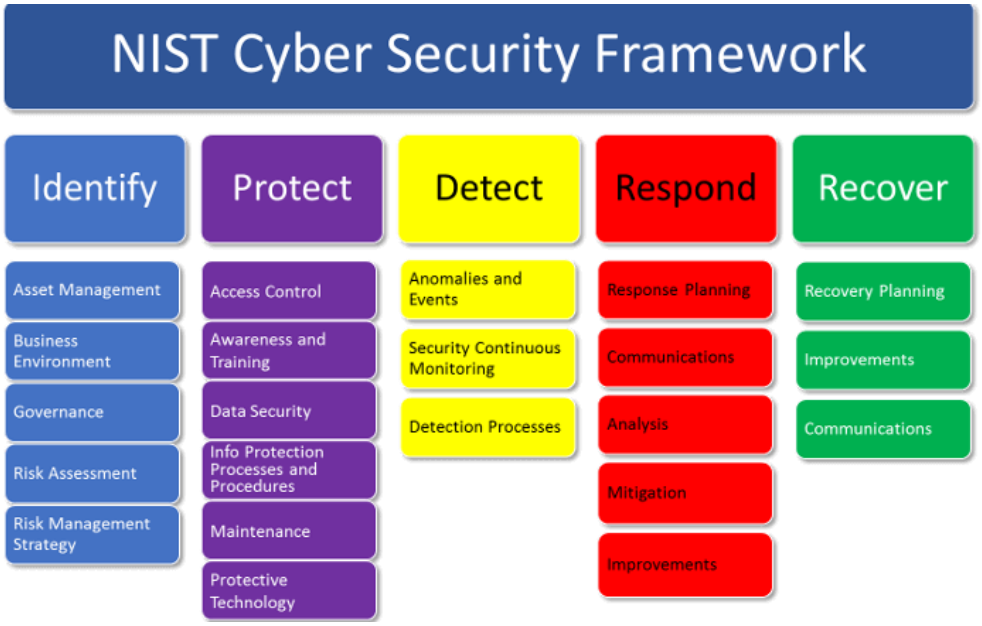

Fig. 2. The NIST cyber security framework

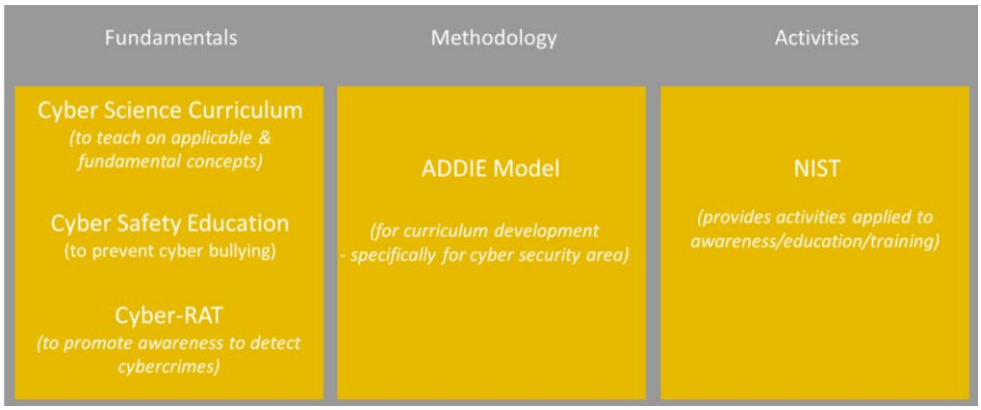

Fig. 3. The SLR result based on the suitability of implementation of the cybersecurity model

4.2 Phase 2: The Data Collection

The questions for the data collection are divided into two categories namely cybersecurity awareness and cybersecurity as a career. In this paper, only the result from the first category is highlighted. Generally, the survey shows that it is the government's responsibility to ensure safety in the cyber world. The government should provide clear rules and regulations as well as guidelines and procedures. Aside from that, the implementation and enforcement are essential to safeguard people from doing illegal things. As shown in Figure 4, one of the questions was asked on, from where they get the information about cybersecurity? The largest count of respondents who get information about cybersecurity is through the internet. Followed by a program and talk event at school. It shows that the students also refer to the internet to know about cybersecurity information. Parents also play important roles in the students' lives since they were responsible to educate their children at early ages. Insignificantly, a few respondents have the opposite opinion that it is the students themselves who need to be responsible for cyber safety. This is because anything can happen if the students explore the Internet unethically.

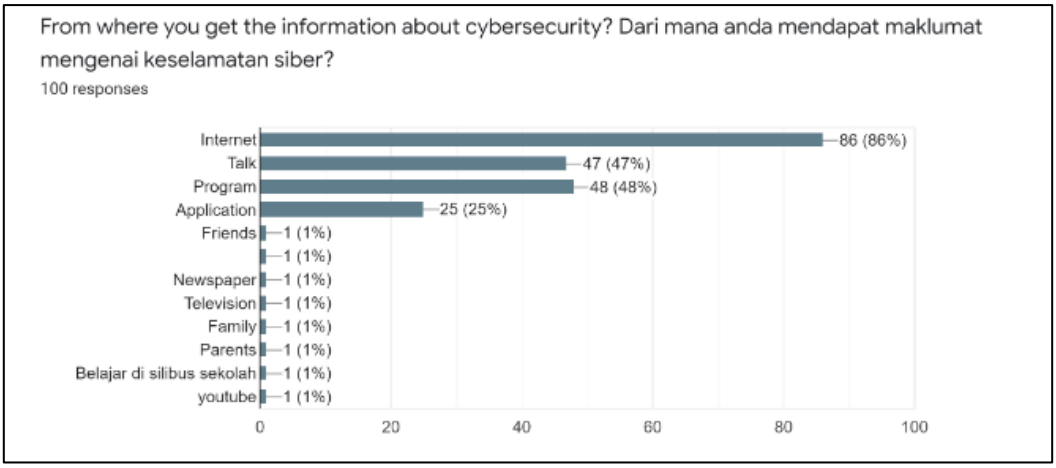

Fig. 4. One of the questions from the survey on the resources of the cybersecurity

Based on the findings of this study, it is evident that a majority of the respondents possess awareness regarding what constitutes personal data or information. Despite this awareness, there appears to be a tendency among the respondents to adopt a somewhat lax attitude towards the safeguarding of their digital presence, despite acknowledging the potential accessibility of their data and online activities by others.

This analysis of the survey questions implies that secondary school students' perceptions and behaviours are significantly influenced by their immediate environment, including parental and educational influences. Consequently, it is advisable for future research endeavours to delve deeper into understanding how these respondents manage and maintain control over their online activities, while simultaneously safeguarding themselves against the looming threats of cybercrimes. Within the school context, counsellors play a pivotal role in providing guidance and advice to students concerning their post-schooling endeavours. It is essential to note that all personal information pertaining to the interviewees was treated with utmost confidentiality and anonymity. Figure 5 shows most of the respondents spend more than 5 hours accessing and browsing the internet a day. The possibility for the students to be involved or being one of the cyber-crime victims is also higher.

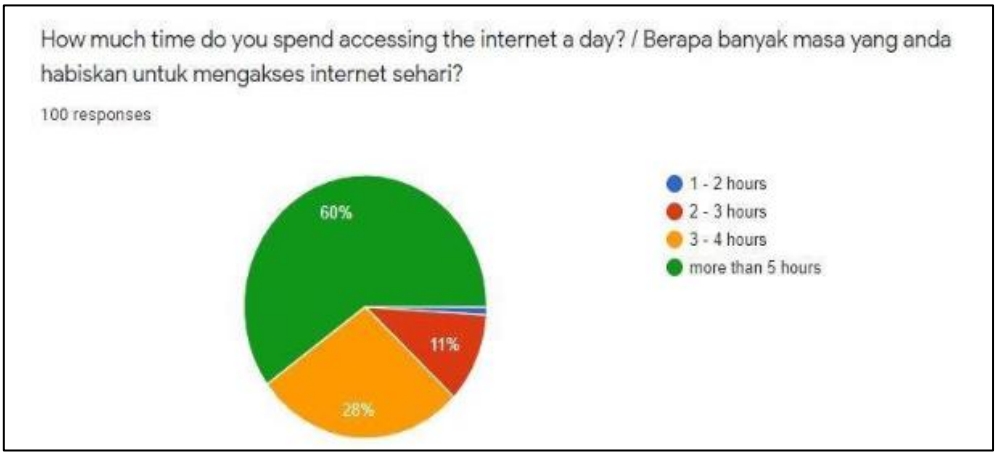

Fig. 5. One of the questions from the survey on the spending hours on the internet

Therefore, this indicates that the influences surrounding the students are very important. Essentially, education should be a top priority for future work while enforcing laws and regulations as well as teachers and parents become good role models [21].

4.3 Phase 3: Data Analysis and Model Development

This is the phase where the object-oriented approach is involved. From the Phase 1 result, NIST and the phase 2 result, the use case diagrams, activity diagram, sequence diagram and class diagrams has been produced as part of the analysis and design phase. From these design diagrams, a mobile application prototype has been developed using Android Studio, Flutter, Firebase. The use case diagram shown in Figure 6 is the representative of the model development of this study. the NIST is reflected in the "View Cybersecurity Resources" and "Answer Awareness Quiz" use case.

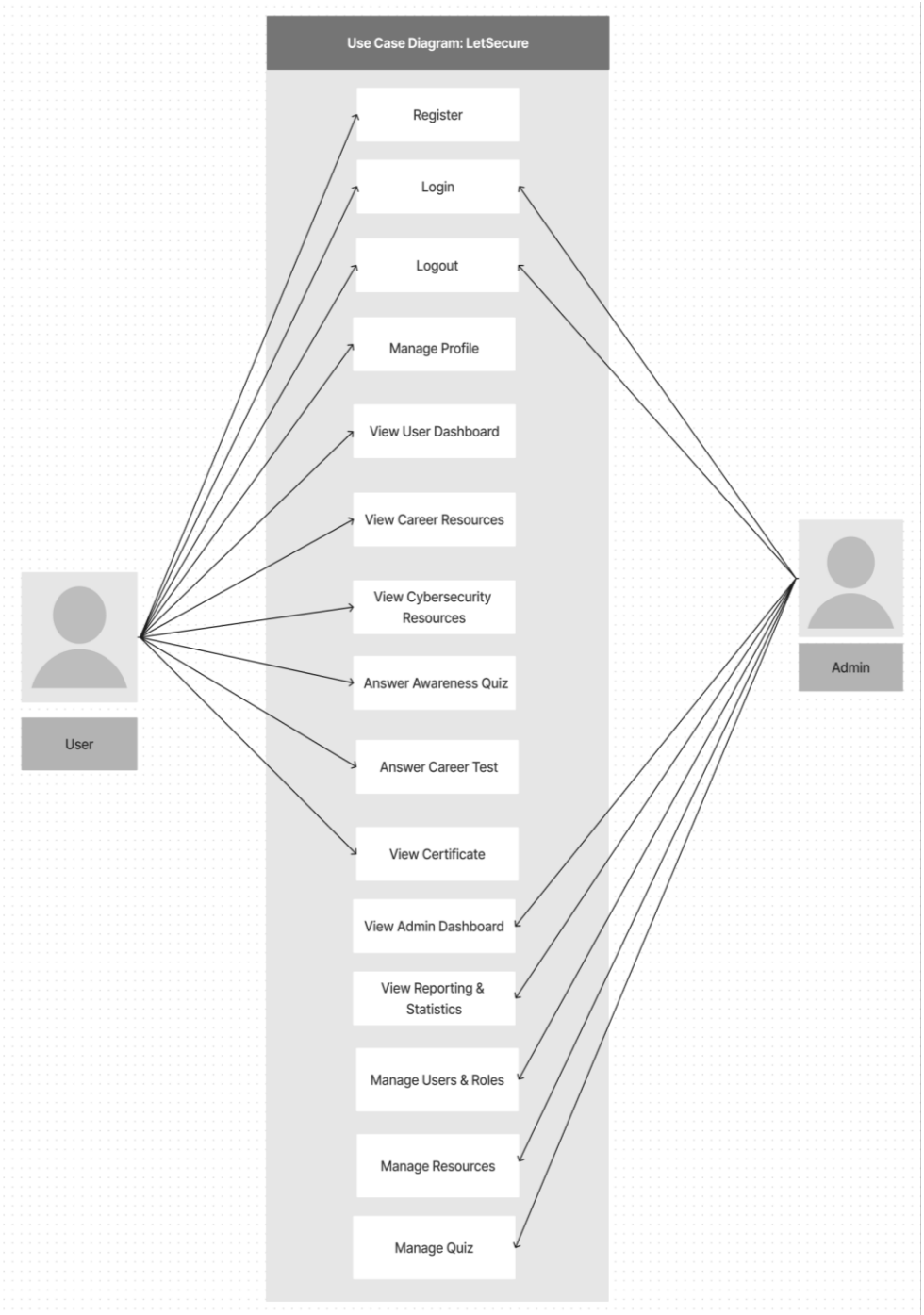

Fig. 6. The representative of the model development of this study

5. Conclusions

Based on the research conducted, it is shown that Malaysians are well-exposed to Internet use from a very young age as a teenager. The number of cybersecurity cases is increasing from time to time especially during the current situation which is changes in lifestyle of the people where they spend more time using the internet and gadgets. Thus, there is a need to monitor closely on the online activities to stay safe online due to the existence of cyber threats reported in the data gathered. The children are also expected to be well-informed of current cyber world issues and must learn to develop an instinct to be safe online. To deliver an effective cyber security education, it is important to ensure the education is able to translate from conceptual knowledge to practice and learning in depth in cyber security. This method improves effectiveness in eliminating gaps between perceived concepts and the actual knowledge [22].

Fig. 7. Login page

Fig. 8. View cybersecurity resources page

Fig. 9. Answer awareness quiz

From the data collection result, it shows that there is a need for a system for cyber security education that could be utilized in teaching cyber security to secondary students using a supplementary module without changing the existing school curriculum for an optimum learning experience since the early age [21]. With the development of the model, followed by the prototype of the mobile application, this would be one of the ways to increase the awareness on cybersecurity especially among the students and also teachers. The internet is now becoming a daily necessity but the usage must be controlled. The prototype of the mobile application can help especially the students to easily access information related with cybersecurity information on social media such as the types of threats, the organizations of cybersecurity in Malaysia and also interesting quizzes feature to evaluate users' understanding and to test their level of knowledge [23]. It is believed that with the advancement of technology, the proposed application is able to help to decrease the number of cybersecurity cases and cyber threats among the students. More applications are needed to spread the awareness of cybersecurity to society. All parties need to cooperate in disseminating the awareness to the young generations in order to prevent any undesirable events such as deepfake, cyberbullying and sexual harassment in social media [24]. The awareness to the young generations

in order to prevent any undesirable events such as deepfake, cyberbullying and sexual harassment in social media [24].

6. Future Research

This paper introduces a mobile application aimed at enhancing cybersecurity awareness, particularly among students and young individuals. The proposed mobile application seeks to provide a comprehensive cybersecurity education, fostering lifelong learning for secondary school students. The information and data within this application not only serve as valuable guidelines for parents and teachers but also offer insights into the current level of cybersecurity knowledge among Malaysian teenagers.

However, it is essential to acknowledge certain limitations and unexplored aspects, such as security and privacy assurance, which can significantly impact students' engagement in the cyber world. In future research, we plan to develop a cybersecurity education model tailored for implementation within school environments, with a focus on identifying the most effective tools for this purpose [24]. Nevertheless, this endeavour necessitates advanced technical enhancements for successful commercialization.

Moreover, leveraging the existing data, further data analytics can be conducted to unveil patterns, facilitating future planning, decision-making, and predictive analysis. We aspire that this study will generate public interest in bolstering cybersecurity awareness for upcoming generations. Consequently, sustained and robust research efforts are imperative to delve into how the internet can pose threats and to enhance security, especially among young individuals.

Acknowledgement

This research was funded by IIUM RESEARCH INITIATIVE GRANT SCHEME (FLAGSHIP) 2019 for a project “The Development of Cybersecurity Awareness Model using CTC – Chaos Theory of Careers for Secondary Schools.” The project id is: - IRF19-033-0033.

References

[1] Hamzah, Shahidah. "Level of Awareness of social media users on cyber security: case study among students of university Tun Hussein Onn Malaysia." *Turkish Journal of Computer and Mathematics Education (TURCOMAT)* 12, no. 2 (2021): 694-698. https://doi.org/10.17762/turcomat.v12i2.923

[2] Ting, T. T., Z. H. Eu, S. B. Lim, and K. S. Chong. "Analysis of Information Security Awareness within Users’ Preference, Practice and Knowledge." *Journal of Advanced Research in Computing and Applications* 12, no. 1 (2018): 1-8.

[3] Ghani, Miharaini Md, Wan Azani Wan Mustafa, Mohd Ekram Alhafis Hashim, Hafizul Fahri Hanafi, and Durratul Laquesha Shaiful Bakhtiar. "Impact of Generative AI on Communication Patterns in Social Media." *Journal of Advanced Research in Computing and Applications* 26, no. 1 (2022): 22-34.

[4] Zain, Azian Mohd, Nur Ekmanita Saberi, Fazlina Jaafar, Farrah Hanani Ahmad Fauzi, Wan Nor Raihan Wan Ramli, and Farrah Aini Lugiman. "Social Media and Cyber Crime in Malaysia." In *International Colloquium of Art and Design Education Research (i-CADER 2014)*, pp. 515-524. Springer Singapore, 2015. https://doi.org/10.1007/978-981-287-332-3_53

[5] Jafri, Azma Melia, and Zahidah Zulkifli. "Cybersecurity awareness mobile apps for secondary school students: Letsecure." *Journal of Information Systems and Digital Technologies* 3, no. 2 (2021): 94-108. https://doi.org/10.31436/jisdt.v3i2.240

[6] Nur Ain Zulaikha Jamaluddin, Azma Melia Jaffri, Zahidah Zulkifli. “Cybersecurity Awareness Mobile App for Secondary School Students: LetSecure.” *4th Digitalized International Invention, Innovation and Design Johor 2021*. eISBN: e-978-967-19663-5-8. Universiti Teknologi MARA Cawangan Johor (2021).

[7] Kementerian Pendidikan Malaysia. “Buku Teks Sains Komputer Tingkatan 4.” *Oxford Fajar Bakti Sdn Bhd.* KPM 2016 ISBN 978-983-47-2013-1. (2016).

[8] Kementerian Pendidikan Malaysia. “Buku Teks Sains Komputer Tingkatan 5.” *Oxford Fajar Sdn. Bhd.* KPM2017 ISBN 978-983-47-2375-0. (2017).

[9] Verma, Mudit Kumar, and Shyam Sundar Kushwaha. "Awareness towards cybercrime among secondary school students: The role of gender and school management." *Safer Communities* 20, no. 3 (2021): 150-158. https://doi.org/10.1108/SC-07-2020-0026

[10] Sidhu, Pramita, Fazlin Shasha Abdullah, and Mohamad Sirajuddin Jalil. "Awareness and Readiness of Malaysian Generation Z Students towards the Fourth Industrial Revolution (IR4. 0)." *Semarak International Journal of STEM Education* 1, no. 1 (2024): 20-27. https://doi.org/10.37934/sijste.1.1.2027

[11] Musofiana, Ida, Aji Sudarmaji, and Ira Alia Maerani. "Aspects of Legal Protection for Children from Cybercrime." *Jurnal Pembaharuan Hukum* 7, no. 3 (2020). https://doi.org/10.26532/jph.v7i3.12820

[12] Berita Harian. "Manipulasi 'deepfake' sukar dikenal pasti dengan mata." *Berita Harian* (2019). https://www.pressreader.com/@nickname12503716/csb_j4AQpoZSI_liFHyjwTo898r6ZEJdMJ1xaGjiSkLhnWlcNGD3No0XdbpYYCcJN50s

[13] Li, Yuezun, and Siwei Lyu. "Exposing deepfake videos by detecting face warping artifacts." *arXiv preprint arXiv:1811.00656* (2018).

[14] Shen, Lei. "The NIST cybersecurity framework: Overview and potential impacts." *Scitech Lawyer* 10, no. 4 (2014): 16.

[15] Almuhammadi, Sultan, and Majeed Alsaleh. "Information security maturity model for NIST cyber security framework." *Computer Science & Information Technology (CS & IT)* 7, no. 3 (2017): 51-62. https://doi.org/10.5121/csit.2017.70305

[16] Kitchenham, Barbara, O. Pearl Brereton, David Budgen, Mark Turner, John Bailey, and Stephen Linkman. "Systematic literature reviews in software engineering–a systematic literature review." *Information and software technology* 51, no. 1 (2009): 7-15. https://doi.org/10.1016/j.infsof.2008.09.009

[17] Jafri, Azma Melia, and Zahidah Zulkifli. "Cybersecurity awareness mobile apps for secondary school students: Letsecure." *Journal of Information Systems and Digital Technologies* 3, no. 2 (2021): 94-108. https://doi.org/10.31436/jisdt.v3i2.240

[18] Carlberg, Conrad, and Conrad George Carlberg. *Statistical analysis: Microsoft excel 2013*. Pearson Education, 2014.

[19] Amirah Fatin Zahari, Zahidah Zulkifli, Nurul Nuha Abdul Molok. "A Systematic Literature Review of Cyber Security Education Models' Implementations." *Malaysian Journal of Youth Studies*. YOURS'19 Vol. 1 (2020).

[20] Nur Ain Zulaikha Jamaluddin, Azma Melia Jaffri, Zahidah Zulkifli. "Cybersecurity Awareness Mobile App for Secondary School Students: LetSecure." *4th Digitalized International Invention, Innovation and Design Johor 2021.* eISBN: e-978-967-19663-5-8. Universiti Teknologi MARA Cawangan Johor (2021).

[21] Zulkifli, Zahidah, Nurul Nuha Abdul Molok, Nurul Hayani Abd Rahim, and Shuhaili Talib. "Cyber security awareness among secondary school students in Malaysia." *Journal of information systems and digital technologies* 2, no. 2 (2020): 28-41. https://doi.org/10.31436/jisdt.v2i2.151

[22] Molok, NN Abdul, and Z. Zulkifli. "Parents' roles in mitigating cyber threats to children in the new norm." In *Proceedings of National Population Conference*. 2021.

[23] Matondang, A., & Siddik, D. "Family Education in The Quran." *IOSR Journal of Humanities and Social Science*, 22 (2006): 07-16. https://doi.org/10.9790/0837-2206010716

[24] Javidi, Giti, and Ehsan Sheybani. "K-12 cybersecurity education, research, and outreach." In *2018 IEEE Frontiers in Education Conference (FIE)*, pp. 1-5. IEEE, 2018. https://doi.org/10.1109/FIE.2018.8659021