Migration Letters

Volume: 20, No: S4(2023), pp. 1039-1049

ISSN: 1741-8984 (Print) ISSN: 1741-8992 (Online)
www.migrationletters.com

Unveiling Cybersecurity Factors in Thailand's Metaverse Adoption

Noppadon Ratanavaraha[1], Chetneti Srisa-An[2]

Abstract

This research aimed to identify and evaluate the Cybersecurity Factors in Thailand's Metaverse Adoption by adopting a mixed-method approach. The qualitative study categorized participants into four groups, which comprised 15 experts in cybersecurity and the Metaverse. Data collection involved e-Focus groups combined with digital surveys and employed Fuzzy Set Theory for data analysis. In the quantitative study, data were collected from 800 Meta users in Thailand using a digital survey and Exploratory Factor Analysis for data analysis. In the qualitative conclusion, the analysis, utilizing the Fuzzy Technique with a 0.917 threshold, identified key components. In the quantitative conclusion, the research encompassed 800 Meta users in Thailand. Exploratory Factor Analysis confirmed a variable set that accounts for 83.885% of the total variance, categorized into four key components. Additionally, eleven factors were consolidated into a unified entity called 'Cybersecurity Factors in Thailand's Metaverse Adoption' (CFTM).

Keywords: *Metaverse, Cybersecurity, Exploratory Factor Analysis, Digital survey, Fuzzy Set Theory.*

Introduction

The Metaverse, inspired by the 1992 novel "Snow Crash," is rapidly gaining traction due to technological advancements and the increased demand for virtual experiences, notably during the COVID-19 pandemic. Mark Zuckerberg's announcement of Facebook's involvement in the Metaverse has further fueled its growth. Thailand has moderate readiness for the Metaverse Economy, spanning government, private sectors, academia, and infrastructure. However, the country faces significant cybersecurity challenges in its digital landscape, particularly among its numerous internet users, including teenagers. Thailand's National Cybersecurity Strategy 2017-2021 addresses key concerns but lacks specific focus on Metaverse cybersecurity.

Thailand's readiness for the impactful Metaverse Economy, bridging reality and virtual worlds through platforms like "Second Life," is moderate but evolving across government, private sectors, academia, and infrastructure. Consumer participation holds economic significance in this next phase of the digital economy (Thammajai, 2021). Thailand is confronted with diverse threats arising from social media technology. The number of internet users has risen to nearly 40 million, encompassing over 24 million individuals aged six and above. Notably, teenagers account for approximately one-third of these users. Weekly internet usage averages 41.4 hours, majorly through smartphones. Facebook and LINE are prominent environments.

[1] College of Digital Innovation Technology, Rangsit University, Pathum Thani, Thailand, noppadon.r64@rsu.ac.th
[2] College of Digital Innovation Technology, Rangsit University, Pathum Thani, Thailand, chetneti.s@rsu.ac.th

Thailand's National Cybersecurity Strategy 2017-2021 tackles eight key concerns, enhancing trust, securing information infrastructure, bolstering the digital economy, promoting responsible online use, countering cybercrime, and highlighting innovation. It evaluates readiness, potential issues, and cyber threats across legal, technical, personnel, system, and investigative dimensions (Office of the National Security Council, 2017). Nonetheless, scant focus has been directed towards exploring the cybersecurity dimensions linked with incorporating the Metaverse in Thailand. This research seeks to pinpoint and assess the cybersecurity elements that impact the acceptance of the Metaverse in the Thai setting.

Literature Review

Skinner et al. (2006) introduced "meta-information," highlighting privacy risks in Metaverse applications like Second Life. Leenes (2008) focused on privacy within Second Life, underlining virtual world privacy issues. Yang et al. (2022) explored blockchain-based games like 'Axie Infinity,' showcasing Metaverse diversity. Lee et al. (2021) emphasized early privacy considerations in Metaverse design. Mufti et al. (2018) developed a security readiness model for broader Metaverse security. Acquisti and Gross (2006) probed privacy on Facebook, shedding light on virtual space privacy.

Duan et al. (2021) presented CUHKSZ Metaverse using blockchain, highlighting its potential. Lim et al. (2022) surveyed Metaverse adoption, enriching our understanding. Dionisio et al. (2013) highlighted the transformative Metaverse potential. Irfan et al. (2019) tailored an IT readiness model for higher education. Sardjono (2019) provided a readiness model methodology. The Metaverse roadmap (2016) outlined Metaverse scenarios. Jon Radoff's framework (2021) structured Metaverse layers. In "Critical Factors of Readiness Model for Metaverse Security and Privacy Adoption" and "Security and Privacy Factors for Metaverse Adoption in Thailand," researchers used Fuzzy, EFA, and CFA techniques to identify essential elements in Metaverse security, privacy, and readiness. These studies contributed to readiness models, emphasizing the importance of addressing key factors for successful Metaverse adoption and regulation, especially in security and privacy contexts.

The Metaverse, a convergence of real and virtual worlds, presents both challenges and opportunities. User authentication remains a hurdle requiring seamless connectivity (Ning 2021). Kim's research highlights the integration of the Metaverse in education, particularly its role in enhancing cybersecurity education (Kim, 2021). Natalia P's work underscores the effectiveness of virtual reality in complex learning (Poddubnaya 2020). Addressing the Metaverse involves considerations of social acceptance, security, privacy, trust, and accountability. Understanding user behavior and mitigating risks like privacy breaches are crucial. Biometric data from VR devices necessitates accuracy and system security improvements (Lee, L.-H. 2021). Joo-Eon JEON's study explores how user experience-driven design innovation influences user-platform relationships within the Metaverse, highlighting factors like identity, attractiveness, novelty, usability, and interaction, which enhance platform identity and commitment (Jeon, J. E. 2021; Tongvijit, 2023).

The role of the digital landscape in education and skill development, particularly for youth, is expanding. However, this shift brings both societal benefits and challenges, including cybersecurity concerns in emerging mirror worlds. Managing data overload is crucial for maintaining balanced human interactions (Channuwong, 2018; Metaverseroadmap 2016). Kim defines the Metaverse as a seamless blend of virtual and real internet worlds. Edge computing addresses data privacy concerns and complements cloud solutions for enhanced Metaverse security (Lee, 2021). Assisted Reality, such as smart glasses, improves screen interaction, facilitating online retail testing. Virtual Reality, facilitated by VR glasses, connects users to digital realms. Huansheng Ning et al.

classify Metaverse dimensions, encompassing social and hyper Metaverse spatial attributes (T., K. 2021; Ning, 2021).

Radoff's framework categorizes the Metaverse into seven tiers: infrastructure, human interface, decentralization, spatial computing, creator economy, discovery, and experience. Each layer addresses key aspects, from infrastructure and user control to blockchain tech and immersive challenges, potentially surpassing the real world (Radoff, 2021). Meanwhile, Sebastian (2023) highlights substantial Metaverse cybersecurity risks, including data privacy, access, blockchain-based NFTs, and more. The research also offers mitigation strategies to address these risks, ensuring a more secure Metaverse environment.

Channuwong et al. (2023) and Kim (2021) emphasized data protection and the educational potential of the Metaverse, particularly in virtual Reality, highlighting its positive impact on learning outcomes. Evangelista (2010) and Ning et al. (2021) identified five critical open issues in the Metaverse, including security, privacy, ethics, interaction, computation, and standardization.

Große et al. addresses methodological challenges in studying critical infrastructure protection (CIP), particularly CIP governance, using the Swedish case of Styrel, a complex electricity prioritization system. It employs document analysis, interviews, and surveys, highlighting obstacles such as information sharing, methodological limitations, policy uncertainty, and data quality issues. The study underscores the importance of fostering collective intelligence and mutual understanding among CIP stakeholders while developing innovative methods to overcome these challenges in research and practice (Große, 2021).

In the field of legislation, the researcher has meticulously gathered a wide range of pertinent Thai legal clauses. This compilation is based on law-related announcements and data collected by the ICT Law Center, covering various potentially relevant laws. In total, this comprehensive collection consists of 39 distinct legal provisions (ETDA, 2021). Leenes (2009) pointed out about the regulation of privacy in the Metaverse. This desire for privacy diverges from second life's fundamental qualities, which emphasize social interaction, transparency, and openness. Consequently, alternative methods of control are imperative. While the environment facilitates the exchange of information about residents, shifts in governance structures are emerging. Internal governance could pave the way for more standardized approaches and resident involvement.

Additionally, robust regulatory tools like law enforcement and the justice system are available. Insights garnered from real-world experiments and governance theories hold considerable value. The safeguarding of fundamental rights, including privacy, necessitates societal commitment (Leenes, 2008; Leenes 2009). Manasan (2021) categorized laws related to the Metaverse as follows: 1) Platform regulations. 2) Laws pertaining to blockchain, cryptocurrency, and NFTs. 3) Intellectual property legislation. 4) Regulations for the protection of personal data. 5) Fraud prevention measures.

Lee's study delves into the adoption dynamics of Metaverse services, including AR, lifelogging, mirror worlds, and virtual worlds. Metrics like IP traffic and iPhone sales are used to assess adoption, employing the Bass model to analyze two years of data (2008-2009). The findings highlight varying levels of innovation and imitation coefficients, with Second Life displaying significant innovation effects. Imitation effects tend to outweigh innovation effects across all services (Lee, 2011). Additionally, Trimi et al. (2011) provided a concise definition of key Metaverse concepts, encompassing virtual and mirror worlds, AR, and lifelogging.

Assessing innovation in the agricultural sector poses challenges due to its complexity. Previous research has predominantly focused on measuring innovation in manufacturing, neglecting agricultural firms (Ariza 2013). The emergence of social media has prompted

educators to rethink learning approaches. This study explores a social business gaming platform that applies social networking concepts in academia, aiming to enhance creative and analytical skills, particularly in information systems security (Neville, 2013).

Theoretical Framework

This study employs a mixed-method research technique. Its main goal is to explore the Cybersecurity aspects involved in Thailand's progression towards adopting the Metaverse (see Figure 1).

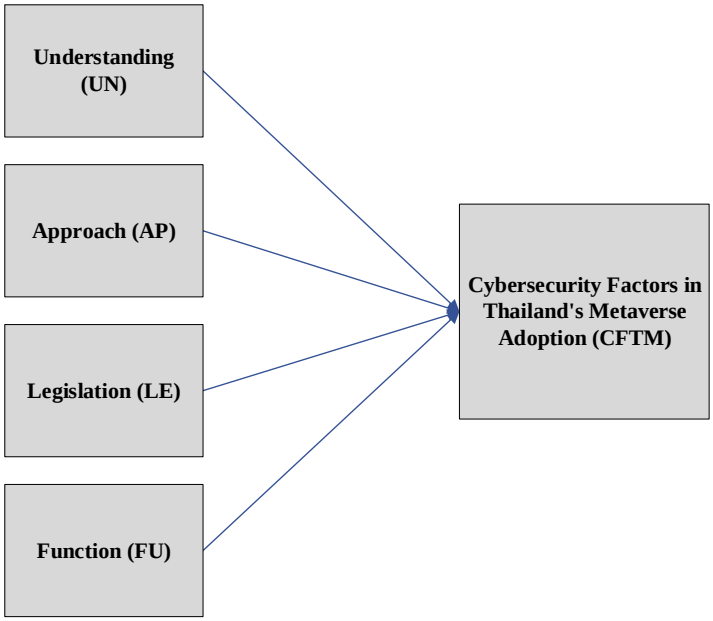

Figure 1: Conceptual framework of the research

Methodology

The aim of this research was to investigate cybersecurity factors in Thailand's metaverse adoption. This research employed a mixed-method approach, encompassing both qualitative and quantitative methodologies. In this section, the researcher employed the following methods:

Qualitative Methodology: For the purpose of this study, the population and sample groups were categorized into four distinct segments: Group 1 consisted of two individuals from the National Cybersecurity board; Group 2 comprised four specialists in the field of Cybersecurity; Group 3 included five university professors; and Group 4 encompassed four experts specializing in the Metaverse domain. Therefore, all four groups consisted of 15 people. The study utilized e-Focus group conducted using Zoom and online surveys administered through Google Forms as its main data collection methods. The chosen data analysis technique was the Fuzzy Set Theory. A questionnaire was combined with e-Focus group involving 15 specialists to address main and sub-issues. Relevant factors and indicators were identified with a threshold of acceptance at 0.917.

Quantitative Methodology: This research collected data from a sample of 800 Meta users in Thailand, selected through a simple random sampling method. In this study, data collection was accomplished through the use of a digital survey. Researchers compiled literature reflecting the insights of 15 experts, which was then utilized to create a 7-point Likert scale questionnaire. The data collection process involved distributing the online questionnaire through various platforms, including the Facebook page, Line Application,

and email. This data collection phase spanned three months and involved 800 respondents. Following this, all 800 datasets underwent thorough scrutiny for accuracy before being utilized in subsequent statistical analyses. Frequency and percentage were used to analyze general data of participants. An exploratory factor analysis (EFA) was conducted using the principal component analysis method with orthogonal rotation, specifically the Varimax rotation method. Indicators with a component weight less than 0.5 or cross-loading greater than 1 were excluded. The remaining indicators in the model were required to possess an Eigenvalue greater than 1.0, in accordance with the recommendations of Hair et al. (2006) and Rangsungnoen (2011) for EFA.

Results

E-Focus group Results: Fifteen specialists were given the option to address the main inquiries using either the Zoom application or they could choose the alternative method of the Google form to gather data. Following the conclusion of the e-focus group, researchers analyzed and distilled insights from the recorded Zoom interactions and submissions via Google Forms, following the outlined procedure.

Understanding (UN): The understanding of the Metaverse is limited, emphasizing the need for education. Legal structures exist but face challenges in enforcement. Cyber-vaccination and cyber-literacy are strategies, but they require sufficient literacy for effectiveness. Immersion in the Metaverse can impact mental well-being, especially for those with depressive disorders, highlighting the importance of awareness. Detachment from reality due to the allure of the virtual world exposes individuals to cyber-threats. Education on Metaverse utilization and safety protocols is crucial to prevent cybercriminal activity. Objectives in the Metaverse vary among user groups, necessitating tailored knowledge dissemination. Collaboration between sectors is vital for understanding user interactions and service provision.

Technological disparities must be addressed to minimize digital discrimination within the Metaverse. Education plays a crucial role in reducing disparities, with most users relying on advertisements, lectures, and seminars for information. Authentication is essential for credibility, and AI-driven behavioral analysis aids in identity recognition and secure transactions. Privacy concerns require international standards, and security risks like data collection and movement must be addressed. Device safety is a concern in the Metaverse, with factors like age, gender, and data security needing consideration. Current designs prioritize functionality over safety, potentially leading to accidents and cybersecurity breaches. Privacy protection for personal data collected by Metaverse devices is crucial, and random checks are necessary to uncover concealed functionalities.

Assessing the necessity of personal data collected by Metaverse devices is crucial. Despite essential data needs, privacy protection might be inadequate. Random checks are necessary to uncover concealed functionalities. Data security should persist throughout a device's lifecycle, including access, maintenance, and repairs. Data providers must consent to sharing with devices. Regulatory gaps leave privacy vulnerabilities due to a lack of alignment with international laws. Undiscovered software vulnerabilities pose cyber threats, and device-user linkages make privacy management contingent on user conduct. The lack of a dedicated regulatory authority or framework for the Metaverse poses challenges, including issues related to audit criteria and data usage standards. The dominance of a few major platform developers with widely used devices makes ensuring reliability and verification complex. In conclusion, the evolving Metaverse requires comprehensive education, tailored initiatives for diverse user groups, collaboration, security, privacy protection, and safety considerations in device and system development.

Approach (AP): In the context of Thailand's Metaverse adoption and its cybersecurity aspects, there is a need for a well-defined approach. This approach should encompass an

educational process catering to both beginners and advanced users, involving both public and private sectors to ensure comprehensive knowledge dissemination across various segments of society. The aim is to explore opportunities for organizational and business benefits while establishing an ethical foundation for the evolving digital landscape. This ethical framework should cover various dimensions, including cybersecurity awareness and procedures, akin to educating individuals about the dangers of drunk driving.

Currently, there is no National Security Awareness Day, and the National Cybersecurity Board should prioritize creating awareness, especially concerning secure smartphone use and personal information protection. The national strategy requires adjustments to address these concerns effectively. Beyond individual cyberattacks, incidents like cryptocurrency billboard scams have revealed educational gaps, particularly among economically disadvantaged individuals with limited digital literacy. Leadership from influential regulators is crucial in addressing these challenges and developing an effective approach despite the shortage of expertise in this field.

In terms of education about the Metaverse, various pathways can be followed, including integration into school curricula and public sector dissemination. Both the public and private sectors need structured efforts to understand Metaverse laws and ensure lawful usage. Establishing a legal framework or enhancing existing ones is crucial, requiring collaboration among organizations to harmonize regulations and assign accountability. Awareness initiatives should align with existing laws, including the Computer Crime Act, the Cyber Crime Act, the Personal Data Act, and regulations related to issues like sexual abuse and defamation. Structured approaches to educate committees about the Metaverse are essential for effective regulation, with oversight mechanisms in place to avoid missed innovation opportunities. Thailand could consider forming a committee overseeing virtual world use, which includes regulators like EDTA and NCSB. This committee would establish procedures, guidelines, and recommendations to align regulatory frameworks with the needs of the business sector.

Legislation (LE): Legislation plays a vital role in governing the Metaverse, but striking the right balance between regulation and innovation is essential. Excessive regulation can stifle innovation and drive away investment and talent, while a lack of regulations can result in vulnerabilities. Thailand should establish tailored laws for the Metaverse to reduce ambiguity and enable effective enforcement, with justice institutions focusing on tracking wrongdoers and penalizing violations. Expanding existing legislation, such as the Personal Data Protection Act (PDPA), to include the Metaverse and assessing the applicability of the Computer Crime Act are important considerations. Education for legal professionals is crucial, as laws should be adaptable to keep up with technological advancements. Supplementary regulations can complement primary laws like the Computer Crime Act and the PDPA.

The impact of law on the Metaverse extends to both users' daily lives and enforcement of activities. Well-crafted laws are crucial for justice and coexistence in the virtual realm, as the Metaverse's impact extends to the real world. Regulations are vital for both virtual and physical actions and can effectively mitigate damage. Comprehensive legislation in Thailand should focus on personal data security, cybercrime, cybersecurity systems development, equipment security standards, and maintaining order against criminal activities. Legal provisions should cover personal data oversight, virtual behavior norms, aggression, and monetary transactions. Establishing jurisdiction over international Metaverses is complex but necessary for surveillance and offender tracking. International collaboration is crucial to address offenses that transcend borders. Sectors associated with content production or distribution within the Metaverse should be provided with precise guidelines, overseen by regulatory bodies with a strong understanding of technology and business.

Regulatory standards should exclusively apply to pivotal aspects of the Metaverse that have significant societal impact, and regular review processes should be instituted to adapt to technological shifts. Striking a balance between regulation and innovation is crucial for the responsible growth of the Metaverse, ensuring both security and continued development.

Function (FU): With no dedicated governing body for the Metaverse, the National Cyber Security Board (NCSB) oversees critical information infrastructure, while private sectors educate users. Regulatory jurisdiction extends to areas like the Stock Exchange of Thailand (SET) regulating Digital Assets, but Metaverse coverage might be inadequate. Ministry of Digital Economy and Society (MDES) oversees technology, involving various sectors. Collaboration among Ministries of Interior, Digital Affairs, and Justice is crucial. Data sovereignty is complex due to European ownership. Educating users and addressing national security are challenges. Regulatory measures, penalties, and collaboration between NCSB and NHSO are recommended for effective oversight.

In cases where the business-oriented group can't provide information, an alternate group might be necessary, albeit originating from the same body as a guiding principle. The passage discusses the collaboration required among various Thai regulatory agencies to oversee the Metaverse. It emphasizes the challenges of regulating a foreign-owned platform and educating users in this context. Experts have highlighted various responsibilities of regulatory bodies, including NCSB's role in security monitoring. ETDA should concentrate on system development and security standards. NCSB is responsible for security laws. Other bodies like The Energy Regulatory Commission, Stock Exchange of Thailand, and Bank of Thailand handle enforcement, monitoring, and response. Collaboration is crucial as the virtual world intersects with reality, requiring coordinated efforts.

Each agency should oversee critical legal matters within their existing jurisdiction, leveraging their understanding of the infrastructure and businesses, which possess broader connections than just the Metaverse. Educational institutions play a pivotal role in imparting direct knowledge and learning lessons, thereby serving as intellectual assets for the future advancement of the virtual economy, setting an example for the succeeding generation and ensuring long-term sustainability.

The research initially identified certain factors from an e-Focus group dataset. Subsequent input from 15 specialists led to the expansion of factors to 131 across 4 components. Further analysis and merging of related concerns resulted in a refined enumeration of 76 factors. This process ultimately led to the synthesis phase, where a final collection of 60 factors was derived. These refined factors were organized within Table 1, representing the comprehensive insights obtained from the study.

Table 1 Demonstrate the amalgamation of factors pertaining to Cybersecurity

Component	Raw factors	Extraction factor	Final factors
Understanding (UN)	45	33	26
Approach (AP)	13	10	10
Legislation (LE)	30	15	12
Function (FU)	43	18	12
Total	131	76	60

Fuzzy Set Analysis Results: The researchers conducted an online survey to obtain input from all fifteen specialists regarding the pertinent factors. This survey consisted of an online closed-ended questionnaire featuring a 7-point rating scale. The survey was facilitated through Google Forms, and participants were requested to evaluate the applicability of the factors. The researchers examined the data contributed by the entire cohort of fifteen specialists using a Fuzzy computer application. Given the presence of fifteen specialists, the process of computing Fuzzy membership values was executed in

the subsequent manner. Based on the responses of experts to a digital questionnaire and the formula Qx = ((n + 1)r)/4, it can be deduced that the entity at position 4 corresponds to Q1, position 8 aligns with Q2, and position 12 corresponds to Q3. Cybersecurity factors in Thailand's Metaverse adoption were determined with a threshold of 0.917.

Quantitative Results: The survey had 800 respondents, comprising 410 females (51.25%) and 390 males (48.75%). The majority fell within the 21-30 age group, accounting for 785 individuals (98.125%), while only 15 respondents were in the 31-40 age group (1.875%). Most of the respondents reported using Meta were from Thailand.

Exploratory Factor Analysis (EFA): The examination of the suitability of the variable set for the study was conducted. After removing some factors, the Kaiser-Meyer-Olkin (KMO) measure of Sampling Adequacy yielded a value of 0.661, surpassing the 0.60 threshold. This indicated that, following Kim and Mueller's criteria, the set of variables was deemed suitable for component analysis. Bartlett's Test of Sphericity revealed a statistically significant correlation among the variables at the 0.000 level, confirming their appropriateness for component analysis, as detailed in Table 2.

Table 2 Kaiser-Meyer-Olkin (KMO) and Bartlett's Test Results

KMO		0.661
Bartlett's Test	Approx. Chi-Square	10218.226
	Df	55
	Sig.	0.000

Table 3 displayed the percentage of the overall variance within the variables that could be accounted for by individual factors. When the variables are mutually independent, the total variance equals the number of variables considered in the analysis. Eigenvalues were employed to determine the appropriate number of factors.

Table 3 Presentation of the Total Variance Explained

Total Variance Explained						
Component	Initial Eigenvalues			Extraction Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	3.643	33.122	33.122	3.643	33.122	33.122
2	2.458	22.348	55.469	2.458	22.348	55.469
3	1.695	15.413	70.882	1.695	15.413	70.882
4	1.430	13.002	83.885	1.430	13.002	83.885
5	0.893	8.114	91.999			
6	0.397	3.613	95.612			
7	0.245	2.231	97.843			
8	0.151	1.375	99.218			
9	0.062	0.561	99.779			
10	0.013	0.118	99.897			
11	0.011	0.103	100.000			

Conclusion

The research involved 800 respondents, predominantly in the 21-30 age group, with 51.25% females and 48.75% males. A notable majority from Thailand reported using Meta. The Exploratory Factor Analysis (EFA) assessed the variable set, meeting suitability criteria with a KMO measure of 0.661 and significant correlations via Bartlett's Test. Its clarified the variance explained by individual factors, totaling 83.885%, with the

first factor contributing 33.122% and the second 22.348%. The third and fourth factors explained 15.413% and 13.002%, respectively.

The study's findings confirmed the appropriateness of the analyzed variables and identified four distinct components comprising a total of eleven significant factors. These components were consolidated into a unified entity referred to as "Cybersecurity Factors in Thailand's Metaverse Adoption" (CFTM). These components and their corresponding factors include:

- Metaverse Governance and Regulatory Framework: This component underscores the necessity for comprehensive laws, knowledge-sharing organizations, government collaborations, and the establishment of the Thai Virtual World Security Agency (TVWSA) to ensure Metaverse safety.
- Digital Behavior and Legal Education: This component encompasses various aspects, such as digital addiction, digital threats, and the importance of legal education.
- Metaverse in Education & Device Security: This component focuses on the implementation of educational Metaverse practices in schools and the security of digital devices.
- Online Security Awareness: Covering topics related to cybersecurity on the internet and the promotion of online security consciousness.

This research adopted a mixed-methods approach to gather insights from specialists, utilizing e-Focus group sessions conducted via Zoom and open-ended online questionnaires through Google Forms. Despite time constraints, open-ended questionnaires, preferred by specialists, provided detailed responses and valuable feedback. The analysis employed closed-ended surveys and the Fuzzy Technique, yielding results that were in harmony with experts' viewpoints concerning the cybersecurity factor in Thailand’s Metaverse adoption. All factors exceeded the permissible threshold of 0.917, confirming their relevance in Metaverse Cybersecurity. In conclusion, the integrated approach effectively collected comprehensive specialist data, leading to the identification of four key components and eighteen distinct factors.

Regarding the quantitative aspect, 800 respondents, primarily in the 21-30 age group with a gender distribution of 51.25% females and 48.75% males, participated. A significant number of respondents from Thailand reported using Meta. The Exploratory Factor Analysis (EFA) determined the suitability of the variable set, meeting the criteria with a KMO measure of 0.661 and significant correlations via Bartlett's Test. The analysis revealed that 83.885% of the total variance could be explained by four identified factors. These factors were consolidated into a single component and given descriptive names aligning with Cybersecurity Factors in Thailand's Metaverse Adoption (CFTM).

The newly identified factors align with research conducted by Manasan (2021), Kim (2021), Radoff (2021), Lee et al. (2021) and Leenes in 2008 and 2009. Additionally, these factors are in accordance with the Office of the National Security Council (2017).

References

Acquisti, A., & Gross, R. 2006. Imagined communities: Awareness, information sharing, and privacy on Facebook. In Proceedings of the 6th International Conference on Privacy Enhancing Technologies (PET'06) (pp. 36-58). Springer-Verlag. https://doi.org/10.1007/11957454_3

Ariza, C., Rugeles, L., Saavedra, D., & Guaitero, B. (2013). Measuring Innovation in Agricultural Firms: A Methodological Approach. The Electronic Journal of Knowledge Management, 11(3), 185-198. Retrieved from http://www.ejkm.com

Channuwong, S. (2018). “The relationship between good governance principles

and organizational justice: A case study of Bangkok Government Officials".

Asia Pacific Social Science Review, 18(3), 43-56.

Channuwong, S., Ruksat, S., & Changcharoen, C. (2023). Buddhist wisdom for reducing mental suffering and improving mental health during the COVID-19. Journal of Advanced Zoology, 44(3), 694-703.

Dionisio, J. D. N., III, W. G. B., & Gilbert, R. 2013. 3D virtual worlds and the Metaverse: Current status and future possibilities. ACM Computing Surveys (CSUR), 45(3), 1-38. Jul. 2013.

Duan, H., Li, J., Fan, S., Lin, Z., Wu, X., & Cai, W. 2021. Metaverse for social good: A university campus prototype. In ACM International Conference on Multimedia (MM), Oct. 2021, pp. 153-161.

ETDA. 2021. ICT Law Center. https://ictlawcenter.etda.or.th

Evangelista, P., Esposito, E., Lauro, V., & Raffa, M. 2010. The Adoption of Knowledge Management Systems in Small Firms. Electronic Journal of Knowledge Management, 8(1), 33-42. https://www.ejkm.com. DOI: https://doi.org/10.34190/ejbrm.19.2.2509

Große, C., Olausson, P. M., & Wallman-Lundåsen, S. 2021. Left in the Dark: Obstacles to Studying and Performing Critical Infrastructure Protection. The Electronic Journal of Business Research Methods, 19(2), 58-70. Retrieved from http://www.ejbrm.com

Hair, J., Black, W., Babin, B., Anderson, R., & Tatham, R. 2006. Multivariate Data Analysis (6th ed.). Pearson Prentice Hall.

Jeon, J. E. 2021. The Effects of User Experience-Based Design Innovativeness on User–Metaverse Platform Channel Relationships in South Korea. Retrieved from https://www.koreascience.or.kr/article/JAKO202131659495625.pdf

Kim, J. 2021. A Study on the Development of Information Protection Education Contents in the Maritime Using Metaverse. Journal of The Korea Institute of Information Security & Cryptology. Retrieved from https://www.koreascience.or.kr/article/JAKO202130865175563.page

Lee, L.-H., Braud, T., Zhou, P., Wang, L., Xu, D., Lin, Z., Hui, P. 2021. All one needs to know about the Metaverse: A comprehensive survey on technological singularity, virtual ecosystems, and research agendas. arXiv preprint arXiv:2110.05352.

Lee, S. G., Trimi, S., Byun, W. K., & Kang, M. 2011. Innovation and imitation effects in Metaverse service adoption. Service Business, 5, 155-172..

Leenes, R. E. 2008. Privacy in the metaverse: Regulating a complex social construct in a virtual world. In S. Fischer-Huebner, P. Duquenoy, A. Zuccato, & L. Martucci (Eds.), Proceedings of the IFIP/FIDIS Summer School on "The Future of Identity in the Information Society" (pp. 95-112). Springer.

Leenes, R. E. 2009. Privacy regulation in the metaverse. In B. Whithworth, & A. Moor (Eds.), Handbook of research on socio-technical design and social networking systems (pp. 123-136). Information Science Reference.

Manasan, S. 2021. Metaverse: Law and Future in a Parallel World. Retrieved from https://www.bangkokbiznews.com/columnist/973315

Metaverseroadmap. 2016. A Cross-Industry Public Foresight Project. Retrieved from https://www.metaverseroadmap.org/MetaverseRoadmapOverview.pdf

Mufti, Y., Niazi, M., Alshayeb, M., & Mahmood, S. (2018). A Readiness Model for Security Requirements Engineering. IEEE Access, PP(99), 1-1. 10.1109/ACCESS.2018.2840322.

Ning, H., Wang, H., Lin, Y., Wang, W., Dhelim, S., Farha, F., Daneshmand, M. 2021. A survey on Metaverse: the state-of-the-art, technologies, applications, and challenges. arXiv preprint arXiv:2111.09673.

Neville, K., & Heavin, C. 2013. Using Social Media to Support the Learning Needs of Future IS Security Professionals. The Electronic Journal of e-Learning, 11(1), 29-38. Available online at www.ejel.org

Office of the National Security Council. 2017. National Cyber Security Strategy 2017-2021. Office of the Prime Minister. Retrieved from https://www.nsc.go.th/wp-content/uploads/2018/08/strategyit60-64-1.pdf

Poddubnaya, N., Kulikova, T., Ardeeva, A., & Alekseeva, P. 2020. Formation of Digital Literacy of Students by Means of Virtual and Augmented Reality Technologies. In SLET-2020: International Scientific Conference on Innovative Approaches to the Application of Digital Technologies in Education. Retrieved from http://ceur-ws.org/Vol-2861/paper_36.pdf

Radoff, J. 2021. The Metaverse Value-Chain. Building the Metaverse. Retrieved from https://medium.com/building-the-metaverse/the-metaverse-value-chain-afcf9e09e3a7

Rangsungnoen, G. 2011. Statistical Analysis of Computer Data for Research. Bangkok: Se-ed Public Company Limited.

Ratanavaraha, N., & Srisa-An, C. 2023. Critical Factors of Readiness Model for Metaverse Security and Privacy Adoption. Retrieved from https://www.eurchembull.com/uploads/paper/95883774fdca3d7bc0cd203fd69dbe18.pdf doi: 10.31838/ecb/2023.12.s3.2502023.01/05/2023

Ratanavaraha, N., & Srisa-An, C. 2023. Security and Privacy Factors for Metaverse Adoption in Thailand. Retrieved from https://www.eurchembull.com/uploads/paper/748450d09009a5709c3a556582e395ba.pdf doi: 10.48047/ecb/2023.12.5.2822023.28/05/2023

Sardjono, W. 2019. Readiness Model of Knowledge Management Systems Implementation at the Higher Education. ICIC Express Letters, 13(6), 1-1.

Sebastian, G. 2023. A Descriptive Study on Metaverse: Cybersecurity Risks, Controls, and Regulatory Framework. International Journal of Secure Software Engineering (IJSSE), 15(1), 1-14. http://doi.org/10.4018/IJSPPC.315591

Skinner, G., Han, S., & Chang, E. 2006. Defining and Protecting Meta Privacy: A New Conceptual Framework With in Information Privacy, 101 - 101. 10.1109/ICDEW.2006.46.

Thammajai, A. 2021. Metaverse Economy: Real-Virtual Economic Opportunities. Business Prachachat. Retrieved from https://www.prachachat.net/columns/news-801147

Tongvijit, M. (2023). A development of online learning format in the age of the new normal life. Journal of Advanced Zoology, 44(3), 254-262.

Trimi, S., Lee, S., & Kang, M. 2011. Innovation and imitation effects in Metaverse service adoption. Retrieved from https://www.academia.edu/26901253/Innovation_and_imitation_effects_in_Metaverse_service_adoption.

T., K. 2021. Metaverse: What is Metaverse and what technologies does it consist of? How is it related to Cryptocurrency within 5 minutes? Techsauce. Retrieved from https://techsauce.co/tech-and-biz/what-is-metaverse

Yang, Q., Zhao, Y., Huang, H., & Zheng, Z. 2022. Fusing blockchain and AI with metaverse: A survey. arXiv preprint arXiv:2201.03201.