JCRINN Journal of Computing Research and Innovation
e-ISSN : 2600-8793

Available online at
https://jcrinn.com/
https://crinn.conferencehunter.com/

Journal of Computing Research and Innovation 10(1) 2025

Journal of Computing Research and Innovation

SWINDLERT©: Development of Augmented Reality Game-Based Interactivity for Enhancing Cybercrime Awareness

Sakinah Ali Pitchay[1*], AH Azni[2], Farida Ridzuan[3], Najwa Hayaati Mohd Alwi[4] & Muhammad Syahmi Imran[5]

[1,3,4,5]*Faculty of Science and Technology, Universiti Sains Islam Malaysia, 71800, Bandar Baru Nilai, Nilai, Negeri Sembilan, Malaysia*

[2]*Cybersecurity and Systems Research Unit, Universiti Sains Islam Malaysia, 71800, Bandar Baru Nilai, Nilai, Negeri Sembilan, Malaysia*

ARTICLE INFO

Article history:
Received 24 October 2024
Revised 31 December 2024
Accepted 10 January 2025
Online first
Published 1 March 2025

Keywords:
Augmented Reality
Cybercrime Prevention
Gamification
Edutainment
3d Environment
Game-Based

DOI:
10.24191/jcrinn.v10i1.497

ABSTRACT

As digital technologies advance, cybercrime has become a primary global concern, posing threats to individuals and organisations. Despite widespread Internet use, public awareness of cybercrime risks is still limited, emphasising the need for educational initiatives. The lack of engaging educational tools for cybercrime awareness is due to outdated, overly technical approaches that fail to captivate modern audiences. Limited investment and collaboration between cybersecurity experts and educational designers result in resources that are not as appealing or user-friendly as they could be. Therefore, this paper introduces SWINDLERT, an augmented reality (AR) game-based tool in a three-dimensional (3D) environment designed to enhance cybercrime awareness and educate users on early prevention. It addresses three key issues: (i) carelessness in sharing credentials, (ii) lack of cybercrime prevention literacy, and (iii) low student engagement in traditional lecture-based education. It has three main objectives: (i) to identify types of cybersecurity crime prevention, (ii) to develop an edutainment AR mobile game with 3D images, and (iii) to evaluate functionality and security. Using Agile methodology, we conduct user requirements through surveys and test the application at SK Teluk Ketapang, Terengganu, and Universiti Sains Islam Malaysia. 98% agree that SWINDLERT has effectively embedded good gamification elements such as levels, scores and timers. Users benefit from password complexity, email verification, and the ability to retrieve their progress on multiple devices. The game features three levels: beginner, intermediate, and hard. This approach blends immersive technology by integrating an AR quiz-based 3D snake and ladder board gamification to transform education, making learning engaging and enjoyable.

1. INTRODUCTION

According to a series of studies conducted towards the end of 2019, 68.4% of business executives expressed concern about their increased susceptibility to cybercrime. Many leaders believe 2020 will be a year of

[1*] Corresponding author. *E-mail address*: sakinah.ali@usim.edu.my

https://dx.doi.org/10.24191/jcrinn.v10i1.497

increased caution compared to this trend of cybercrime movements (Lazic, 2021). A review of 2019 cybercrime statistics shows that cybercriminals seeking financial gain were the driving force behind the majority (72%) of cybersecurity breaches. However, motives linked to espionage and other similar purposes accounted for 26% of cybercrimes (Lazic, 2021). This shows the severe cybercrimes that happened in 2019 when the pandemic occurred. The lack of preventative measures by society itself led to an increase in all of these crimes. This study focuses on three main issues. The first problem identified was carelessness in sharing credentials and data. Society does not take preventive steps to save their data on the Internet or share it with the public. Most do not care about what they share or give their credentials or data to an organisation without checking its policy or uploading photos or videos containing credential information to social media. As reported by Sunbiz thesundaily.com (2021) only 7% of Malaysian society know that their identities have been stolen, while the other 12% said that it may happen. From this statistic, it can be shown that Malaysian society does not care about their identities, whether they have been stolen or not, and only a few of them are aware of that situation and take action.

The second issue was illiterate in preventing cybercrimes. As the Internet grows extremely fast, society still does not know or know how cybercrimes trap victims on the Internet. Dewan Rakyat said that 51,631 online fraud cases were registered in Malaysia from 2019 to 2021, resulting in a loss of about RM 1.61 billion (Nuradzimmah, 2022). The Department of Statistics Malaysia (DoSM) reported that cybercrimes increased by 99.5 per cent, with about 20805 cases in 2020 from 10426 in 2019 (Nurul, 2021). Cases doubled in just a year, showing that cybercrimes increased drastically during this pandemic. Furthermore, the most significant rise in complaints was for the misleading element, which increased by 117.6% to 6,637 from 3,050 in 2019 (Nurul, 2021). From those statistics, it can be concluded that society is still unaware of how cybercrimes work and how to prevent them from being the victims.

This research examines the issue of student disengagement in preventing cybercrimes. Traditional lecture-based teaching often distracts students, posing a significant educational challenge (Hu-Au et al., 2017). Traditional cybersecurity education methods are often inadequate as they heavily rely on passive learning techniques, such as lectures and static content, which fail to engage diverse audiences. Many current approaches lack interactivity and real-world simulations, making it difficult for learners to grasp the practical implications of cyber threats. Additionally, they often use overly technical language that alienates non-experts, lack personalization to different skill levels, and do not address the rapidly evolving tactics used by cybercriminals, resulting in outdated or incomplete training.

This lack of engagement contributes to various detrimental behaviours that hinder student advancement, including dissatisfaction, negative experiences, and dropout rates. As a solution, SWINDLERT is introduced as an educational entertainment, or edutainment, application that utilizes augmented reality to both entertain and educate. Researchers have found that it is crucial to stimulate students' interest and engagement with a topic when using virtual reality. For example, virtual reality can be used to educate students about cybercrime and its prevention, leading to increased spatial memory and enhanced understanding. Additionally, mobile gamification has been tailored for secondary school and university students, indicating that 67% of students complete online coursework on a mobile device, and 87% use a mobile device when searching for e-learning courses (Tamm, 2022). Given the current pandemic, augmented reality and mobile gamification are well-suited to help students prevent cybercrimes.

1.1 Research Background

Wood (1995; 2002) introduced the Human Firewall theory, emphasizing that user behaviour can undermine technical security measures. He suggested that organizations should raise. The study explored the inadvertent threats posed by human errors, which are often challenging to manage despite being easily made (Mohd et al., 2012). Based on Mary Douglas' cultural perspectives, they pinpointed critical threats and highlighted the impact of these perspectives on vulnerability. The study underscores the importance of incorporating cultural views into e-learning security strategies. Thus, four categories of cybercrimes are identified: cyber-trespass, cyber-deception, cyber-obscenity, and cyber-violence (Holt et al., 2018). Cyber-

https://dx.doi.org/10.24191/jcrinn.v10i1.497

trespass is a way to get into the computer infrastructure that does not belong to the person who did that cyber-trespass (Nicholas et al., 2019).

In other words, cyber-trespass involves any technique the attackers use intentionally and without authorisation access to targeted systems or computers. Examples of cyber-trespassing are data breaches, hacking, disruption of computer systems, altering the system, and many more. A survey has been conducted by Trend Micro Incorporation, resulting in 73% of the local organisations in Malaysia being most likely to be hacked in the next 12 months (Nurul, 2021). Cyber-deception, on the other way, involves hiding our networks, generates ambiguity and confusion in the face of the enemy's efforts to develop situational awareness, and influences and misdirects adversary perceptions and decision-making processes. According to the Malaysia Computer Emergency Response Team (MyCERT), the General Incident Classification statistics in 2023 and 2024 show that significant cases over that year were fraud, as shown in Fig. 1 and 2.

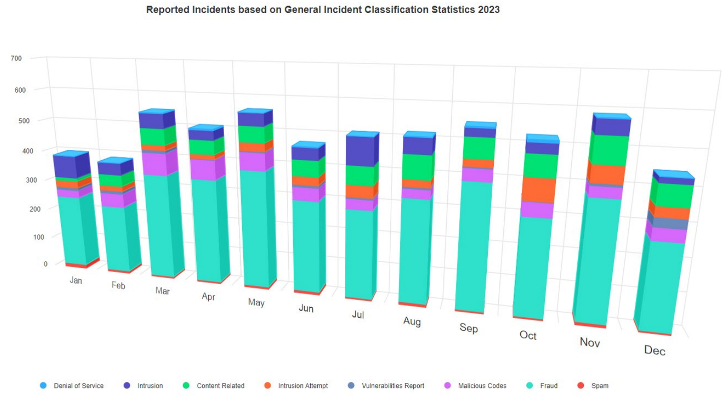


Fig. 1. Most reported incidents in 2023 were fraud cases (Coloured in turquoise)

Source: Malaysia Computer Emergency Response Team, CyberSecurity Malaysia (2023)

In comparing both statistics for fraud cases, there is a 13.6% increment from 2400 incidents (Jan – Aug 2023) to 2778 (Jan – Aug 2024). It demonstrates the necessity of teaching the next generation about cybercrime awareness to prevent them from falling for Internet fraud.

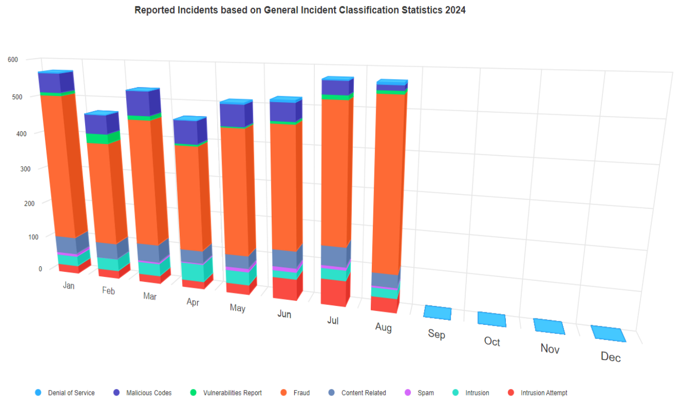


Fig. 2. Most reported incidents in 2024 were fraud cases (Coloured in orange)

Source: Malaysia Computer Emergency Response Team, CyberSecurity Malaysia (2024).

https://dx.doi.org/10.24191/jcrinn.v10i1.497

As outlined by Nandini (2020), cyber-obscenity encompasses the distribution and trading of sexually explicit materials in cyberspace, including but not limited to pornography and content related to the exploitation of children. This material is widely shared or uploaded online for global viewing or purchase. Additionally, in their scholarly work titled "Malaysia's Legal Response to Tackling the Crime of Online Child Pornography," Kirama Nasim and Juriah (2020) reported that Malaysia holds the third position in Southeast Asia for the possession and distribution of child pornography. Furthermore, cyber-violence, a distinct form of cybercrime, involves verbal or visual acts of harm through the Internet, such as threats, bullying, and harassment, which have the potential to cause psychological, emotional, or physical damage (Sung-Man Bae, 2021). These acts are commonly perpetrated through online chats, gaming platforms, and other digital mediums. Therefore, there is a need to educate the young generation about cybercrime awareness in an interactive way to engage the users.

The concept of edutainment, a blend of education and entertainment, has emerged to make learning more interactive and enjoyable for children who may find traditional education uninspiring. This approach traces its origins to the pedagogy of educator J. Komensky, who incorporated play into the learning process (Rusman & Ismail, 2020). Technological advancements have further propelled the evolution of edutainment, particularly by integrating virtual reality (VR) and augmented reality (AR). VR, introduced by Jaron Lanier in the 1980s, allows users to immerse themselves in computer-generated environments. AR, coined by Thomas Caudell and David Mizell in 1990, overlays digital data onto the real world (Elmqaddem, 2019). These technologies have significantly enriched educational experiences, making them more captivating and interactive.

2. EXISTING RELATED APPLICATION ON CYBERCRIME

Each system/application has its future, security measures and limitations, but their purpose is similar: educating users on cybersecurity prevention but not focusing on cybercrime. Table 1 summarises the comparisons between the five existing applications.

Table 1. Comparisons between existing related applications

Application	Features	Security Measures	Limitations
Interland (Google, 2017)	- Cross-platform on any device. Only required browser with Internet connection. - Easy tutorial understanding at the start of the game. - Friendly interface suitable for children.	- No register or login account is required. - Do not require any permission on the phone or other device.	- Progression of the game not saved. - No reward or experience point for each level. - No VR/AR features.
Cyber Security Quiz (Sana Edutech, 2021)	- Have both practice and timed quiz-style options. - Have an explanation for every question that is answered. - Can store favourite questions with the answer.	- No register or login account is required. - Do not require any permission to use the phone.	- Contains a lot of advertisements. - Need to pay for the pro version. - No reward or experience point for each quiz. - No VR/AR features.
WebME – The Cybersecurity Game (Mrigank Pawagi, 2018)	- Real interface practice on when to apply and how to prevent cybercrime. - The progression of the practice is saved - Friendly interface design.	- No register or login account is required. - Do not require any permission to use the phone.	- Cannot review the last practice that has been done. - No reward or experience point for each quiz. - No VR/AR features.

https://dx.doi.org/10.24191/jcrinn.v10i1.497

Learn Computer Security (Mohammed AlRiyami, 2021)	- Categorized information in computer security. - User friendly interface.	- No register or login account is required. - Do not require any permission to use the phone.	- Direct information about computer security without any quiz or game-based. - No approach was taken to attract the use of the application towards the user. - No VR/AR features.
Cyber Security Tycoon (Adrian Kopec, 2021)	- Save the progression of the game. - Easy tutorial understanding at the start of the game. - Compete each other with the ranking of the leaderboard.	- No register or login account is required, but only use the company name to rank between users. - Do not require any permission to use the phone.	- Only shows the information about the attack that happened towards the company without showing how to prevent it. - No VR/AR features.

The analysis presented in Table 1 indicates that current cybercrime applications do not incorporate VR or AR features. Additionally, these applications primarily focus on educating about cybersecurity and cybercrime, often lacking proper authentication measures. The absence of user verification in gaming raises significant security concerns, leaving games vulnerable to unauthorized access, cheating, and fraudulent activities. This lack of security compromises the gaming experience for legitimate players. It poses a risk of privacy breaches and data theft due to the exposure of personal data associated with user profiles. Furthermore, developers may face challenges implementing features such as multiplayer matchmaking and leaderboards without robust player verification, as unverified players can disrupt the competitive balance. Addressing these limitations, the SWINDLERT mobile gamification was specifically designed to enhance security measures in gaming applications.

3. METHODOLOGY

The Agile model depicted in Fig. 3 is highly effective for developing mobile applications to raise awareness about cybercrime. Its flexibility and iterative approach enable quick adaptation to evolving cybercrime trends and timely updates to counter emerging threats. Through short incremental cycles, known as sprints, developers can consistently incorporate user feedback, ensuring that the application remains current and impactful in educating users about the latest cybercrime tactics. This methodology also promotes rapid prototyping, allowing for swift testing and improvement of features to enhance user awareness and engagement with cybersecurity practices.

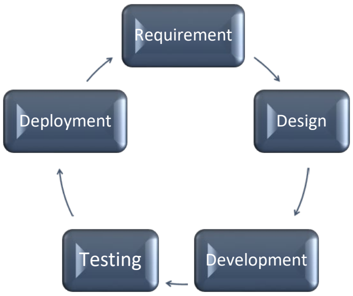


Fig. 3. Process of Agile Model

The first phase of the Agile model is the requirement analysis, which consists of identifying and analysing the problem statements and scope for the project development.

https://dx.doi.org/10.24191/jcrinn.v10i1.497

3.1 Requirement Phase

This preliminary survey is conducted to analyse cybercrime awareness and the effectiveness of edutainment via mobile gamification. 51 respondents are university students in Malaysia. Most respondents are from Universiti Sains Islam Malaysia (USIM), with 71%, and the remainder are from Universiti Teknologi Mara (UiTM), Universiti Sultan Zainal Abidin (UniSZA), Universiti Malaya (UM), Universiti Teknologi Malaysia (UTM), and other private institutions as summarise in Table 2.

Table 2. Institution demographic of the respondents

Institution	Percentage (%)
USIM	71
UiTM	8
UniSZA	6
UM	6
UTM	4
Others	6

In Table 3, two specific closed-ended questions were presented to the participants as part of the survey. The data revealed that 86% of respondents demonstrated awareness and knowledge about cybercrime, while 14% expressed uncertainty or lack of awareness. This indicates that university students may need to enhance their general knowledge and understanding of cybercrime. Furthermore, 88% of the participants recognized and acknowledged the significant rise in cybercrime incidents in recent years, as depicted in the summary provided in Table 3.

Table 3. Respondent feedback on two close-ended questions on cybercrime

Did you know what cybercrime is?	Percentage (%)	Do you know that cybercrime cases have increased in recent years?”	Percentage (%)
Yes	86	Yes	88
No	8	No	12
Maybe	6		

Fig. 4 illustrates the types of cybercrime by respondents. Phishing leads the most answered, followed by fraud, Internet, financial, card, and identity fraud.

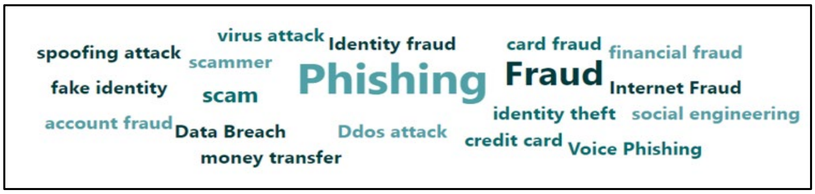


Fig. 4. 21% of respondents answered phishing for the types of cybercrime

Moreover, 45% of the respondents said they had experienced a cybercrime victim, as summarised in Table 3. This demonstrates that attackers can still obtain information obtained from respondents, and respondents do not safeguard their credential information. The top-ranked choices also correspond with the recent article on the Top 10 Trends in Phishing, which discusses emerging phishing methods such as Business Email Compromise (BEC) and vishing (phone-based phishing). The article underscores the increasing use of combined email and phone scams by attackers to deceive individuals, utilizing stolen credentials and spoofed domains to impersonate legitimate entities (SOCRadar, 2024). Furthermore, the article highlights the growing influence of generative AI in creating more convincing phishing emails, resulting in increasingly sophisticated attacks that are harder to identify.

Table 4. Respondent feedback on close-ended questions on the experience and edutainment approach

Have you experienced any cybercrime as a victim, or did your family experience it?	Percentage (%)	The edutainment (education and entertainment) approach to mobile gamification should be implemented so that students can simultaneously learn and play about cybercrimes.	Percentage (%)
Yes	45	Yes	98
No	55	No	2

In the following exploratory study, Table 4 reveals that 98% of the participants support the implementation of edutainment to enable students to learn and play about cybercrimes simultaneously. The majority also agree that informal interactive learning through mobile gamification involving virtual or augmented reality can effectively engage users, as detailed in Table 5. With virtual or augmented reality, educators can develop immersive learning environments that increase student engagement and make learning material more dynamic. Learning experiences can become more efficient and pleasurable due to this improved engagement, which can also promote motivation and knowledge retention.

Table 5. Respondent feedback on VR and AR

Virtual or augmented reality implementation can improve student engagement with mobile gamification.	Percentage (%)
Yes	98
No	2

In Fig. 5, 14% of the respondents suggested incorporating game elements into feature recommendations to enhance productivity and engagement. Other ideas included extending the duration and complexity of game levels, keeping it simple, and incorporating quiz segments. By integrating game elements such as progressive challenges, where users face increasingly difficult tasks, and reward systems like badges, points, or virtual currency, mobile edutainment can be improved, motivating users to continue engaging. Additionally, including leaderboards fosters friendly competition among players while unlocking content upon achieving learning objectives, which enhances the user experience. Educational puzzles and mini-games maintain user interest, while story-driven narratives captivate users and contribute to increased retention and engagement. In the proposed SWINDLERT development, mini-games with quizzes, varying difficulty levels, point systems, and leaderboard scores are implemented.

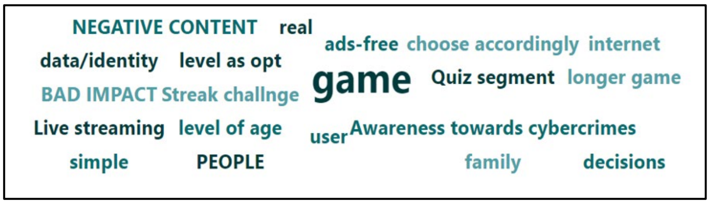


Fig. 5. Some feature recommendations that can be integrated into the gamification by respondents

3.2 Design Phase

Early visual representations are designed to validate design concepts. The use case diagram and the flowchart illustrate the system design, as shown in Fig. 6. It shows how the user acts as a player.

https://dx.doi.org/10.24191/jcrinn.v10i1.497

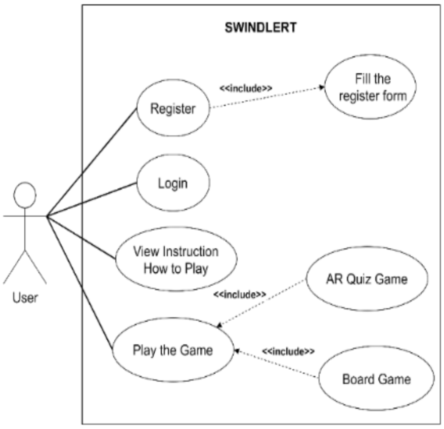


Fig. 6. Use Case of SWINDLERT

The flowchart in Fig. 7 presents the registration step of the application and gameplay in the SWINDLERT application. The user needs to register in the application to ensure that it saves the current progression of the user and benefits them to monitor their progress in the future.

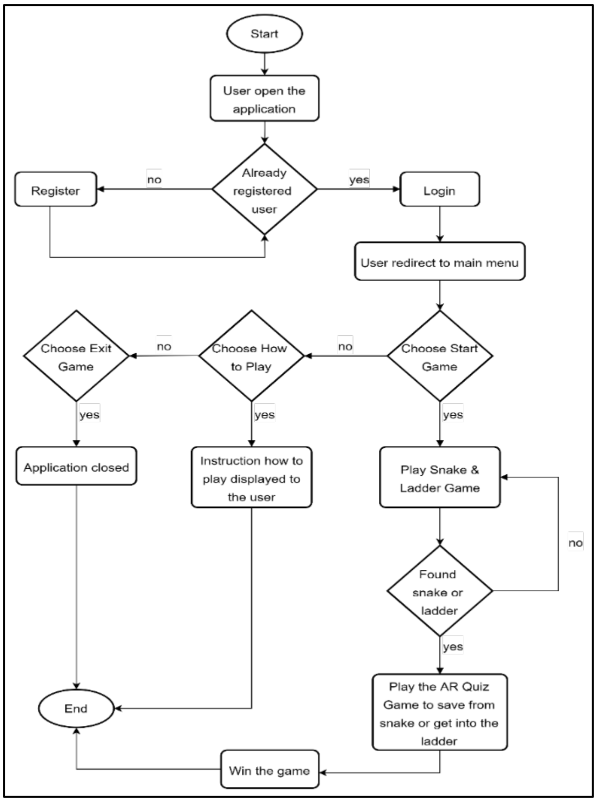


Fig. 7. Flowchart for SWINDLERT mobile application

https://dx.doi.org/10.24191/jcrinn.v10i1.497

3.3 Development Phase

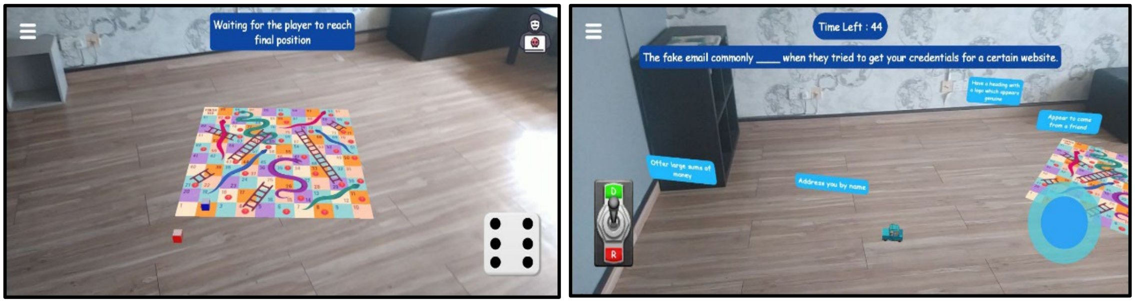
In the development phase of Agile methodology, Java programming language was used as the backend application, and it was designed with Extensible Markup Language (XML) in Android Studio. During this phase, the team iteratively codes and integrates AR features, ensuring real-time testing and feedback to refine interactions and enhance the user experience. This phase focuses on delivering functional AR components in short sprints, allowing developers to adapt to changing requirements and improve performance with each iteration.

3.4 Testing Phase

To ensure SWINDLERT's release is in optimal condition, feedback was collected from primary, secondary, and university students, focusing on functional and security authentication testing. During usability testing, users answered quizzes by controlling a car to select answers or received cybercrime information if they landed on an info spot. The game ends when the player or machine reaches the final position on the digital snake and ladder board. First-time players can access the How to Play section from the main menu for better understanding. To start, users scan a plane to render the board, then tap to roll the dice and move. Feedback was gathered from 53 respondents, and eight test cases were conducted for functional and security testing. Any failures identified will lead to redesign and improvement. Testing is carried out at SK Teluk Ketapang, Terengganu, and around Universiti Sains Islam Malaysia (USIM), focusing on functionality, usability, and security authentication.

4. RESULTS AND DISCUSSION

Based on the functional and usability testing results, SWINDLERT scored 87% in application functionality and 88% in security authentication testing. Additionally, 98% of respondents agreed that SWINDLERT effectively incorporated gamification elements such as levels, scores, and timers. Fig. 8 depicts the virtual dice in a 3D real environment, allowing players to answer quiz questions by manipulating the virtual gear.


Waiting for the player to reach final position

Time Left : 44

The fake email commonly ____ when they tried to get your credentials for a certain website.

Have a heading with a logo which appears genuine
Appear to come from a friend
Offer large sums of money
Address you by name
D
R

Fig. 8. Snake and ladder board game with the dice (right). Quiz-based while playing the SWINDLERT by controlling the gear and hitting the correct answer with the car

The cybersecurity applications listed in Table 1 do not require registration or login for security purposes and do not offer VR/AR features for gamification. Additionally, they do not provide rewards or experience points for completing quizzes. In Fig. 5, the game offers an interactive experience where players control a car to hit the correct answer. Upon reaching the last position, it provides cybercrime information or starts a quiz. During the quiz, players tap the scanned plane to spawn the car and answer, receiving feedback on whether their response is correct or wrong. It displays scores and reveals the correct answer if a mistake is made. Players compete against a Non-Player Character (NPC), with the first to the last position winning and earning a bonus score.

https://dx.doi.org/10.24191/jcrinn.v10i1.497

4.1 Gamification Elements

SWINDLERT incorporates three key gamification elements: levels, points, and a timer. Players are required to complete three progressively challenging levels, each with its own set of objectives. The beginner level focuses on general cybercrime prevention measures and logical thinking, while the intermediate level delves into various cybercrimes worldwide. The advanced level educates users about commonly used cybercrime attacks, providing detailed insights on identification and prevention techniques. The application underwent rigorous functional testing, including black box testing, to ensure compliance with the specified requirements. Moreover, a survey conducted during the National Science Week Carnival 2023 for Negeri Sembilan level revealed that 98% of respondents, spanning primary, secondary, and university students, thoroughly enjoyed playing SWINDLERT.

5. CONCLUSION AND RECOMMENDATIONS

Our primary contribution is a 3D immersive cybercrime awareness game that utilizes augmented reality to create a snake and ladder board concept-based user requirement study. SWINDLERT is a mobile gamification application that offers informal, interactive learning through three quiz levels (beginner, intermediate, hard) on cybercrimes. Gamification elements such as levels, points, and timers enhance the learning experience, with levels providing a seamless learning path. The game is designed for single players aged 8 and above who compete against a machine. It aims to reduce cybercrime incidents by promoting digital learning in a fun and practical manner. The functional and usability survey has yielded significant and convincing findings. This game can serve as a valuable tool for cybercrime awareness campaigns, aligning with the motto "Be Smart Stay Alert" of the Commercial Crime Investigation Department of The Royal Malaysia Police and engaging school and university students. Future work could expand the game by adding more questions, creating a multiplayer mode and making it available across platforms like iOS. Besides, the educational value of SWINDLERT can be enhanced by integrating adaptive difficulty levels on cybercrime prevention and personalized learning paths, making the experience more tailored to users with different skill levels. Moreover, incorporating real-time scenarios based on current cybercrime trends will ensure the content remains current and enhance the game's effectiveness in teaching practical prevention strategies.

6. ACKNOWLEDGEMENTS/FUNDING

The authors would like to acknowledge the Faculty of Science and Technology from Universiti Sains Islam Malaysia (USIM) for providing the facilities and support for this research.

7. CONFLICT OF INTEREST STATEMENT

The authors agree that this research was conducted in the absence of any self-benefits, commercial or financial conflicts and declare the absence of conflicting interests with the funders.

8. AUTHORS' CONTRIBUTIONS

Sakinah Ali Pitchay: Conceptualisation, methodology, project administration and writing-original draft; **AH Azni**: Methodology and investigation; **Farida Ridzuan**: Investigation, writing – review and editing; **Najwa Hayaati**: Testing and validation; **Muhammad Syahmi Imran**: Visualization and development.

https://dx.doi.org/10.24191/jcrinn.v10i1.497

9. REFERENCES

Adrian Kopec. (2021). Cyber Security Tycoon (Version 4.0). Mobile App. Google Play Store. https://apkpure.com/cyber-security-tycoon/com.AdrianKopec.CyberSecurityTycoon/download

Google. (2017). *Interland* (Version 1.0). [Mobile apps]. Web Educational Game. https://beinternetawesome.withgoogle.com/en_us

Holt, T. J., & Adam M. Bossler. (2012). 'Cybercrime', Oxford handbook topics in criminology and criminal justice. Online Edition, Oxford Academic, 2 June 2014. https://doi.org/10.1093/oxfordhb/9780199935383.013.002

Hu-Au, E., & Lee, J.J. (2017). Virtual reality in education: A tool for learning in the experience age. *International Journal of Innovation in Education*, *4*(4), 215. https://doi.org/10.1504/IJIIE.2017.091481

Lazic, M. (2023). January 17. “39 worrying Cyber Crime Statistics [updated for 2023]”. https://legaljobs.io/blog/cyber-crime-statistics/

Lege, R., & Bonner, E. (2020). Virtual reality in education: The promise, progress, and challenge. *The Jalt Call Journal*, *16*(3), 167–180. https://doi.org/10.29140/jaltcall.v16n3.388

Malaysia Computer Emergency Response Team. (2023). *Report incidents based on general incident classification statistics 2023.* https://www.mycert.org.my/portal/statistics-content?menu=b75e037d-6ee3-4d11-8169-66677d694932&id=2862eb40-2bc0-4b4e-90ed-07d4eef73b7b

Malaysia Computer Emergency Response Team. (2024). *Report incidents based on general incident classification statistics 2024*. https://www.mycert.org.my/portal/statistics-content?menu=b75e037d-6ee3-4d11-8169-66677d694932&id=23627097-41f2-4a21-8541-00a2b5c3352c

Mamadouh, V. (1999). Grid-group cultural theory: An introduction. *GeoJournal*, *47*(3), 395–409. https://doi.org/10.1023/A:1007024008646

AlRiyami M. (2021). *Learn Computer Security* (Version 1.0). [Mobile App]. Google Play Store. https://play.google.com/store/apps/details?id=com.app.learncomputersecurity

Pawagi M. (2018). WebME – *The CyberSecurity Game* (Version 1.0). [Mobile App]. Google Play Store. https://play.google.com/store/apps/details?id=com.thunkable.android.mrigankpawagi.WebME

N. H. M. Alwi and I. -S. Fan. (2012). Cultural views inclusive in e-learning risk analysis. *In IEEE Symposium on E-Learning, E-Management and E-Services* (pp. 1-6). IEEE Xplore. https://doi.org/10.1109/IS3e.2012.6414957

Nicholas, C & Gisela, B. (2019). Guarding against cyber-trespass and theft: Routine precautions from the hacking community. *International Journal of Cyber Criminology*, *13*(1), 101-106.

Nuradzimmah, D. (2022, March 14). Online scammers rake in RM1.6 billion, over 51,000 reports lodged in 2 years. *News Strait Times*. https://www.nst.com.my/news/nation/2022/03/779915/online-scammers-rake-rm16-billion-over-51000-reports-lodged-2-years

Nurul, S. (2021). 73% of local organizations likely to experience data breach. *The Malaysian Reserve*. https://themalaysianreserve.com/2021/08/25/73-of-local-organisations-likely-to-experience-data-breach/

Nurul, S. (2021, November 26). “Cybercrimes Went Up 99% in 2020”. *The Malaysian Reserve*. https://themalaysianreserve.com/2021/11/26/cybercrimes-went-up-99-in-2020/

https://dx.doi.org/10.24191/jcrinn.v10i1.497

Sana Edutech. (2021). *Cyber Security* (Version 1.09) [Mobile App]. Google Play Store. https://play.google.com/store/apps/details?id=com.sanaedutech.cyber_security

SOCRadar. (2024). *Top 10 Trends in Phishing Attacks (2024)*. https://socradar.io/top-10-trends-in-phishing-attacks-2024/

Sunbiz. (2021). April 26. "Identity Theft a Clear and Present Threat in Malaysia". *The Sun Daily*. https://www.thesundaily.my/business/identity-theft-a-clear-and-present-threat-in-malaysia-YL7793562

Tamm, S. (2022, January 8). "100 Essential E-Learning Statistics for 2022 - E-Student". *E-Student.org*. https://e-student.org/e-learning-statistics/

Wood CC. (1995). IS security awareness raising methods. *Computer Fraud & Security Bulletin*, June 13-15.

Wood CC. (2002). The human firewall manifesto. *Computer Security Journal*, *18*(1),15-18.

About the Authors

Sakinah Ali Pitchay, PhD is an Associate Professor in the Information Security and Assurance Program at Universiti Sains Islam Malaysia. She received her PhD in Computer Science from the University of Birmingham, UK, a Master's degree in Software Engineering from Universiti Teknologi Malaysia and a B.IT from Universiti Malaysia Terengganu. Her research interests include image enhancement, information security, and software engineering. She has numerous publications, won many innovation competitions with 54 medals and a Special Innovation Award in the Bank Innovation Challenge 2024. She achieved first place in the OIC-CERT Global Cybersecurity Award in UAE. She can be reached at sakinah.ali@usim.edu.my

Azni Haslizan, PhD is an Associate Professor in the Information Security and Assurance Programme at the Faculty of Science and Technology, Universiti Sains Islam Malaysia. She earned her PhD in Computer Science from Universiti Teknikal Malaysia Melaka, a Master's in Digital Communication from Monash University, Australia, and a Bachelor's in Computer Information Systems from Bradley University, USA. Currently serving as Deputy Dean (Research and Innovation) at USIM, she is widely recognized for her cryptography, data privacy, and wireless security expertise. She actively contributes to academia with numerous publications and 10 innovation medals to her credit. She serves on editorial boards, including the OIC-CERT Journal and the Journal of Machine Intelligence and Computing.

Farida Ridzuan, PhD is an Associate Professor in the Information Security and Assurance Program at the Faculty of Science and Technology, Universiti Sains Islam Malaysia. She earned her first-class B.Sc. (Hons.) in Computer Science from Universiti Teknologi Malaysia, an M.Sc. in Discrete Mathematics and Its Applications from the University of Essex, U.K., and a Ph.D. from Curtin University, Australia. Her research focuses on steganography and cryptography, with numerous publications in top-tier journals and RM2 million in secured research funding. She can be reached at farida@usim.edu.my

Najwa Hayaati Mohd Alwi, PhD is an Associate Professor in Information Security at Universiti Sains Islam Malaysia (USIM). She earned her PhD from Cranfield University in 2012 and is a certified 1Citizen trainer, ISMS Internal Auditor, and Digital Leadership Educator. She was a Malaysian Higher Education Teaching and Learning Council member and part of the Malaysia E-learning Council (2013-2018). Appointed as

Deputy Director for USIM’s Centre of Excellence for Teaching and Learning in 2021, her expertise spans information security, digital content, and socio-technical research. She is also a certified Cyber Defender Associate and Data Protection Officer and can be reached at najwa@usim.edu.my

Muhammad Syahmi Imran holds a Bachelor of Computer Science (Hons) in Information Security and Assurance from Universiti Sains Islam Malaysia. His expertise extends across web, mobile and game development, with a strong focus on leveraging technologies to create seamless user experiences and secure digital solutions. Passionate about innovation, he continuously seeks opportunities to integrate new tools and methodologies into his work. Muhammad Syahmi can be reached at syahmi.imran92@gmail.com

https://dx.doi.org/10.24191/jcrinn.v10i1.497