A PRELIMINARY CONCEPT ON CYBERSECURITY SKILL TRAINING FRAMEWORK FOR A CAPTURE-THE-FLAG GAME USING 5-STEP GAMIFICATION APPROACH

Khoo Li Jing[1,2], Maizatul Hayati Mohamad Yatim[2], and Wong Yoke Seng[2]

[1]School of Creative Media and Computing, University of Wollongong Malaysia, Jalan Kontraktor U1/14, Seksyen U1, 40150, Shah Alam, Selangor, Malaysia
[2]Faculty of Computing and Meta-Technology, Sultan Idris Education University, Tanjong Malim, Malaysia

ABSTRACT

This paper discusses about how to design a teaching and learning (T&L) framework for cyber security using game at higher education in Malaysia. The paper begins with literature review of key concepts and issues associated with Capture the Flag (CTF) and cybersecurity education framework, which led to the process of defining the CTF game to support the research aims. A version of CTF game was created using an open-source engine through Technology Pedagogy and Content Knowledge (TPACK) framework and five-step gamification approach, which was aligned to the course structure of cyber security courses offered in two institutions of higher education in Malaysia. The intended learning outcomes of the course were mapped into the CTF game features. The constructive alignment and the CTF game were then verified by subject matter experts. Pre and post-test are conducted to study the difference in students' performance. Mixed-mode research approach with quasi experiment will be used to study the difference among the treatment group. Data collection and analysis require supplement from follow-up interviews in order to complete the analysis of this T&L framework.

KEYWORDS

Capture the Flag, Cybersecurity, Game-based Learning, TPACK, Malaysia

1. INTRODUCTION

In the face of the growing cybersecurity skills gap, educators and researchers have explored innovative approaches to engage and train the next generation of cybersecurity professionals. One promising strategy is the use of Capture the Flag (CTF) competitions, which have been shown to effectively develop and assess cybersecurity skills [1] [2] [3]. However, the current forms of CTF exercises often require extensive technical knowledge or lengthy time commitments, making them inaccessible to a wider student audience [2]. By studying the knowledge and skill gap between Malaysia and other countries students, [1] there is a need to customize a CTF training framework that addresses these challenges and provides a more inclusive and engaging cybersecurity education experience among Malaysia undergraduates. To address this challenge, this study proposes incorporating principles of TPACK and gamification to create student-focused CTF experiences [4].

2. CYBERSECURITY EDUCATION AND SKILL BUILDING

The National Initiative for Cybersecurity Education (NICE), led by the National Institute of Standards and Technology (NIST) in the U.S. Department of Commerce, is a partnership between government, academia, and the private sector focused on cybersecurity education, training, and workforce development to promote a robust network and an ecosystem of cybersecurity education, training, and workforce development [5]. The curriculum designs in NICE Cybersecurity Workforce Framework are aimed to increase the impact of cybersecurity educational practice in depth and breadth [6]. Reflecting the trend to Malaysia, in the effort of leveraging Internet Communication Technology (ICT) to scale up quality learning across Malaysia as part of Malaysia Education Blueprint 2013-2025 (Ministry of Education Malaysia, 2013), there is a huge gap to be filled in order to prepare Malaysian technology students to be as competence as a cybersecurity defender. The Malaysian Administrative Modernization and Management Planning Unit (MAMPU) in 2015 embarked on the development of the Cyber Security Framework for Public Sector (Rangka Kerja Keselamatan Siber Sektor Awam - RAKKSSA). The RAKKSSA framework was developed to provide guidance to the public sector on managing cybersecurity protection and safeguarding government information and communication technology assets. However, the framework focuses on maintaining the current IT implementations but did not cover cybersecurity education in depth as a long-term solution to resist cybersecurity threats.

The challenge got tougher when Malaysia's world ranking in mathematics and science standards had increased but fell below the middle point of scale in Trends in International Mathematics and Science Study (TIMSS) and Programme for International Student Assessment (PISA) [7]. This is a vital issue which cybersecurity topics covers not only covering programming logics but also computational thinking and troubleshooting skills. An ISACA's studies (2015) found that there is a significant lack of trained security experts, which will result in a shortfall of as many as 1.5 million workers by 2020, according to Frost & Sullivan and the International Information Systems Security Certification Consortium ISC2 [8]. (ISC)2 has verified the skill gap persists in 2018 with 37% of the participating organizations experiencing lack of skilled cybersecurity personnel. Despite the investment flowing in with conferences and workshops to increase awareness, a constant upgrade in cybersecurity learners is needed to sustain the movement of defending cyber threats. Compared to 2016 studies by Cloud Passage, the top 10 U.S. computer science programs now require a cybersecurity course for graduation [9]. This indicates that there is an urgent need to inculcate innovative teaching and learning framework in cybersecurity education to fulfill the industry demand [10].

Educators find it challenging to reasonably standardize a core curriculum that students are expected to learn. Besides gaining experience at higher level of organizational policies and operations, learners have a series of fundamental technical knowledge such as malware analysis, information protection, system security, and network security etc. Personalized learning has shifted the learning behavior. Learners were used to being tested with replication of situations through multiple choice or short answers, but this phenomenon has gradually changed to virtual laboratories and online collaborations [11]. However, utilization of latest ICT facilities in Malaysia tertiary education are yet to be exerted [12]. Common T&L process of cybersecurity courses are still following the conventional learning methods in tertiary level education. Traditional approaches including lectures, coursework, live-through case studies, paper-based case study are often used to educate graduates [13] . The T&L process should stimulus learner's intrinsic motivation to explore the lesson that has been taught [14]. This is because learners still have to refer to the lecture notes during their post-learning session to understand the theories, thus being able to link the theory with the actual application. In other words, learners have to imagine within their mind just to be able to combine the concepts and theories learned without

clear learning medium during assessments. Despite having different student learning capabilities, to prove the efficiency, this research will also provide empirical evidence to support the use of CTF towards the T&L of cybersecurity. There is a need in increasing the interest of future Malaysian workforce in defending cyber threats, covering from home to organizational environment. Influenced by the increment of cybersecurity awareness but constrained by the gap of ICT skills between Malaysian students and other countries, this paper aimed to design a framework for cybersecurity education using CTF before moving into higher level of challenges.

2.1. Core Intelligence Domain Knowledge in Cybersecurity

Gardner's multi-intelligences theory suggests that individuals possess varying levels of different types of intelligence, including linguistic, logical-mathematical, spatial, bodily-kinesthetic, musical, interpersonal, and intrapersonal intelligence [15] Cybersecurity education should aim to develop multiple forms of intelligence in students, besides just focusing on technical skills. Effective cybersecurity professionals require a combination of technical skills such as system administration, programming, networking and cryptography while non-technical skills cover critical thinking, problem-solving, and peer communication [16]. For introductory-level cybersecurity training courses, the curriculum should initially emphasize the development of logical-mathematical intelligence, with other forms of intelligence, such as linguistic, spatial, and interpersonal, gradually incorporated as the training progresses.

The fundamental areas for developing cybersecurity skills include the core principles of information security, such as preserving confidentiality, maintaining integrity, and ensuring availability, as well as addressing common security threats and attack methodologies [16] [17]. Additionally, the supporting technologies and mechanisms required encompass cryptography, vulnerability identification, and recognition of defense controls. Capture the Flag events are an effective way to engage participants in applying these concepts in a simulated, hands-on environment. The challenge creator can reproduce the vulnerable scenario so that individuals can practice their skills in a monitored, safe environment [1][18].

The cybersecurity training framework can be designed to align with the multiple intelligences theory by incorporating learning objectives that cover a range of skills according to Bloom's Taxonomy. This hierarchy can progress from the lower-order abilities of applying cybersecurity knowledge to the higher-order skills of analyzing and evaluating security incidents. This research targets cybersecurity beginners and will focus on the lower and mid-level skills in Bloom's Taxonomy, such as comprehending security principles, identifying common vulnerabilities, and analyzing security threats. Unlike advanced CTF participants, the novice learners in this study will not need to develop customized tools for automated attacks, but rather concentrate on acquiring fundamental cybersecurity skills [17] [19].

2.2. Inclusive Approach for Diverse Learning Styes

While current focus is on improving technical skills, which aligns well with cybersecurity and CTF activities, the development of human-centric skills is equally important. Cybersecurity professionals require a combination of technical expertise and non-technical competencies like communication, teamwork, and creativity [20]. The gamification framework should strive to cultivate a holistic set of skills, catering to learners with diverse backgrounds and learning preferences. In diverse learning modalities, the 3 fundamental types of learners are: visual, auditory and kinesthetic learners. This research focuses on skill building especially on technical cybersecurity knowledge such as system administration, Linux commands, network traffic analysis, and cryptography. Soft skills in problem-solving, critical thinking, communication and collaboration are also emphasized after the core knowledge is established. In mapping the CTF

into TPACK framework and gamification guidelines, challenges exist in providing an inclusive and comprehensive skill training framework to cater wider range of learners while still maintaining the focus on cybersecurity skills.

In technological knowledge of TPACK, the nature of CTF provides flexibility in learning paths, allowing learners to explore, discover and self-pace their learning journey based on their individual learning preferences and interests [21] [22]. The integration of narrative elements and interactive features in the gamified CTF lessons could cater to the learning preferences of visual and auditory learners. Meanwhile, the hands-on, exploratory nature of the CTF activities would suit the needs of kinaesthetic learners. This approach aligns with the pedagogical knowledge component of the TPACK framework, as it incorporates diverse teaching strategies to address the learning styles of students. While the gamification elements may not encompass the full content knowledge specified by the TPACK framework, they can be leveraged to present various cybersecurity concepts through diverse formats, such as narrative-driven and visual-based approaches.

The effectiveness of the cybersecurity training framework will be evaluated through a multifaceted assessment approach. This will include pre- and post-tests to measure knowledge gains, observations of learner behaviours and engagement levels, as well as surveys to gather feedback on the overall learning experience. In CTF challenge design, the challenges in the CTF shall be structured to provide visual collaborative, reflective and narrative-based to cater different learning styles.

2.3. Capture the Flag (CTF)

Capture the Flag (CTF) competitions are events designed to test participants' cybersecurity skills through a series of challenges [23]. However, CTF are usually designed to cater for experienced participants, and may not be suitable for students at the secondary or tertiary level [4]. In the context of Southeast Asia countries such as Malaysia, CTFs have been primarily used for awareness raising purposes rather than as an integral part of cybersecurity education curriculum [1]. A typical CTF event involves a series of challenges that participants must solve in order to gain points in a limited time. The challenge categories vary from general coding, cryptography, web vulnerabilities, forensic analysis and reverse engineering [23]. Cybersecurity professionals and enthusiasts around the world host and participate in these events to test and improve their skills. Among the famous CTFs are Defcon, CSAW, HITCON, PlaidCTF and National Cyber League [1].

There has been a growing interest in utilizing Capture the Flag as a pedagogical tool in cybersecurity education [24] [23]. Advanced countries such as the United States, the NICE framework structures a holistic framework to foster a partnership between government, academia, and the private sector focused on cybersecurity education, training, and workforce development [25]. Without the support of an education framework for cybersecurity, Malaysian students are only exposed to formal Information Communication Technology (ICT) courses during their tertiary education. In the fast-evolving cybersecurity landscape, students will receive inconsistent knowledge and skills without a cybersecurity education framework. Compared to several countries implementing K12 education systems where cybersecurity concepts are introduced at elementary level, Malaysian students require to speed up their learning in both ICT skill and specialized cybersecurity topics within their university term [26].

A review of Southeast Asia cybersecurity landscape, the cybersecurity threat statistics are not at the critical level but there is a need in filling the workforce gap by fostering more Malaysian cyber defenders [27][9]. Cybersecurity scientists have moved the cyber landscape from Big Data

Analytics into Artificial Intelligence (A.I.). Defense Advanced Research Projects Agency (DARPA) has invested 3 years and more than USD 2 million in Cyber Grand Challenge (CGC) to develop an automated cybersecurity tool to take part against human players in a digital attack and defense competition (DARPA, 2014). However, cybersecurity education is still suffering from the gap in catching up the pace of fast changing cybersecurity landscape. Cybersecurity courses is not widely introduced across tertiary level institutions. Previous studies [28] [4] [1] have suggested that CTF competitions can increase student engagement and motivation in cybersecurity education, but the requirements to design a CTF framework that can be integrated into cybersecurity curricula and pedagogical approaches remain a challenge [29] [10]. After the success of CGC, studies on gamification of cybersecurity have been initiated in the United States on the effect of cybersecurity games to produce next generation of talent [23][30]. Studies showed that novices and individual who is lacked cybersecurity domain knowledge find it difficult to engulf the fast evolving and vast coverage area of cybersecurity [31][10].

However, the current design of CTF events may not be fully aligned with the learning requirements of students. Tertiary-level students often still require development of foundational computing knowledge, and traditional CTF events may exceed the skill level of this student population [32]. To address the shortcomings of traditional cybersecurity education and the limited use of CTFs, this research aims to develop a cybersecurity skills training framework that leverages the use of CTFs, underpinned by the TPACK model and 5-step gamification approach.

2.4. Experiential Learning in Capture-the-Flag Exercises

Experiential learning is a key aspect of cybersecurity education as it allows students to actively engage with security concepts through hands-on activities. Cybersecurity graduates are expected to begin their professional careers with strong technical expertise and skills, which they can then leverage to advance to managerial roles over time [33]. To achieve this, educators must design curricula that go beyond lectures and labs, and instead immerse students in simulated security scenarios where they can apply their knowledge and hone their skills [34]. One effective approach to experiential learning in cybersecurity is the use of Capture the Flag exercises. A typical CTF challenge requires participants to perform various security-related tasks such as vulnerability identification, exploit development, and incident investigations. Extensive practical experience allows learners to reinforce the technical knowledge and skills they have gained through other educational activities.

2.5. Technology Pedagogy and Content Knowledge (TPACK) Framework

Mishra and Koehler's Technological Pedagogy and Content Knowledge framework [1] can be a suitable model to design the CTF framework. TPACK emphasizes the complex interplay of 3 key components of knowledge: content, pedagogy, and technology, and the intersection between them. For cybersecurity education, the content knowledge includes the fundamental concepts and techniques such as cryptography, networking, programming; the pedagogical knowledge involves selecting appropriate teaching methodologies; and the technological knowledge encompasses the tools and platforms used in the learning process; the technology knowledge includes using a CTF platform, developing CTF challenges and automating the evaluation and scoring process.

Emerging research suggests that for CTF to be an effective educational tool, the competition should be designed with a focus on promoting student engagement and learning, rather than just technical mastery [4]. By integrating the TPACK framework into the design of the CTF-based training, the framework can ensure that the technical skills development is balanced with appropriate pedagogical approaches and leverages relevant technological tools. In this research, the academic, CTF creator, and student perspective will be considered to develop the integrated

framework. The academic will focus on the content and pedagogical knowledge, the CTF creator will contribute the technological and content knowledge, and the student perspective will ensure the framework meets the learning needs and motivations of the target audience.

2.6. Five-Step Gamification

Huang and Soman's five-step gamification framework can be a useful approach to guide the design of the CTF-based training [35]. The steps include: 1) Understanding the target audience and their characteristics; 2) Defining the learning objectives; 3) Structuring the experience; 4) Identifying the resources; and 5) Applying gamification elements.

In the first step, the target audience of tertiary-level students in learning cybersecurity would be profiled to identify their prior knowledge, learning preferences, and motivational drivers. It can be achieved by providing a pre-test assessment. The learning objectives in the second step would be aligned with the TPACK framework to ensure technical mastery, pedagogical effectiveness, and technological integration. This requires the close collaboration between academic and the CTF challenge creators. The third step of structuring the experience would involve designing the CTF challenges with appropriate difficulty levels, feedback mechanisms, and peer collaboration and competition. Academics can adopt the formative assessment and the CTF creator can perform real-time monitoring of the learner's progress. The fourth step of identifying resources would encompass the selection of the CTF platform functions, development of challenge scenarios, and facilitation of the learning activities. Finally, the fifth step of applying gamification elements would incorporate game-like features such as scoring, rewards and recognitions, and progress tracking to enhance student engagement and motivation.

By integrating the 5-step gamification into TPACK-aligned CTF design, the CTF-based training can be designed to effectively engage students, scaffold their learning, and evaluate their progress. Learners can leverage the benefits of gamified learning to develop well-rounded cybersecurity knowledge and skills. To validate the effectiveness of the proposed framework, empirical studies can be conducted to measure the impact on student learning outcomes, engagement, and motivation. The framework can then be refined based on the findings and feedback from academics, industry experts and experienced CTF organizers.

3. RESEARCH OBJECTIVES

This research aimed to design and develop a cybersecurity skill training framework for teaching and learning (T&L) cybersecurity in Malaysia through a Capture the Flag (CTF) game. The proposed framework will incorporate the TPACK model and the 5-step Gamification model to design and develop the CTF-based cybersecurity training. Efficiency in learning cybersecurity within the limited time becomes an important matter. Undergraduate degree students have an average of four years studies to acquire knowledge and skills on cybersecurity, before entering the workforce associated to cyber and information technology sector. The problems identified were:

1. Malaysia is lacked a framework for T&L cybersecurity
2. Malaysian students suffer a skill gap in cyber security area
3. There is no guideline for Malaysian educators in delivering cybersecurity modules

A CTF game has been recognized as the game to support this skill training framework. This game is embedded with real time gameplay, which possesses generic game characteristics, such as avatar, scoring system, instant feedback, social connections and reward, affording lecturers or

instructors to monitor learning progress. The game can capture real time data for use in analyzing the cybersecurity skill training framework. To attain the research aim, the following research objectives are formulated in this study:

1. To design a CTF-based cybersecurity training framework using the TPACK and 5-step Gamification models.
2. To assess the effectiveness of the proposed CTF-based cybersecurity training framework in improving cybersecurity knowledge and skills among Malaysian undergraduate students.
3. To compare the effectiveness of the proposed CTF-based cybersecurity training framework with traditional classroom-based cybersecurity training.

Research questions are derived from the identified problems and research objectives:

1. Is there a statistically significant difference in students' performance in acquiring fundamental cybersecurity concepts before and after learning through a CTF game?
2. Is there a statistically significant difference in students' performance in acquiring types of cybersecurity threats before and after learning through a CTF game?
3. Is there a statistically significant difference in students' performance in acquiring cryptography concepts before and after learning through a CTF game?

4. METHODS

The CTF training framework is based on a constructive mapping of Introduction to Security or similar module in 2 universities. An initial prototype will be tested and evaluated by academics and subject matter experts. Pilot test evaluation with students from different cohort and respective assessor will be followed up.

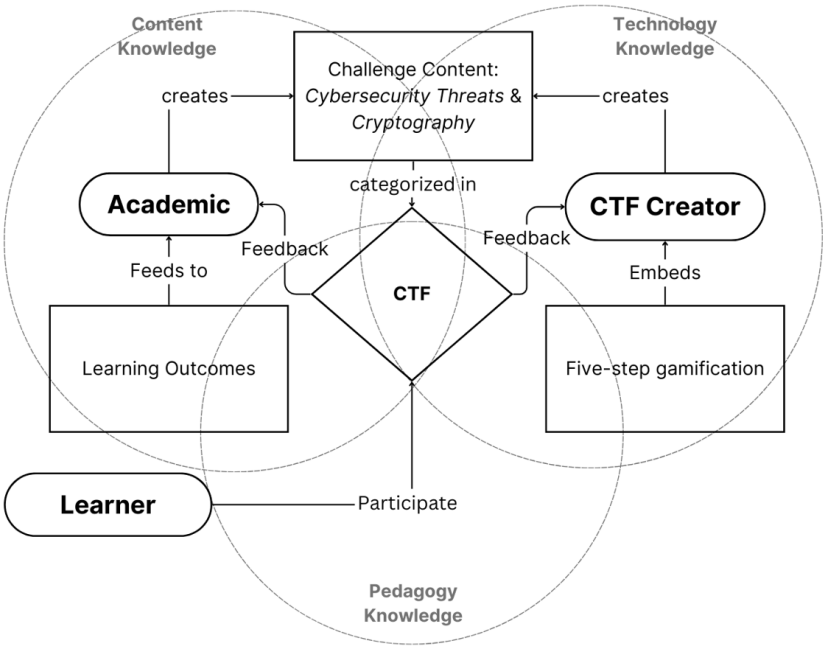

Figure 1. The conceptual framework of the digital game platform where CTF is embedded in the TPACK and Gamification models

The proposed framework suggests a unique approach to cybersecurity education and training, centered around the cybersecurity concepts of fundamental concepts, types of threats, and

cryptography, along with game design elements. This research will be using a combination of quantitative and qualitative methods. For the quantitative approach, a quasi-experimental design will be used to assess the effectiveness of the proposed CTF-based cybersecurity training framework. The experiment involves involve a pre-test and post-test design to measure the students' knowledge gain in cybersecurity concepts after using the CTF-based training framework. Interviews and focus groups will be used for the qualitative approach to gather in-depth feedback on the proposed framework from subject matter experts, lecturers, and students.

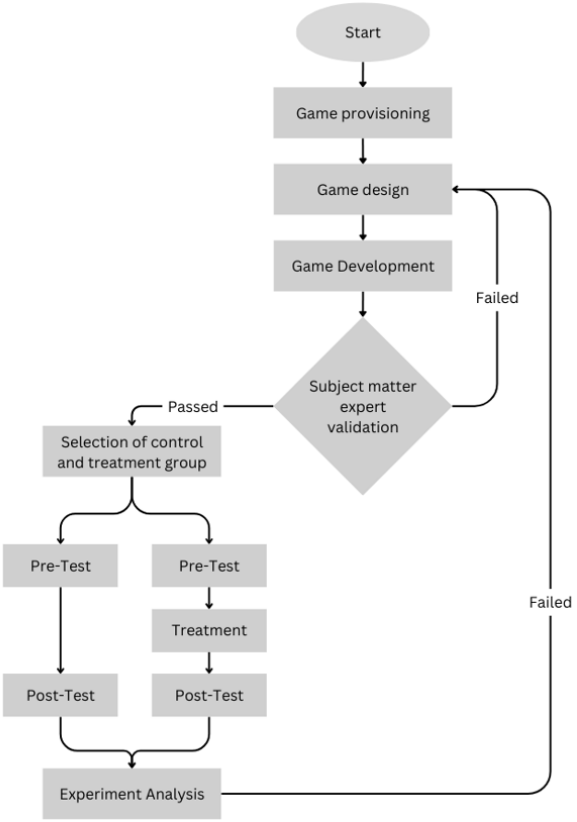

Figure 2. The research design using quantitative approach involving expert validation of the skill training framework

5. METHODS

The participants for this study will be undergraduate university students majoring in software engineering, computer science, or information technology programs at selected universities in Malaysia. The participants will be randomly assigned to either the experimental group, which will use the proposed CTF-based cybersecurity training framework, or the control group, which will receive traditional classroom-based cybersecurity training. The participants are expected to be between 18-25 years old, with no prior formal training in any cybersecurity domains.

Recruiting sufficient number of participants for this study may prove challenging due to the limited enrollment in an academic year for Malaysia cybersecurity programs. As a result, the participants will likely be drawn from a pool of students enrolled within the same cohort, who will then be randomly assigned to either the control or experimental group.

The duration of the research and skill training will take place over a 10-week period. To reduce validity threats on the control group, participants in the experimental group will be required to

sign a non-disclosure agreement, prohibiting them from discussing the details of the experiment with individuals outside the study. They will access the CTF platform using unique identifiers linked to their university accounts. Participants' access time, IP addresses, and game progression data will be tracked to ensure reliable data collection. This will help maintain the integrity of the study and prevent any potential contamination of the control group by the experimental group participants. The research team will closely monitor the participants' engagement and performance throughout the 10-week training period.

6. RESEARCH INSTRUMENTS

cybersecurity knowledge. This is to study if there is a statistically significant difference in the students' performance before and after using the proposed CTF-based cybersecurity training framework, as compared to the control [1] [36] group. The pre-test and post-test will consist of 20 multiple-choice questions covering the three key cybersecurity concepts: fundamental concepts, types of threats, and cryptography.

Additionally, semi-structured interviews and focus group discussions will be conducted with the experimental group participants, instructors, and subject matter experts to gather in-depth qualitative feedback on the proposed CTF-based cybersecurity training framework. The interviews will be conducted during the pilot test and the actual experiment. This qualitative data will provide valuable insights into the participants' experiences, perceptions, and opinions regarding the effectiveness and usability of the framework. The interviews and focus groups will explore aspects such as the learning experience, engagement with the CTF game, application of cybersecurity concepts, and overall satisfaction with the training approach. The feedback collected from these sessions will help the researchers identify areas for improvement and refine the framework to better meet the needs and expectations of the target audience.

7. EXPECTED OUTCOME

The expected outcome of this research is a novel CTF-based cybersecurity training framework that can effectively improve cybersecurity knowledge and skills among undergraduate students. CTFs are usually conducted in limited time such as one-day events, but this research proposes an integrated training framework that incorporates the CTF game as a core component over an extended duration of 10 weeks. This extended duration is expected to provide more opportunities for students to engage with the CTF game, explore cybersecurity concepts, and develop their skills. The control group may have exposure to other CTF competitions through extra-curricular activities, but it is expected that the experimental group, who will use the proposed CTF-based training framework, will demonstrate a significantly higher performance level in acquiring cybersecurity knowledge and skills. This is because the customized CTF game is embedded within the TPACK and gamification models, which are tailored to the specific research objectives. Both the control and experimental groups will undergo the same post-test, covering similar topics in the pre-test, at the end of the study to measure the effectiveness of the proposed framework. For further analysis, the experimental group's in-game performance data will be correlated with their pre-post test scores to establish the relationship between CTF game engagement and improvement in cybersecurity knowledge. This comprehensive assessment will provide valuable insights into the effectiveness of the proposed CTF-based cybersecurity training framework in enhancing students' cybersecurity skills and knowledge

8. CONCLUSION

Game-based Learning is not a novel concept in the education sector [37]. This paper aims to extend the use of GBL to develop specialized profiles for students in Malaysia, particularly in the cybersecurity field. The study's outcome will contribute to enhancing cybersecurity education. Educators will be guided on the key areas to emphasize in curriculum design and delivery. Learners who adopt this learning approach will not only acquire cybersecurity skills and knowledge but also develop valuable employability skills.

While there are existing studies on games for Science, Technology, Engineering, and Mathematics education, including cybersecurity [30][38], this research specifically targets Malaysian cybersecurity students to help them become self-sustaining in adapting to the dynamic cyber threat landscape. The roadmap of a cybersecurity practitioner typically starts from the front-line roles, such as security testers and incident responders, before progressing to managerial positions like department leaders and policy makers. This study aims to extend the application of GBL to a specialized industry that operates on diverse platforms, requiring logical reasoning and operations.

The study will be supported by creating and assessing the logical-mathematical intelligence from the seven core intelligence profiles proposed by Gardner [39]. This research will also empower educators to focus on the skill development process and assessments, helping students achieve the industry's needs and expectations.

ACKNOWLEDGEMENTS

The authors would like to thank the Sultan Idris Education University for the financial and other research support for this research.

REFERENCES

[1] A. D. B. Ibrahim, A. H. A. Hanafi, H. Rokman, M. N. A. Zawawi, Z. Ibrahim and F. A. Rahim, "Comparative Analysis on Student's Interest in Cyber Security among Secondary School Students using CTF Platform".

[2] C. Scherb, L. B. Heitz, F. Grimberg, H. Grieder and M. Maurer, "A Serious Game for Simulating Cyberattacks to Teach Cybersecurity".

[3] A. Horcher, "Shall We Play a Game? : Building Capture the Flag Games for Non-Traditional Players".

[4] D. Szedlak and A. M'manga, "Eliciting Requirements for a Student-focussed Capture The Flag".

[5] B. D. Caulkins, K. Badillo-Urquiola, P. Bockelman and R. D. Leis, "Cyber workforce development using a behavioral cybersecurity paradigm".

[6] C. Paulsen, E. McDuffie, W. Newhouse and P. Toth, "NICE: Creating a Cybersecurity Workforce and Aware Public".

[7] N. M. Nor, W. K. H. W. Ramli, N. E. Jauhari and M. Mahmud, "An Analysis of Mathematics Achievements Based on Student Engagement and Attitude in Asean Countries Compared with TIMSS 2011 and TIMSS 2015".

[8] "ISC2 Insights".

[9] F. H. Sohime, R. Ramli, F. A. Rahim and A. A. Bakar, "Exploration Study of Skillsets Needed in Cyber Security Field".

[10] C. Daniel, M. Mullarkey and M. Agrawal, "RQ Labs: A Cybersecurity Workforce Skills Development Framework".

[11] A. Moldovan and I. Ghergulescu, "Leveraging Virtual Labs for Personalised Group-based Assessment in a Postgraduate Network Security and Penetration Testing Module".

[12] Z. Mahmood, A. H. A. Hashim, M. A. Abuzaraida, O. O. Khalifa and M. Mustafa, "Teaching Lab-based Courses Remotely: Approaches, Technologies, Challenges, and Ethical Issues".
[13] A. Ahmed, K. Lundqvist, C. Watterson and N. Baghaei, "Teaching Cyber-Security for Distance Learners: A Reflective Study".
[14] J. M. Keller, "First principles of motivation to learn and e3-learning".
[15] R. J. Sternberg et al., "The Cambridge Handbook of Intelligence".
[16] G. Jin, M. Tu, T. Kim, J. Heffron and J. White, "Evaluation of Game-Based Learning in Cybersecurity Education for High School Students".
[17] H. Santos, T. Pereira and I. Mendes, "Challenges and reflections in designing Cyber security curriculum".
[18] J. Idziorek, J. A. Rursch and D. Jacobson, "Security across the curriculum and beyond".
[19] J. Vykopal, P. Čeleda, P. Šeda, V. Švábenský and D. Tovarňák, "Scalable Learning Environments for Teaching Cybersecurity Hands-on".
[20] T. Crick, J. H. Davenport, P. Hanna, A. Irons and T. Prickett, "Overcoming the Challenges of Teaching Cybersecurity in UK Computer Science Degree Programmes".
[21] V. Švábenský, P. Čeleda, J. Vykopal and S. Brišáková, "Cybersecurity knowledge and skills taught in capture the flag challenges".
[22] S. Chang, K. Yoon, S. Wuthier and K. Zhang, "Capture the Flag for Team Construction in Cybersecurity".
[23] K. Leune and S. J. Petrilli, "Using Capture-the-Flag to Enhance the Effectiveness of Cybersecurity Education".
[24] A. O. Affia, A. Nolte and R. Matulevičius, "Integrating Hackathons into an Online Cybersecurity Course".
[25] W. Newhouse, S. Keith, B. Scribner and G. Witte, "National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework".
[26] A. F. M. Ajis, R. Ahmad, S. Osman and I. Ishak, "Catalyst of Information Security in Malaysia Higher Learning Institutions".
[27] R. Dillon, "The Future of Cybersecurity in Southeast Asia along the Maritime Silk Road".
[28] T. J. Burns, S. C. Rios, T. K. Jordan, Q. Gu and T. Underwood, "Analysis and Exercises for Engaging Beginners in Online CTF Competitions for Security Education.".
[29] B. M. Dioubate, W. R. W. Daud and W. Norhayate, "Cyber Security Risk Management Frameworks Implementation in Malaysian Higher Education Institutions".
[30] M. Gáliková, V. Švábenský and J. Vykopal, "Toward Guidelines for Designing Cybersecurity Serious Games".
[31] M. Nkongolo, N. Mennega and I. V. Zyl, "Cybersecurity Career Requirements: A Literature Review".
[32] M. Ellis, L. Baum, K. Filer and S. H. Edwards, "Experience Report: Exploring the Use of CTF-based Co-Curricular Instruction to Increase Student Comfort and Success in Computing".
[33] M. Nkongolo, N. Mennega and I. V. Zyl, "Cybersecurity Career Requirements: A Literature Review".
[34] J. Mirković, A. Tabor, S. S. Woo and P. Pusey, "Engaging Novices in Cybersecurity Competitions: A Vision and Lessons Learned at ACM Tapia 2015".
[35] T. A. Nguyen and H. Pham, "A Design Theory-Based Gamification Approach for Information Security Training".
[36] M. Azzeh, A. M. Altamimi, M. G. Al-Bashayreh and M. Aloudat, "Adopting the Cybersecurity Concepts into Curriculum The Potential Effects on Students Cybersecurity Knowledge".
[37] T. Awojana, T. Chou and N. Hempenius, "Review of the Existing Game Based Learning System in Cybersecurity".
[38] S. Karagiannis and E. Magkos, "Engaging Students in Basic Cybersecurity Concepts Using Digital Game-Based Learning: Computer Games as Virtual Learning Environments".
[39] M. Malatesta and Y. Quintana, "Multiple Intelligences and quotient spaces".

AUTHORS

Khoo Li Jing is an academic in University of Wollongong Malaysia. His research interests are in game-based learning, andcybersecurity skill development. He is completing his Ph.D. in Game-Based Learning at Sultan Idris Education University, Malaysia. He completed his M.Sc. in Computer Network Security from Liverpool John Moores University, U.K., and his Bachelor in Information Systems from Tunku Abdul Rahman University of Management and Technology, Malaysia.

Maizatul Hayati Mohamad Yatim is an associate professor of Human-Computer Interaction in Computing Department, at Sultan Idris Education University, Malaysia. Her research interests are specifically on game design and development, game usability, and game-based learning. She received her Ph.D. in Computer Science from Otto-von-Guericke University of Magdeburg, Germany, her M.Sc. in Information Technology, and her Bachelor in Information Technology both from Northern University of Malaysia.

Ts. Dr. Wong Yoke Seng is the Deputy Director (Data & Strategic Planning), of the Research Management Centre in Universiti Perguruan Sultan Idris. His specialisation is in Game-based Learning. He received a B.S degree in Information System Engineering from Campbell University and M.S.C in Computer Game Technology from Liverpool John Moores University, UK. He has been teaching game design and game programming related subjects for over 20 years and actively involved in game related research projects. His current research involves using computer game as learning tool for learning object-oriented programming in tertiary level and his current interests are gamification, game design, data structures & algorithms and object oriented system analysis and design. Malaysia