Security and Privacy Factors for Metaverse Adoption in Thailand

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

[1]*School of Digital Innovation Technology, Rangsit University, Pathumthani, Thailand (noppadon.r64@rsu.ac.th)*
[2]*School of Digital Innovation Technology, Rangsit University, Pathumthani, Thailand (chetneti@rsu.ac.th)*

Abstract –Since 2021, Metaverse has been the first complete online virtual world platform that provides a realistic user experience. To transform its service into a Metaverse application, Facebook changed its name to Meta, and the application has been widely adopted since then. As the market value of Metaverse has significantly increased, there is a growing need for increased security and privacy measures. Currently, there is a lack of research on the Security and Privacy Factors that affect Metaverse adoption in Thailand. This study aims to identify such factors by conducting a mixed methodology approach, combining questionnaires, e-Focus groups, and Fuzzy analysis with 15 specialists. Ultimately, the study identified 5 components and 25novel factors that are affected to the research.

Keywords – Security, Privacy, Metaverse, Fuzzy, Electronic Focus group

1. Introduction

In the past few years, there has been a considerable movement towards digitalization, which encompasses the concepts of digital disruption and digital transformation. The COVID-19 pandemic has also played a crucial role in accelerating this trend. This has led to Thai people relying more heavily on digital technology in their daily lives. With the possibility of future crises and the uncertainty of returning to pre-COVID-19 lifestyles, Thai people must adapt to new ways of life. Health and safety have become top priorities, leading to the adoption of social distancing as a new way of life. To satisfy their need for entertainment while maintaining safety, Thai people have turned to virtual events, which provide a live atmosphere and a sense of community while minimizing health risks. Virtual events are gaining popularity as they allow for creative expression and the formation of micro-communities, enabling people to connect with each other and adapt to the digital lifestyle as a new form of media consumption. The problems related to the security and privacy of social media technology in Thailand persist and have significantly increased in line with the growth of the market. In February 2021, online shopping in Thailand increased by 42.8%, while online food ordering statistics increased by 38.2%, leading to various issues that exploit social media technology channels for fraudulent purposes. (EverydayMarketing,2021)

Metaverse, a virtual reality social media technology, was first introduced in 1992 in the science fiction novel "Snow Crash," which portrays a virtual space where everyone exists in parallel with reality. The term "Metaverse" gained prominence in the social media world when Facebook founder Mark Zuckerberg announced that the future of the company would expand beyond building social applications and developing hardware. Facebook aims to create new experiences resembling science fiction, which is commonly known as the "Metaverse".(Jittipong,2021)

The Metaverse Economy is considered the next generation of the digital economy due to its fast-paced and high-impact nature. However, Thailand is currently only at a low to medium level of readiness to deal with various businesses, including government, private, academic, and infrastructure. While Thais may not be producers of technology, they can still be buyers and users of it, and this can lead to significant economic implications. The Metaverse Economy presents a huge economic opportunity as it combines the real and virtual worlds through a 3D virtual universe, creating what is known as Second Life. This will be an important step in the development of virtual economics. (Anusorn,2021)

Various threats exist to social media technology. According to statistics from the National Electronics and Computer Technology Center (NECTEC)in 2016, the number of internet users in Thailand nearly reached 40 million, up from less than 30 million in 2014, accounting for 16 percent of internet users in Southeast Asia, which is approximately 250 million people. A 2015 survey of internet users on computers, mobile phones, and various devices and technologies showed that Thailand has a population of over 24.6 million internet users aged 6 years and above, which is equivalent to 39.3 percent of all internet users. Teenagers aged 19 or younger accounted for about one-third of all internet users, approximately 8.4 million. A survey conducted by the Electronic Transactions Development Agency (ETDA) revealed that, on average, people spend 41.4 hours per week using the internet, with smartphones being the most popular means of accessing the internet (accounting for 80.9 percent), followed by desktops and laptops. In

terms of applications, Facebook and LINE are the most popular social media platforms.Thailand's National Cybersecurity Strategy 2017-2021has identified eight strategic issues, including enhancing confidence and trust in all sectors, protecting critical infrastructure managed by information systems, protecting national interests and security, strengthening the digital economy system, raising awareness and promoting domestic cooperation, promoting a culture of appropriate use of cyberspace, promoting work on the prevention and suppression of crime, and promoting Thailand's creative role in the region and internationally. The strategy assesses the readiness, problem conditions, and trends of cyber threats in five main areas: legal and regulatory measures, technical readiness to deal with cyber threats, personnel readiness, system and technology readiness, and investigative and cyber intelligence readiness. (National Cyber Security Strategy 2017-2021,2017)

However, little has been discussed about the security and privacy factors for Metaverse adoption in Thailand. This research aims to determine the security and privacy factors that affect the adoption of Metaverse in Thailand.

2. Literature Review

The virtual world is becoming a primary tool for learning in many areas, enabling individuals to acquire new job skills and collaborate more cost-effectively and efficiently. For young people growing up in this environment, their physical lives may be more Spartan, while their virtual lives are rich and exotic. Promoting access to 2D and 3D web technology could also help illiterate youths in emerging countries to develop significantly in the virtual world. With more people involved in the virtual world, positive social changes will occur, and some aspects of the physical world may collapse.The mirror world, particularly for home applications, will be a major new market for security, property insurance, moving and storage, rental and trade-in, interior decoration, construction, and home automation. While only a few industries will be significantly affected, the data power of these tools will pose new challenges for crime prevention and privacy protection. Connecting the Mirror World will allow for the development and understanding of global and community events by education, organizations, and commerce.As virtual information continues to proliferate, data overload is becoming a common problem. However, the advantage is that these problems govern human use of the system regarding nature, rest, and recreation. On the other hand, AR technology can be used to hide images that are considered disturbing or offensive, leading to self-obsession, isolation, and addiction. Some individuals may choose to see only what they are interested in, leading to biased information, a disguise of reality, media services, or religious groups. Economic and political processes should ensure that these systems have more power than any one person to guarantee the availability of information for later review.These rapid technological developments, including technological trends, connectivity, bandwidth, storage capacity, sensor accuracy, miniaturization, and affordability, have led to the use of monitoring systems in law enforcement agencies. Data is connected to a data center that serves to prevent deletion and recover data from theft, and many devices have been developed to record events for different purposes, including physical safety and health. However, limitations may arise, such as older people having difficulties adapting to new technologies and preferring a simpler lifestyle.The preservation of past experiences is fully functional, and the recall and analysis of those experiences have continually improved over the lifetime of the user. Once saved, the record will last forever, allowing for a better understanding of others from their point of view. The potential for such applications will bring benefits to law enforcement applications, such as better education, training, mentoring, self- and social awareness, remediation of conflicts, etc. However, it is also a powerful example of modern state surveillance capabilities, raising questions about the responsibility for spreading malicious misinformation and the sufficiency of the existing legal framework.Such technology may not only serve as a backup memory but also as a backup of the subconscious mind, providing powerful cognitive reinforcement and guidance from past examples. Looking at the bigger picture, the ongoing development of artificial intelligence has made merging the "mind" of humans and machines a potential lifesaving virtue.The growth of the Radio Frequency Identification (RFID) industry has been hindered by privacy concerns, which have in turn led to an expansion of surveillance capabilities. The ubiquity of cameras on phones has made it easier to record all kinds of activities in mirror worlds, AR, and lifetime recording, which can then be duplicated. Users may resist or impose restrictions on technology development if they believe their privacy may be violated or threatened as a result. When it comes to intellectual property issues, existing laws around copyright often limit the ability of technologies that record or access copyrighted material. Weak digital rights management systems tend to be ineffective and useless. (Metaverseroadmap,2016)

Verifying user interactions is one of the main challenges when connecting human users in the physical world with the Metaverse. It is crucial that this connection is always easy, fast, and accurate.(H. Ning,2021)Kim J. defines the Metaverse as a virtual world that supports real-time operations, which will be integrated with existing real-world internet elements.(Kim J,2018)

Jon Radoff has proposed an intriguing concept that outlines the structure of the Metaverse, dividing it into seven distinct layers. The first layer focuses on the infrastructure, including internet speed, cloud computing speed, graphics processing unit (GPU), and material quality in the Metaverse world.The second layer is the human interface, which comprises devices that enable humans to connect to the Metaverse world, such as wearable

devices like Oculus glasses, smart glasses, or even sensors that can connect to muscles to control the Metaverse world.The third layer is decentralization, which refers to technologies like Blockchain that facilitate a virtual economy within the Metaverse world.The fourth layer is spatial computing, which is the central system of the Metaverse world, including 3D engines, virtual reality (VR), augmented reality (AR), and user interfaces.The fifth layer is the Creator Economy, which involves creating various businesses, games, and trading within the Metaverse world.The sixth layer is Discovery, which is the process of attracting new users to the Metaverse world through community-driven means such as word of mouth, search engines, or other earned media.The seventh and outermost layer is Experience, which includes adventure-style challenges that create a Lock-in Effect, making users feel engrossed in the virtual world where their society resides. Ultimately, the Metaverse will dominate the real world when this occurs.(Jon Radoff,2021)

According to Jin Kim's research, implementing metaverse technology in teaching and learning can improve the overall learning experience for students. By combining virtual reality user experiences with education, better learning outcomes can be achieved. This can overcome the limitations of offline education by utilizing education and webinars. In addition, learners can acquire knowledge on cybersecurity threats through the use of virtual worlds. Furthermore, simulated cyber-attacks and accidents can be created to experience the impact they have on any activity. Finally, virtual exhibition halls can be developed for events to promote social and safety awareness. The researcher believes that developing learning on the Metaverse is crucial for virtual experiences to become real experiences for Metaverse users (Jin Kim,2021). Furthermore, the use of virtual reality technology can significantly enhance technical and complex learning with higher learning efficiency.(Natalia P,2020)

Three key areas that need to be addressed in the metaverse are social acceptance, security and privacy, and trust and accountability. Users expect that their activities in the metaverse are free from privacy-related risks and security threats. To ensure security in the metaverse, blockchains can be used as a centralized storage system. One advantage of blockchains is that millions of other nodes can be referenced to fix an error in case of a mistake in one node, which guarantees decentralization and security. Authentication can also be achieved through blockchains, which ensures data security. Additionally, data in blockchains is encrypted and moved to anonymous nodes for storage, and a tamper-proof mechanism is used to ensure the security of shared data. Smart contracts and access control can also be used to track all users' data access behavior.Security and privacy are critical for managing data in the metaverse. While clouds collect and search end-user data on the service provider side, there is a significant risk of privacy leaks. Edge computing provides a better solution by allowing data processing and storage at the Edge, increasing security and privacy. A solution that trains at the edge and aggregates at the cloud can improve the security and privacy of the metaverse. However, innovative data security and privacy mechanisms are necessary to guarantee results.In summary, edge computing is a promising solution that complements cloud solutions in the metaverse. It can reduce the latency of the user experience, provide real-time local multi-user interaction with improved mobility support, and enhance the privacy and security of metaverse users.Designers and developers need to develop ethical approaches in the metaverse and protect digital twins. They must evaluate user behavior in the metaverse and the risks they may be exposed to, such as privacy invasions or ongoing monitoring. Biometric data, such as information collected from VR headsets and wearables, is a key metric in the field of security and privacy. Security researchers should consider new mechanisms to enable authentication options, such as biometric authentication. However, these authentication systems still need improvement in terms of security level, detection accuracy, and speed.Based on the research by Lik-Hang Lee et al., the authors consider it a key metric in the field of security and privacy, providing critical insights into privacy behavior in the metaverse and design ethics.(L.-H. Lee,2021)

Assisted Reality is a technology that enables users to interact with screens without using their hands, also known as hands-free technology. Examples of devices used in AR include smart glasses that connect to the internet, allowing users to communicate and give commands via voice, and receive information directly in their field of vision.Another technology is virtual world technology, which can simulate the real world and is often used by retail businesses to allow customers to test products online. For instance, IKEA has developed an app that uses AR technology to allow customers to try out furniture in their own rooms.Multiverse or parallel worlds refer to platforms or communities in the digital world that operate independently of each other. Examples include Facebook, Minecraft, Instagram, Roblox, Fortnite, and Discord. In theory, the Metaverse can bring these multiverses together into one place. Non-Fungible Tokens (NFTs) enable anyone to own, buy, sell, and create value for digital products. The blockchain technology regulates ownership and prevents theft. NFTs can be traded using cryptocurrencies. Virtual Reality, also known as virtual experiences, refers to the use of devices or technologies that connect users with the digital world. In the novel Ready Player One, for example, characters use virtual reality glasses to immerse themselves in the game world.(Kultida T,2021)

Joo-Eon JEON carried out a study titled "The Effects of User Experience-Based Design Innovativeness on User–Metaverse Platform Channel Relationships in South Korea." This research aimed to analyze the influence of innovation on different aspects, including identity, attractiveness, novelty, usability, and interaction, as well as their relevance to virtual worlds, mirror worlds, augmented reality, and lifelogging.The results of the

research show that attractiveness and interaction improve the Metaverse Platform's identity and commitment, and the platform's identity enhances participation in both virtual worlds and mirror worlds. This research indicates that the development of the Metaverse Platform is continuously progressing to achieve the concepts of the Metaverse in four areas: virtual worlds, mirror worlds, augmented reality, and lifelogging.(Joo-Eon JEON,2021)

Huansheng Ning et al. identified five aspects of the metaverse: 1) Network infrastructure, 2) Management technology, 3) Basic common technology, 4) Virtual reality object connection, and 5) Virtual reality convergence. They also presented the spatial nature of the social and hyper metaverse. (H. Ning,2021) Skinner, Geoff, Han, Song, and Chang, Elizabeth defined a new term, "metadata," as data that contains personal or personally identifiable information and classified it as a Meta Privacy Risk.(Skinner,2006)

Leenes, R. E., conducted research on Privacy Regulation in the Metaverse and drew an interesting conclusion that Second Life can be thought of as a microscopic world in which ordinary people lead a more developed and private social life. This demand seems to contradict the essential characteristics of Second Life: social interaction, transparency, and openness. Therefore, special attention must be paid to other control schemes. The environment is designed to support sharing and gathering information about other residents, but changes to the governance structure have begun. Internal governance could lead to a more standardized governance structure and offer a way for residents to participate in governance. Additionally, there are tools for stronger regulation, such as the police and the justice system. Much can be learned from theories and real-world experiments on different forms of governance and policies. The protection of fundamental rights, such as privacy, must be guaranteed by society as a whole.(Leenes,2008),(Leenes,2009)

Silvana T. conducted research on Innovation and Imitation Effects in Metaverse Service Adoption and presented an intriguing definition of Virtual Worlds, Mirror Worlds, Augmented Reality, and Lifelogging. According to this research:Augmented Reality is a technology that enhances information about the physical outside world by layering information that a person can utilize.Lifelogging is an ancillary technology that records and reports the life history status of objects and users. It is categorized into two main types: Object Lifelogs, which record the environment and conditions of the physical world, and User Lifelogs, which record the lives of users.Mirror Worlds are enhanced virtual simulations or mirrors of the physical world. The world is also constructed from external sources such as environmental and geospatial data.Virtual Worlds simulate the socio-economic life of a physical world community. Simulations enable individuals to have a second self in the virtual world.(Silvana T,2011)

Regarding law, the researcher has compiled a list of relevant Thai laws based on announcements of related laws or announcements compiled by the Information and Communication Technology Law Center Law Office, including consideration of other laws that may be relevant. The total number of collected laws is 39 items.(ETDA,2021)

Sumaporn (Srisoonthorn) Manasan has suggested that laws related to the Metaverse can be divided into five categories:1) Laws that establish technological standards for the Metaverse platform. 2) Laws relating to blockchain transactions, cryptocurrencies, and NFTs. 3) Intellectual property law. 4) Personal Data Protection Laws. 5) Laws relating to dishonest or fraudulent acts. However, all of the above-mentioned legal issues are only part of the laws that may arise in the future as humans attempt to create another world parallel to the original world. When that day comes, there will be many more challenging legal issues for users, organizations, and governments to face.(Sumaporn M,2021)

The research on critical factors for the readiness model in Metaverse security and privacy adoption utilized a combination of research methods, including EFA, CFA, and Fuzzy Threshold=0.83. This approach helped to discover the readiness model and identify the top ten critical factors, which are as follows:Devices that prioritize privacy compatibility, Secure devices designed for use in the Metaverse, Efficient monitoring of data collection from used devices, Availability of devices and applications for privacy inspection, Laws and regulations pertaining to the Metaverse, Education for regulators directly related to the Metaverse, Education on how to use the Metaverse, Existing laws that cover foreign Metaverse systems, Comprehensive laws regarding foreign Metaverse systems that are suitable for users, and The Ministry of Education should play a role in setting up educational curriculums and providing knowledge related to Metaverse in schools.Furthermore, the formula equation for the readiness model was defined. (Noppadon R., 2023)

Fuzzy set theory is a mathematical framework that deals with uncertainty and vagueness. It extends classical set theory by allowing partial membership in a set, where an element can belong to a set to a certain degree between 0 and 1, instead of just fully belonging or not belonging. The concept of partial membership is expressed through membership functions, which map elements to degrees of membership in a set. Fuzzy set theory finds applications in various fields, such as artificial intelligence, control systems, decision making, and pattern recognition.(Marisol H,2022),(Thongchai P,2012)A fuzzy set is a group of objects that have varying degrees of membership. Each object is assigned a grade of membership between zero and one through a membership function that characterizes the set. The concepts of inclusion, union, intersection,

complement, relation, and convexity are applicable to fuzzy sets, and their properties in this context are well-established. One notable property is the separation theorem for convex fuzzy sets, which is proven without the condition that the sets be disjoint. (L.A. Zadeh,1965)

Electronic focus group is a research technique that employs online communication technology to conduct focus groups. Instead of physically gathering, participants use a virtual platform or chat room to engage in group discussions and provide feedback on a specific topic. These groups can be conducted in real-time or asynchronously, allowing participants to join and contribute at their convenience. Electronic focus groups offer several advantages, including increased flexibility and convenience for participants, reduced costs and time for researchers, and the ability to reach a wider audience across geographical boundaries. Nevertheless, there may be some limitations in terms of group dynamics and nonverbal communication cues compared to traditional in-person focus groups. (Ketkanok U,2019)

3. Conceptual framework

The researchers have synthesized data from the literature review related to security and privacy factors regarding metaverse adoption, along with the conceptual framework illustrated in Figure 1.

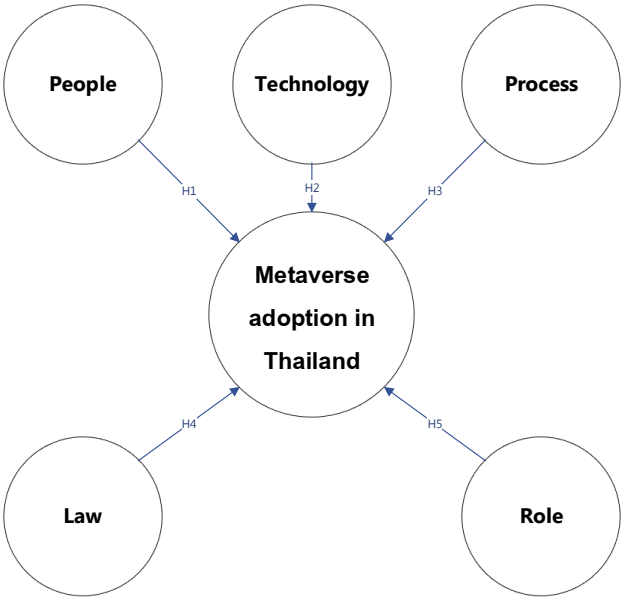

Figure 1. Conceptual framework.

4. Methodology

4.1 **The population and sample groups** for this research were divided into 4 groups as follows: Group 1) National Cybersecurity board with 2 persons, Group 2) 4 Cybersecurity specialists, Group 3) 5 university professors, and Group 4) 4 Metaverse specialists.

4.2 **Tools**: The data collection tools for this research were electronic focus groups using the Zoom application and online questionnaires through Google Forms.

4.3 **Documentary Research**: The researcher studied and synthesized information from various sources, including literature, books, websites, research papers in Thailand and abroad, and electronic focus groups. The researcher scheduled a focus group with 15 specialists, conducted it effectively, and securely stored and backed up the group chat logs and questionnaire data for further analysis.

4.4 **Data Analysis**: The researcher selected the Fuzzy Set Theory as the data analysis method and used a questionnaire in conjunction with the electronic focus group for both main and sub-issues with 15 specialists. The relevant factors and indicators were extracted using an acceptance criterion of 0.91.

5. Experiment

5.1 **Literaturereview results**:The researcher has synthesized the data related to security and privacy factors for Metaverse adoption in Thailand, resulting in a total of 60 issues, as shown in Table 1.

Table 1. Table of synthesis of security and privacy factors for Metaverse adoption in Thailand.

#	Related issues
1	The industrial sector has adopted a modern management system that utilizes various technologies, including Cloud, Big Data, and AI, to optimize efficiency. Virtual reality technology, known as Digital Twin, has also been implemented to manage and control various systems within a workplace from a single remote location, creating a realistic simulation of the actual environment. This development is progressive and can be applied in Thailand to create an industry that closely resembles the concept of Metaverse.
2	The virtual world can become a primary tool for learning in many areas, to acquire new skills for effective assessment and collaboration.
3	The context of youth growing up in such conditions may include more Spartan life in the physical world and a rich and exotic life in the virtual space.
4	Promoting access to the 2D and 3D WEB may also help illiterate youth in emerging countries.
5	There is a huge development in the virtual world, when more people are involved in the virtual world, the subsequent social changes will bring positive effects and the collapse of some in the physical world.
6	The home glass world will be a major new market; security, property insurance, moving and storage, leasing and trade-in, interior decorating, construction, and home automation are just a few of the industries that have been affected. The data power of these tools will pose new challenges in crime prevention and privacy protection.
7	Connecting the world of mirrors will enable education, enterprise, and commerce to develop and build understanding of global and community events.
8	As virtual data expands, data overload is a common problem. But the good thing is that these problems govern the use of human systems regarding nature, rest and recreation.
9	Using AR to hide images that are considered disturbing or offensive. It's a new form of self-obsession, isolation, and addiction. Some people may choose to see only what they are interested in, which may be information that caters to bias. The masking of unwanted realities, media services, religious groups, economic and political processes should help ensure that these systems are more powerful than those controlled by any individual
10	This ensures that what a person sees and hears remains available for later review. Technological trends, connectivity, bandwidth, storage capacity, sensor accuracy, miniaturization, and affordability all of this is due to rapid technological developments.
11	Lifetime recording is used in law enforcement agencies. Data is connected to the service data center to prevent deletion and recovery from theft.
12	There are various devices many more developed to record events for various purposes, including physical safety, health, etc.
13	Record-related limitations, for example, older generations may have difficulty adjusting and want to live a simple old life.The preservation of past experiences is now fully functional, the recall and analysis of those experiences has also improved. It is continuously updated over the lifetime of the user.
14	Saved and will last forever.On the positive side, those notes will help in understanding the other person from that person's point of view more easily.The potential of such applications will bring benefits to law enforcement, education, training, mentoring, self-awareness and society, conflict resolution, etc. In addition, It is also a powerful example of surveillance which is a capability of the modern state.
15	Responsibility for the dissemination of harmful false information, Is the existing legal framework sufficient?

16	Lifetime recording is not just a spare memory. Rather, it is a backup of the subconscious mind, which provides powerful cognitive reinforcement and guidance from past examples. Looking at the biggest picture, coupled with the ongoing work on the development of artificial intelligence, life recordings have become one of the many valuable things to unite the "mind" of humans and machines.
17	Verifying user interactions will be one of the main challenges. Connecting human users in the physical world with the Metaverse must always be easy, fast and accurate.
18	Fears over privacy have slowed the growth of the Radio Frequency Identification (RFID) industry and have resulted in a significant expansion of surveillance capabilities. And with the proliferation of camera phones, it is highly likely that all areas and activities will be recorded. Mirror worlds, AR, and lifetime records make it possible to replicate.
19	The user will push or cause limitations in development.If the user sees Privacy may be violated or threatened as a result of such technology.
20	Intellectual property issues: Existing intellectual property laws almost impair the ability of any technology to record or access copyrighted material. Weak digital rights management systems tend to be ineffective and useless.
21	The learner experience can be enhanced by applying Metaverse Technology in teaching and learning.
22	Breaking through the limitations of offline education by using online education and seminars.
23	Learning cybersecurity threats becomes more effective using virtual worlds.
24	The virtual world will simulate learning cyber-attacks and accidents, making it possible to experience the effects.
25	The virtual world can foster social awareness and raise security awareness by developing a virtual exhibition hall for cybersecurity.
26	Learning aspect cybersecurity metaverse Is it necessary or not, how to improve learning on Metaverse? To provide a virtual experience that will be a real experience for Metaverse users.
27	The use of virtual reality technology has significantly enhanced learning efficiency in technical and complex learning.
28	Cybersecurity Metaverse Learning. This learning resource deserves to be developed in the Metaverse.
29	Virtual worlds should consider three key areas of social acceptance, security, and privacy, as well as trust and accountability.
30	Users have the expectation that Their activities are free of privacy-related risks and no security threats.
31	Blockchains are centralized storage systems to guarantee security in the metaverse.
32	Blockchains: If there is an error in one node, millions of other nodes can be referenced to fix the error. Hence, decentralization and security are two distinct features of blockchain.
33	Authentication can be done through the blockchain, which guarantees the security of the data.
34	Data Sharing In blockchains, data is encrypted and moved to anonymous nodes for storage, thereby increasing the security of the data.
35	Tamper-proof mechanism, using blockchain access protection mechanism to guarantee the security of shared data and using smart contract and access control to track all users' data access behaviour.
36	Security and privacy are of the utmost importance for managing data in the metaverse.
37	Blockchain is a very secure information platform that allows companies to share information.
38	Currently, the cloud collects and retrieves end-user data and on the service provider side. Therefore, there is a serious risk of privacy leakage. On the other hand, Edge Computing provides a better solution for both security and privacy by allowing data to be processed and stored at the Edge.
39	Solution (train at the edge and aggregate at the cloud) can increase the security and privacy of the metaverse.
40	Edge computing requires innovative data security and privacy mechanisms to guarantee results.
41	Edge Computing is a promising solution that complements cloud solutions in the metaverse as it can 1) reduce the available latency of the metaverse user experience 2) provide real-time multi-user interactionwith improved mobility support, and 3) improved privacy and security for metaverse users.
42	The user accepts the consequences of security and privacy by comparing them with the risks in this area. For example, GPS location is used to find nearby friends, in the case of VR, which is the primary display device in the Metaverse. New ways to enable this more immersive environment (e.g., touch devices, Wearables to track user movements in detail) can pose new threats to users.
43	Metaverses can be thought of as social microcosmos where individuals using Metaverses can exhibit realistic social behaviour.In this

	ecosystem, individual awareness of privacy and security can track real behaviour.
44	Regarding the privacy and security risks that individuals may face when using Metaverse. It performs in-depth analysis of user behaviour in the metaverse and the risks they may face, such as privacy invasions or ongoing monitoring and privacy attacks on individuals. This may be experienced in metaverses such as deep-fakes and alternate representations. Evaluate how designers and developers can develop ethical approaches in the Metaverse to protecting digital twins. The focus is on biometric data where devices such as VR headsets and wearables can collect information about people when using Metaverse.
45	In the game, players do things like those in the Metaverse as a second life. Therefore, the privacy and security behaviourarelike the real thing. Players may experience extortion, surveillance or eavesdropping when their avatar interacts with other avatars in the Metaverse.
46	One solution to privacy and security threats in virtual worlds is the use of multiple avatars and copies of privacy in the metaverse.
47	Attackers can create avatars that look like victims' friends in hopes of extracting some personal information. (In the virtual world)
48	Blockchain uses a proof-of-work consensus mechanism that requires participants to try to solve puzzles to guarantee the security of their data. However, the verification process for encrypted data is not as fast as conventional methods.
49	Regarding security in distributed Edge environments at different layers, even a slightly vulnerable Edge device can lead to detrimental consequences for the entire Edge ecosystem.
50	Security and privacy metaverse services for highly digitized physical security will require users to frequently verify their identity when accessing applications and services on metaverse.
51	Devices that are compatible with privacy.
52	Secure devices for use in the Metaverse.
53	Efficient monitoring the of devices'sdata collection.
54	Readiness of privacy inspectiondevices.
55	Laws concerned with the Metaverse.
56	Education of directlyregulators related to the Metaverse.
57	Education on how to use the Metaverse.
58	Existing laws that cover foreign Metaverse systems.
59	Comprehensive laws regarding foreign Metaverse systems that are suitable for users.
60	The Ministry of Education should setting up educational curriculums and providing knowledge related to the Metaverse in schools.

5.2 The results of electronic focus group and the results of data analysis

On the day of the electronic focus group, 15 specialists participated at 9:00 AM, and the session was completed at 11:22 AM. Specialists were free to answer the main questions either via Zoom application or by using the Google form to store data as an alternative method.After completing the electronic focus group, the researchers synthesized and extracted the specialists from the recordings of the electronic focus group on the Zoom application and recordings from Google forms as follows.

5.2.1 People (H1): The Metaverse is a virtual world within the digital realm that brings people together and allows them to interact with each other as if they were in the same physical space, exchanging goods and services. Some aspects of the Metaverse can even be translated into tangible items in the real world. However, currently, there is limited knowledge about the Metaverse, and it is essential to provide more education in this field.Using technology to its maximum potential requires a deep understanding of its workings. Nevertheless, the knowledge required for users may differ from that required for creators or operators. Although Europe has laws in place, their administration is challenging. Educating people on cyber-vaccination and cyber-literacy can mitigate these issues. However, without proper literacy, there can be problems, and it is crucial to focus on individuals rather than regulation.

The virtual world is a social attraction for us, and we spend a lot of time engaging with technology. Regardless of age or stage in life, spending time in the Metaverse requires awareness of its impact on our health, especially for individuals with depression disorders. It is easy to lose oneself in the virtual world, forgetting the real world, and this may lead to cyber-threats. Therefore, it is essential to educate oneself on the proper use and

purpose of the Metaverse, as well as safety practices to avoid falling victim to cybercriminals.The purpose of use in the Metaverse differs for each group, and knowledge should be divided accordingly. For example, children nowadays like to own assets, while businesspeople are more focused on generating income. There should be a focus on the basics of accessibility, and the education provided should be tailored to the different user groups. Knowledge on how to take advantage of staying in the Metaverse is just as important as knowing how to access it.

There are different groups of knowledge, and it may not be appropriate to divide them by age. Instead, dividing the education based on the intended use of the Metaverse is more effective. It is important to raise awareness of how users use it and how service providers should provide their services. The public and private sectors and platform owners should work together to establish a framework for acceptable use to prevent illegal activities. Platform owners must cooperate with the government sector, and individuals should be informed about what to do if they encounter a problem, such as theft or impersonation.As the Metaverse develops, the potential for fake identities and scams increases, and education becomes even more critical. While legal matters may not require too much control, a legal framework must be established to ensure authenticity and protect users. Access to the Metaverse should be controlled, and identity verification is essential to trace any virtual offenses.In conclusion, the Metaverse is a fascinating and rapidly evolving virtual world that requires proper education to use safely and effectively. The education provided should be tailored to the different groups of users and focus on accessibility, awareness, and safety. By working together, we can establish a legal framework and provide more knowledge to promote the safe and secure use of the Metaverse.

Unequal access to technology highlights the importance of understanding digital discrimination and reducing social inequalities to increase opportunities in the metaverse. Educating those who are not familiar with digital technology is crucial in bridging the gap and reducing inequalities. Currently, most Metaverse users lack knowledge and rely solely on general advertisements, lectures, and seminars for information. In the digital world, distinguishing between real and fake is a challenge, leading users to rely on others for guidance. Thus, authentication is essential to ensure credibility. Cyber threats are a growing concern, particularly regarding users' acceptance and understanding of the contextual differences associated with the Digital Divide.

As each person's access to technology is not equal, knowledge about digital discrimination becomes crucial in order to increase opportunities and reduce social gaps or inequality in accessing the metaverse. Educating non-digital groups is essential to bring them into the metaverse and exploit its potential to reduce inequality. Currently, most Metaverse users have limited knowledge, and they mostly rely on lectures and seminars based on general advertisements. However, in the virtual or digital world, it is hard to differentiate between what is real or fake, and referring to others may occur. Therefore, authentication is critical. Cyber threats are becoming increasingly severe, especially in terms of other users' acceptance and understanding of the contextual differences associated with the Digital Divide.

It is imperative for Metaverse users to have knowledge about their usage and be aware to reduce the chances of being scammed and victimized. Users should understand the usage of technology and be aware of the threats surrounding both financial and lifestyle impacts. Using AI to analyze behavioral patterns can help identify identity when interacting with people or systems and transactions related to the platform, which may have more impact than other types of activities. Therefore, awareness will help maximize the use and safety, which can be used appropriately and profitably.To ensure the safety and security of Metaverse users, it is essential for them to possess knowledge about cyber threats since the Metaverse operates in cyberspace. Understanding various cyber threats and being vigilant can prevent falling victim to constantly evolving tactics, technology, and formats, which can result in financial loss and other damages.

Moreover, personal data in the Metaverse world can be linked to real-world data, which can be used to harm us. Therefore, users must possess significant knowledge about Security & Privacy on the Internet of Things (IoT) to protect themselves. They should be aware of the information used in the services they access and the devices they use to access them. Thorough understanding of privacy and security is essential, and users must

respect everyone's privacy and comprehend the use of IoT devices before entering the Metaverse world. It's important to note that accessing and using Metaverse worlds come with security and privacy risks, especially on devices or systems with an Internet connection.

People should be divided into groups based on their location in urban or rural societies, as they have different levels of access to technology. Urban areas often have greater accessibility to technology, including access to the metaverse, which has its own accessibility issues. However, prolonged use of technology can lead to health problems such as eye strain from mobile phone use or dizziness from using large VR AR devices. Some individuals may also have limitations due to health issues such as uneven fluid in their ears. Metaverse users should be equipped with the necessary tools and applications to use the metaverse safely and securely. It is essential to have a protection system for devices and applications to maintain the confidentiality of data and ensure a secure connection. Users must understand how to use the application as each application has both advantages and disadvantages. Privacy is a significant issue and establishing international standards for equipment and health matters is necessary. At present, access to various devices and applications is limited to specific groups due to budget, personal preferences, or fascination with technology. However, there are security issues related to collecting data and movement, such as with iPhone devices storing all data when moved. Backdoors and bad settings can also pose security risks, such as with Bitcoin Crypto Blockchain, where the wallet is not secure, and there is a chance of being hacked. Education about authentication is essential, and there are concerns about white-collar crime and violations of privacy in the metaverse. Government agencies and regulators must eventually be involved in regulating the virtual economy. The term "Domain" will replace the "26 Industries" of this world in the virtual economy, as it will be necessary to support security, privacy, and resilience one domain at a time. The word "Device" in the metaverse will flow according to the domain. The standardization of devices proposes that the initial phase use TIS with ISO27001, 27701, 20000, 30000, 18000, and 50000 as a baseline and then overlay with domains.

5.2.2Technology (H2): Devices used in the Metaverse may not provide adequate physical and cybersecurity for users. The designers of such devices should consider a variety of factors such as the age, gender, weight of the device, wear, mobility, and secure use of personal data of the people who will be accessing them. Currently, the design of these devices primarily focuses on their function, with safety considerations still being relatively small. For instance, from a physical perspective, using VR and walking in the Metaverse can lead to accidents when users walk into obstacles. From a cybersecurity standpoint, simply registering an App to use various devices with an insecure username/password or storing an insecure username/password can lead to future threats. This is considered a high risk, and conclusive comparative studies of equipment properties in various aspects, especially safety, may be scarce or unavailable due to the small number of device manufacturers in the market. Therefore, physical and cybersecurity devices and systems used in the Metaverse should be developed with a focus on safety.

You must evaluate how much personal data is being requested by the devices used with Metaverse, and whether it is necessary or not. Even if real data is required, there may still be insufficient privacy protection. Random checks should be conducted to identify hidden or undocumented features in the products. Access, including maintenance and repairs, must ensure that data remains secure throughout the device's lifecycle. Data providers should not be forced to provide data to the device without their consent. Although there are universal principles, oversight of designers in the Metaverse world may not always be followed by developers. The platform has not yet been regulated in accordance with international legal requirements or penalties, and privacy risks still exist. Because hardware devices rely on software to function, there may be undiscovered vulnerabilities that could be exploited by cyber attackers. Furthermore, the device must be linked to a user account and an internet connection, making privacy management highly dependent on user behavior.

There is currently no direct supervisory authority or regulatory framework in place to address the unique challenges presented by the metaverse, such as eligibility requirements for audits and data usage. Given that only a few mainstream platform developers own relatively monopolized devices that are popularly used, it is difficult to verify or ensure reliability.

5.2.3Process (H3): In terms of the security and privacy aspects of deploying the Metaverse in Thailand, many processes have yet to be defined to support a comprehensive implementation. This includes an educational process to guide beginners and advanced users. The public and private sectors should establish a process to educate people from all sectors of society in various areas of Metaverse use, in order to identify channels and opportunities for the greatest benefit to organizations or businesses. Sufficient knowledge should be provided on the use of applications in various sectors, along with ethics for the new normal that will become standard in the future. This should encompass all dimensions of ethics, including processes for vaccination and cybersecurity awareness.

Cybersecurity has been compared to drunk driving before, but National Security Awareness Day has yet to be seen. However, the National Cybersecurity Board is now working to make it happen by promoting awareness and encouraging safe smartphone use before sharing personal information. The national strategy should be adjusted to place more emphasis on these issues. Cyber attacks are not limited to hacker, virus, and malware attacks on individuals. For example, billboards that encourage investment in cryptocurrency without awareness have highlighted the issue of education. Research from the University of San Francisco shows that low-income individuals with inadequate access to digital literacy may not be able to protect themselves. It would be beneficial for the government and Thai Health to promote public education, but it must be led by regulators with influence. The challenge is finding the right approach, and there are only a few individuals with the expertise to do so.

Regarding security and privacy testing, it is recommended that a National LAB be established to test and rank security benchmarks. The National Cyber Security Board (NCSB) has already published a Critical Information Infrastructure (CII) ranking of cybersecurity levels. A National LAB that ranks products would allow customers to make informed decisions. Although NECTEC, the National Standard, exists, a National LAB should be established to control matters concerning national security.

The process of educating people is diverse and can be undertaken in many dimensions. It can start with educational institutions such as schools and universities including it in their curriculum. Public sector government agencies can also provide knowledge about new technology to students and the public, with hosts assigned to each group. Regulators should provide clear knowledge on the testing process and ranking of related technologies through their respective agencies. The government should pay attention and raise awareness about the use of Metaverse and its potential applications in various industries. This can begin with a focus on each domain of the metaverse, such as understanding the economy, business models, and technologies such as VR, AR, and XR.

In other processes, both public and private sectors should have a structured approach to educate themselves on the laws and regulations related to Metaverse to ensure its proper and legal use. However, before reaching that point, it is necessary to examine how the law can be enhanced or developed to address the concerns raised by Metaverse. There should be an organization or cooperation between various organizations to coordinate the determination of regulations and to designate a person who is directly responsible for this task. This should also include campaigns and awareness-raising activities related to relevant laws such as the Computer Crime Act, the Cyber Crime Act, the Personal Data Act, as well as laws related to sexual abuse, defamation, and others.

The public and private sectors should have a process to educate the various committees on the Metaverse to regulate its use properly. Achieving adequate oversight is important to not deprive ourselves of opportunities for innovation. Thailand could establish a committee to clearly regulate the use of the virtual world and issue concrete measures for compliance. This committee could include related regulators such as EDTA, NCSB, and various regulatory offices. Its aim would be to provide preliminary procedures and guidelines and disseminate recommendations to third parties so that the regulator's regulations align with the business sector.

In particular, the sector that owns or participates in the production or distribution of content entering the metaverse world should be provided with specific clarity in both structure and content process in relation to the law that the regulator oversees. Since the government that is the regulator may be outdated or not up to date with technology, they should regulate in principle such as not acting for fraud or fraud under good morals and ethics of reasonable people. These regulators will be closer to the entities or business owners who produce or distribute the content than those outside the sector and will have a better understanding of the technology and business infrastructure, which can potentially support growth in that business. Ultimately, the Metaverse will involve all sectors and therefore requires knowledge and understanding to provide appropriate support.

The public and private sectors should establish procedures to verify the security of devices and applications used in the metaverse in terms of access, storage of personal data, and confidentiality. It is important for users to have peace of mind knowing that there is a monitoring agency ensuring their safety. The concept of regulation should adopt King Rama IX's guidance, "*which states that the goal is not to make everyone a good person, but to promote good people and control bad people from having power to prevent trouble and chaos".*

Supervision should have stages of enforcement to avoid hindering the growth and development of technology. Standards issued by regulators should only apply to important aspects of the metaverse that have a broader social impact. Finally, there should be a review process that periodically assesses the use of devices and applications, with reference cycles set according to version or technology changes and disseminated to relevant parties.

5.2.4Law (H4):Important lessons can be learned from the crypto industry where excessive regulation can hamper innovation. If regulations become too strict, investors will move their investments to other countries, causing a loss of benefits for the country. Similarly, when talented individuals migrate elsewhere, it reduces the opportunity for growth. In order to prevent loss of opportunities in areas such as people, innovation, and country income, it is essential to have software and devices that are secure. Consumers expect to use devices safely, but there are no random security checks in place in Thailand. In contrast, in America, random checks detect backdoors, among other things. When everything is new, it can be difficult to set rules around it without hampering innovation. However, having no law in place can result in vulnerability. Thailand should have relevant laws specifically tailored to the use of Metaverse or other social media platforms to reduce interpretation and ensure proper enforcement. Justice institutions should be involved in the formulation of various technological laws. Two important things to focus on are: 1) Service providers must have measures to track and identify offenders and have a clear process of cooperating with competent officials to find offenders quickly. 2) Measures must be put in place to detect and punish those who violate, harass, cause disturbances, or commit any fraudulent acts.

In terms of the basic law, it's worth considering whether the PDPA Act needs to be interpreted and expanded to cover the Metaverse, and whether the Computer Crime Act also covers it. Prosecutors, judges, and lawyers may not have comprehensive knowledge in this area, so it's important to provide education and training to ensure they understand the technology. Laws must be flexible, easily amended, and able to keep pace with technological changes. Additional notices could be issued from the existing main laws, taking into account relevant content under acts such as the Computer Crime Act, the Cyber Crime Act, and the Personal Data Act.Metaverse and its relation to the law can be divided into two parts: 1) controlling activities to ensure orderliness, and 2) handling related offenses. Currently, cyber law is comprised of four main parts: the Cyber Act, Computer Act, PDPA Act, and Criminal Law. In terms of content, the offenses associated with advertising in the Metaverse may need additional details to be added to relevant laws. The Computer Crimes Act previously added offenses related to posting pictures of deceased persons. However, in the case of Metaverse, further clarifications may be necessary.

The Cyber Act focuses on CII and may not be directly applicable to the Metaverse. Hence, additional minor laws may need to be introduced to support the Metaverse. In terms of standards, it is recommended to agree on National Standards and National LAB that will provide additional measures to ensure the safety of equipment and systems.Other offenses related to content, such as illegal sales and advertising, have already been covered by existing online activity laws. However, with the integration of blockchain and cryptocurrency, prosecuting such offenses may become more difficult. Digital assets will also affect various investigations. Without specific laws to address such issues, prosecution may be challenging.The law must provide clear provisions, and interpretation should be accurate to ensure effective implementation. Updating legislation to align with actual Metaverse activities should be done in sections, identifying potential problems and updating legislation accordingly. Moreover, it is crucial to educate prosecutors, judges, and lawyers about technology to ensure comprehensive knowledge in handling cases related to the Metaverse.

The impact of the law on Metaverse can be divided into two parts - 1) how it affects the daily lives of Metaverse users and 2) its impact on prohibiting and enforcing certain activities. Good laws are important to ensure justice and coexistence in the virtual world, as Metaverse is not disconnected from the real world and can cause real-world damage. Regulatory measures are necessary in any action in the virtual world, as well as in the real world.

While some may argue that the law may have negative effects, specialists believe that it will have more positive effects in ensuring the safety of honest users and reducing the chances of misuse. Having a law in place can also minimize the potential damage that may occur better than not having one. In the end, the law will likely become a part of Metaverse users' daily lives, just as social media is today.The legislation related to Metaverse in Thailand should be comprehensive, especially in the areas of personal data security and cybercrime. The law should cover the following areas: 1) Development of related systems to ensure security and privacy. 2) Equipment security standards. 3) Maintaining order and dealing with criminals.

Other areas of law should also contain relevant content such as the supervision of personal data, behaviour, aggression in the virtual world, and the regulation of the use of money in the virtual world to prevent advantages or disadvantages, excessive speculation, fraud, and money laundering.The law should include mechanisms to regulate and prevent related offenses such as those under the Computer Crime Act, Cyber Crime Act, Personal Data Act, Sexual Abuse Act, Defamation, Fraud, and other criminally sanctioned acts, particularly those related to advertising, illegal sales, and civil damages claims.It is important to provide the scope of the laws to cover activities that occur on the Metaverse and ensure that they are characterized by litigation or damages provided for in these laws.

Since the Metaverse is primarily based in foreign countries, ensuring legal coverage of Metaverses abroad can be difficult. However, if it can be accomplished, it would be beneficial because it would aid in surveillance and tracking of offenders. The cyber world or the Metaverse is a borderless world, and jurisdiction has always been a legal challenge since the advent of the internet. It is essential to seek cooperation to make legal proceedings effective in a cross-border or globally oriented manner. Each country should have laws that protect its citizens so that they can travel anywhere in the world and use services safely. Various offenses that occur are not limited to specific countries, and the offender or victim may be in different jurisdictions. Coordination and determination of fault bases are necessary to classify the offense of both states, which will lead to the coordination of the arrest and extradition of offenders.

5.2.5Role (H5): As there is no direct agency involved in Metaverse, the NCSB oversees critical information infrastructure, and the private sector should play a role in educating users. The government regulates the big picture, for example, the Stock Exchange of Thailand (SET) regulates Digital Assets. However, this may not be a direct responsibility and could be not covered thoroughly due to potential misunderstandings. The Ministry of Digital Economy and Society (MDES) should oversee the technology, but it affects many parts of the government. Therefore, it is a matter of cooperation and collaboration. The Ministry of Interior works with the Ministry of Digital Affairs and the Ministry of Justice as a committee and oversight office. The platform's owner is based in Europe, making data sovereignty a challenging matter. Educating users is also challenging, but it is essential to address national security concerns. Regulatory measures should be implemented as much as possible, and penalties could be set as a minimum requirement in the beginning. It would be beneficial if regulators such as the NCSB and National Health Security Office (NHSO) cooperate. Direct and indirect regulators may be difficult to coordinate, requiring a regulator joint force. Soft power could be used to advise users, and the MDES should be involved in the big picture. The same group should handle education and supervision. If the group overseeing business cannot provide information, another group may be necessary, but it must be the same group in principle.In summary, the passage discusses the different agencies responsible for regulating and overseeing Metaverse in Thailand, as well as the need for collaboration among them. It emphasizes the challenges in regulating a platform owned by a foreign entity and educating users.

Specialists have provided general comments on roles, including the NCSB's responsibility for security and attack surveillance. The ETDA should focus on system development with regards to various aspects of security, and they issue standards related to business and society. The NCSB is responsible for issuing security laws. Regulators that are indirectly related to metaverses, such as The Energy Regulatory Commission, the Stock Exchange of Thailand , and the Bank of Thailand, are responsible for enforcing and monitoring use, response, transactions, and exchanges while staying up to date with various threats. This is because the virtual world of the future is the real world that must go hand in hand. The NCSB should only be responsible for the metaverse issues in the context of the Cyber Act, as well as other agencies, should be responsible according to their main legal authority. Each agency should be responsible for key legal issues under which they already have jurisdiction because they have knowledge and understanding of the infrastructure and business, which has links to other contexts than the metaverse. Educational institutions should provide direct knowledge and help learn lessons to be an intellectual capital for the future development of the virtual economy, being a role model for the next generation and ensuring sustainability.

5.2.6 Others: Thailand is not yet fully prepared for the challenges that the Metaverse will bring. Senior management must be convinced of the need to invest in personnel and infrastructure for this field. A dedicated team should be established to develop the necessary regulations, standards, and measures.Specialists should advise the government on the national strategy for the Metaverse, as this is a new form of hybrid warfare. While the Metaverse is still in its infancy, it will have a major impact on society.Currently, there is only a basic level of awareness of the various threats and effective response plans. It is crucial for people to understand the importance of security and privacy, as ignorance can lead to damage in the future.Mental health is another aspect of Metaverse access that presents a challenge. Technical issues, governance, and cyber sovereignty are also concerns. Existing laws must be comprehensive enough to address these issues. In case of incidents, users, service providers, and platform owners must know who to rely on for support. The police should have a presence in the Metaverse to ensure safety.The Ministry of Digital Economy and Society may take the lead in regulating the Metaverse or delegate this task to a dedicated agency. Policies and regulations could require Metaverse-related equipment to pass a proficiency test, or users may need to obtain consent or follow-up on usage.Regulating the Metaverse is comparable to regulating drone use, which requires permission to operate and specific frequency usage. A practical approach could be to have knowledge tests and awareness training, similar to drone regulations.Schools and universities have a role to play in educating students about the impact of the Metaverse on their health and wellbeing. They should also address addiction and the blurring of reality in the Metaverse. Overall, there is much to consider and prepare for before the Metaverse becomes a reality in Thailand.

Based on the data collected from an electronic focus group, it can be concluded that initially there were 25 factors in 5 components. However, after conducting the focus group and gathering ideas from 15 specialists, there were 131 factors in 5 components. The researchers then extracted and combined similar issues, resulting in 76 factors in 5 components. Finally, the researchers synthesized the factors and arrived at the final factor in 5 components, which consisted of 60 factors, as presented in Table 2.

Table 2. shows a synthesis of factors related to security and privacy.

Component	Initial Factors	Raw factors	Extraction factor	Final factors
People (H1)	5	32	25	15
Technology (H2)	5	13	8	11
Process (H3)	5	13	10	10
Law (H4)	5	30	15	12
Role (H5)	5	43	18	12
Total	25	131	76	60

The researchers administered an online opinion questionnaire to all 15 specialists to gather their opinions on the relevant factors. The questionnaire was a closed-ended questionnaire with a 7-level estimation scale, and it was conducted using Google Forms. The specialists were asked to express their opinions on the suitability of the factors. The results of the questionnaire are presented in Table 3.

Table 3. Results of questionnaire responses by specialists.

Q	E1	E2	E3	E4	E5	E6	E7	E8	E9	E10	E11	E12	E13	E14	E15
c1	6	6	5	6	7	7	7	6	7	6	7	6	6	6	6
c2	7	7	5	6	6	7	7	6	7	6	7	6	6	7	7
c3	7	6	5	6	7	7	7	6	7	6	7	6	7	6	7
c4	6	6	5	7	7	7	7	6	7	6	7	6	7	7	6
c5	7	6	5	6	6	7	7	6	7	7	6	7	7	5	7
c6	6	6	5	7	7	7	7	6	7	6	6	7	6	6	5
c7	6	6	5	6	6	7	7	6	7	7	7	7	5	7	7
c8	6	6	5	7	6	7	7	6	7	6	6	7	5	6	6
c9	6	6	5	7	6	7	7	6	7	6	7	6	5	6	6
c10	7	6	5	5	6	7	7	6	7	6	7	6	7	7	7
c11	7	6	5	7	6	7	7	6	7	6	6	7	7	6	6
c12	7	6	5	7	6	7	7	6	7	6	6	7	7	7	7
c13	6	6	5	7	6	7	7	6	7	7	6	7	6	6	6
c14	7	6	5	6	6	7	7	6	7	7	7	7	6	5	5
c15	5	6	5	6	6	7	7	6	7	6	7	7	5	7	6
c16	5	6	5	6	6	7	7	6	7	7	7	7	6	6	7
c17	6	6	5	6	7	7	7	6	7	7	7	7	7	7	7
c18	7	6	5	6	6	7	7	6	7	6	6	6	7	6	7
c19	7	6	5	6	6	7	7	6	7	7	6	6	6	7	6
c20	6	6	4	6	6	7	7	6	7	7	7	7	6	5	5
c21	6	6	4	6	6	7	7	6	7	7	7	7	6	5	7
c22	6	6	4	6	6	7	7	6	7	7	7	7	5	5	7
c23	7	6	4	6	7	7	7	6	7	6	7	7	7	5	7
c24	6	6	5	6	7	7	7	6	7	7	7	7	7	5	7
c25	7	6	5	6	7	7	7	6	7	7	7	7	6	5	6
c26	6	6	5	6	6	7	7	6	7	6	6	6	7	6	6
c27	6	6	6	5	6	7	7	6	7	6	7	6	5	6	6
c28	7	6	6	6	6	7	7	6	7	6	6	6	7	7	7
c29	6	6	6	6	6	7	7	6	7	7	6	6	6	6	7
c30	6	6	6	5	6	7	7	6	7	7	7	6	7	6	7
c31	7	6	6	5	6	7	7	6	7	7	6	7	5	7	6
c32	6	6	6	5	6	7	7	6	7	6	7	7	7	7	6
c33	6	6	6	5	7	7	7	6	7	6	6	7	6	5	6
c34	6	6	6	5	6	7	7	6	7	7	6	7	6	7	6
c35	6	6	6	5	6	7	7	6	7	7	7	7	7	7	7
c36	6	6	6	5	7	7	7	6	7	7	7	7	7	6	6
c37	6	6	6	7	7	7	7	6	7	7	7	7	6	7	7
c38	7	6	6	6	7	7	7	6	7	6	7	7	6	6	6
c39	6	6	6	5	6	7	7	6	7	7	7	7	7	6	5
c40	6	6	6	5	6	7	7	6	7	7	7	6	7	7	7
c41	7	6	6	5	6	7	7	6	7	7	6	6	7	5	7
c42	6	6	6	5	6	7	7	6	7	7	6	7	7	7	7
c43	5	6	6	5	6	7	7	6	7	7	6	7	7	6	6
c44	5	6	6	5	6	7	7	6	7	7	6	7	7	7	6
c45	6	6	6	5	6	7	7	6	7	7	7	7	7	5	6
c46	7	6	6	5	6	7	7	6	7	7	7	6	6	7	7
c47	7	6	6	7	6	7	7	6	7	7	7	6	6	7	5
c48	6	6	6	6	6	7	7	6	7	6	7	6	6	6	6
c49	7	6	6	6	5	7	7	6	7	7	6	6	6	7	7

c50	6	6	6	6	6	7	7	6	7	7	7	7	6	7	6
c51	6	6	6	5	6	7	7	6	7	6	6	7	7	6	6
c52	6	6	6	5	6	7	7	6	7	6	6	7	7	6	5
c53	6	6	6	5	6	7	7	6	7	7	7	7	6	7	7
c54	7	6	6	6	6	7	7	6	7	7	7	7	7	5	7
c55	7	6	6	6	6	7	7	6	7	7	7	7	6	5	6
c56	7	6	6	6	6	7	7	6	7	6	6	7	7	5	6
c57	6	6	6	6	6	7	7	6	7	6	6	6	7	7	6
c58	7	6	6	6	6	7	7	6	7	6	6	6	7	7	7
c59	6	6	6	5	6	7	7	6	7	6	7	7	6	6	7
c60	6	6	6	5	6	7	7	6	7	7	7	7	5	6	7

The researchers analyzed the data provided by all 15 specialists using a computer program based on the Fuzzy Analytic Hierarchy Process. As there were 15 specialists, the researchers calculated the Fuzzy membership as follows.

$$Q1 = ((n+1)r)/4 = ((15+1)1)/4 = 16/4 = 4$$

$$Q2 = ((n+1)r)/4 = ((15+1)2)/4 = 32/4 = 8$$

$$Q3 = ((n+1)r)/4 = ((15+1)3)/4 = 48/4 = 12$$

Based on the values of Q1, Q2, and Q3, as determined by the expert opinions on the questions, it can be concluded that the member in position 4 corresponds to the value of Q1, the member in position 8 corresponds to the value of Q2, and the member in position 12 corresponds to the value of Q3. The accepted security and privacy factors for Metaverse adoption in Thailand, as determined by using a Threshold of 0.91 are presented in Tables 4 and 5.

Table 4 Specialists' opinion data table after setting Q1, Q2, Q3.

	E1	E2	E3	E4	E5	E6	E7	E8	E9	E10	E11	E12	E13	E14	E15	Q3	Q2	Q1	IQ
c1	6	6	5	6	7	7	7	6	7	6	7	6	6	6	6	6	6	6	0
c2	7	7	5	6	6	7	7	6	7	6	7	6	6	7	7	6	6	6	0
c3	7	6	5	6	7	7	7	6	7	6	7	6	7	6	7	6	6	6	0
c4	6	6	5	7	7	7	7	6	7	6	7	6	7	7	6	6	6	7	-1
c5	7	6	5	6	6	7	7	6	7	7	6	7	7	5	7	7	6	6	1
c6	6	6	5	7	7	7	7	6	7	6	6	7	6	6	5	7	6	7	0
c7	6	6	5	6	6	7	7	6	7	7	7	7	5	7	7	7	6	6	1
c8	6	6	5	7	6	7	7	6	7	6	6	7	5	6	6	7	6	7	0
c9	6	6	5	7	6	7	7	6	7	6	7	6	5	6	6	6	6	7	-1
c10	7	6	5	5	6	7	7	6	7	6	7	6	7	7	7	6	6	5	1
c11	7	6	5	7	6	7	7	6	7	6	6	7	7	6	6	7	6	7	0
c12	7	6	5	7	6	7	7	6	7	6	6	7	7	7	7	7	6	7	0
c13	6	6	5	7	6	7	7	6	7	7	6	7	6	6	6	7	6	7	0
c14	7	6	5	6	6	7	7	6	7	7	7	7	6	5	5	7	6	6	1
c15	5	6	5	6	6	7	7	6	7	6	7	7	5	7	6	7	6	6	1
c16	5	6	5	6	6	7	7	6	7	7	7	7	6	6	7	7	6	6	1
c17	6	6	5	6	7	7	7	6	7	7	7	7	7	7	7	7	6	6	1
c18	7	6	5	6	6	7	7	6	7	6	6	6	7	6	7	6	6	6	0
c19	7	6	5	6	6	7	7	6	7	7	6	6	6	7	6	6	6	6	0
c20	6	6	4	6	6	7	7	6	7	7	7	7	6	5	5	7	6	6	1
c21	6	6	4	6	6	7	7	6	7	7	7	7	6	5	7	7	6	6	1
c22	6	6	4	6	6	7	7	6	7	7	7	7	5	5	7	7	6	6	1
c23	7	6	4	6	7	7	7	6	7	6	7	7	7	5	7	7	6	6	1
c24	6	6	5	6	7	7	7	6	7	7	7	7	7	5	7	7	6	6	1
c25	7	6	5	6	7	7	7	6	7	7	7	7	6	5	6	7	6	6	1
c26	6	6	5	6	6	7	7	6	7	6	6	6	7	6	6	6	6	6	0

c27	6	6	6	5	6	7	7	6	7	6	7	6	5	6	6	6	6	5	1
c28	7	6	6	6	6	7	7	6	7	6	6	6	7	7	7	6	6	6	0
c29	6	6	6	6	6	7	7	6	7	7	6	6	6	6	7	6	6	6	0
c30	6	6	6	5	6	7	7	6	7	7	7	6	7	6	7	6	6	5	1
c31	7	6	6	5	6	7	7	6	7	7	6	7	5	7	6	7	6	5	2
c32	6	6	6	5	6	7	7	6	7	6	7	7	7	7	6	7	6	5	2
c33	6	6	6	5	7	7	7	6	7	6	6	7	6	5	6	7	6	5	2
c34	6	6	6	5	6	7	7	6	7	7	6	7	6	7	6	7	6	5	2
c35	6	6	6	5	6	7	7	6	7	7	7	7	7	7	7	7	6	5	2
c36	6	6	6	5	7	7	7	6	7	7	7	7	7	6	6	7	6	5	2
c37	6	6	6	7	7	7	7	6	7	7	7	7	6	7	7	7	6	7	0
c38	7	6	6	6	7	7	7	6	7	6	7	7	6	6	6	7	6	6	1
c39	6	6	6	5	6	7	7	6	7	7	7	7	7	6	5	7	6	5	2
c40	6	6	6	5	6	7	7	6	7	7	7	6	7	7	7	6	6	5	1
c41	7	6	6	5	6	7	7	6	7	7	6	6	7	5	7	6	6	5	1
c42	6	6	6	5	6	7	7	6	7	7	6	7	7	7	7	7	6	5	2
c43	5	6	6	5	6	7	7	6	7	7	6	7	7	6	6	7	6	5	2
c44	5	6	6	5	6	7	7	6	7	7	6	7	7	7	6	7	6	5	2
c45	6	6	6	5	6	7	7	6	7	7	7	7	7	5	6	7	6	5	2
c46	7	6	6	5	6	7	7	6	7	7	7	6	6	7	7	6	6	5	1
c47	7	6	6	7	6	7	7	6	7	7	7	6	6	7	5	6	6	7	-1
c48	6	6	6	6	6	7	7	6	7	6	7	6	6	6	6	6	6	6	0
c49	7	6	6	6	5	7	7	6	7	7	6	6	6	7	7	6	6	6	0
c50	6	6	6	6	6	7	7	6	7	7	7	7	6	7	6	7	6	6	1
c51	6	6	6	5	6	7	7	6	7	6	6	7	7	6	6	7	6	5	2
c52	6	6	6	5	6	7	7	6	7	6	6	7	7	6	5	7	6	5	2
c53	6	6	6	5	6	7	7	6	7	7	7	7	6	7	7	7	6	5	2
c54	7	6	6	6	6	7	7	6	7	7	7	7	7	5	7	7	6	6	1
c55	7	6	6	6	6	7	7	6	7	7	7	7	6	5	6	7	6	6	1
c56	7	6	6	6	6	7	7	6	7	6	6	7	7	5	6	7	6	6	1
c57	6	6	6	6	6	7	7	6	7	6	6	6	7	7	6	6	6	6	0
c58	7	6	6	6	6	7	7	6	7	6	6	6	7	7	7	6	6	6	0
c59	6	6	6	5	6	7	7	6	7	6	7	7	6	6	7	7	6	5	2
c60	6	6	6	5	6	7	7	6	7	7	7	7	5	6	7	7	6	5	2

Table 5 provides a summary of the analysis results obtained using Fuzzy and the accepted factors.

C	Average			Crisp	0.91
1	0.783	0.923	0.993	0.900	Rejected
2	0.813	0.943	0.993	0.917	Accepted
3	0.813	0.943	0.993	0.917	Accepted
4	0.813	0.943	0.993	0.917	Accepted
5	0.797	0.933	0.987	0.906	Rejected
6	0.777	0.920	0.987	0.894	Rejected
7	0.797	0.933	0.987	0.906	Rejected
8	0.767	0.913	0.987	0.889	Rejected
9	0.767	0.913	0.987	0.889	Rejected
10	0.797	0.933	0.987	0.906	Rejected
11	0.803	0.937	0.993	0.911	Accepted
12	0.823	0.950	0.993	0.922	Accepted
13	0.793	0.930	0.993	0.906	Rejected
14	0.770	0.917	0.980	0.889	Rejected
15	0.760	0.910	0.980	0.883	Rejected
16	0.787	0.927	0.987	0.900	Rejected
17	0.833	0.957	0.993	0.928	Accepted

C	Average			Crisp	0.91
31	0.787	0.927	0.987	0.900	Rejected
32	0.803	0.937	0.993	0.911	Accepted
33	0.767	0.913	0.987	0.889	Rejected
34	0.793	0.930	0.993	0.906	Rejected
35	0.823	0.950	0.993	0.922	Accepted
36	0.813	0.943	0.993	0.917	Accepted
37	0.850	0.967	1.000	0.939	Accepted
38	0.820	0.947	1.000	0.922	Accepted
39	0.787	0.927	0.987	0.900	Rejected
40	0.813	0.943	0.993	0.917	Accepted
41	0.787	0.927	0.987	0.900	Rejected
42	0.813	0.943	0.993	0.917	Accepted
43	0.777	0.920	0.987	0.894	Rejected
44	0.787	0.927	0.987	0.900	Rejected
45	0.787	0.927	0.987	0.900	Rejected
46	0.813	0.943	0.993	0.917	Accepted
47	0.813	0.943	0.993	0.917	Accepted

18	0.793	0.930	0.993	0.906	Rejected	48	0.790	0.927	1.000	0.906	Rejected
19	0.793	0.930	0.993	0.906	Rejected	49	0.803	0.937	0.993	0.911	Accepted
20	0.747	0.893	0.970	0.870	Rejected	50	0.820	0.947	1.000	0.922	Accepted
21	0.773	0.910	0.977	0.887	Rejected	51	0.783	0.923	0.993	0.900	Rejected
22	0.757	0.900	0.970	0.876	Rejected	52	0.767	0.913	0.987	0.889	Rejected
23	0.793	0.923	0.977	0.898	Rejected	53	0.813	0.943	0.993	0.917	Accepted
24	0.807	0.940	0.987	0.911	Accepted	54	0.823	0.950	0.993	0.922	Accepted
25	0.797	0.933	0.987	0.906	Rejected	55	0.803	0.937	0.993	0.911	Rejected
26	0.773	0.917	0.993	0.894	Rejected	56	0.793	0.930	0.993	0.906	Rejected
27	0.757	0.907	0.987	0.883	Rejected	57	0.800	0.933	1.000	0.911	Accepted
28	0.820	0.947	1.000	0.922	Accepted	58	0.820	0.947	1.000	0.922	Accepted
29	0.800	0.933	1.000	0.911	Accepted	59	0.793	0.930	0.993	0.906	Rejected
30	0.803	0.937	0.993	0.911	Accepted	60	0.787	0.927	0.987	0.900	Rejected

It can be concluded that the factors that affect the security and privacy of Metaverse adoption in Thailand, obtained from the literature review, electronic focus group, and Fuzzy data analysis, revealed that there were 5 components and 25 factors, as shown in Table 6. Finally, the model of this research as shown in Figure 2.

Table 6presents factors affecting the research.

Component	Factors
People (H1)	Awareness
	Cyber Threat
	Internet security and privacy
	Ethics
	Addictive
Technology (H2)	Secure devices
	National LAB
Process (H3)	Law Education Process
	The process of educating the direct regulator
	The process of educating the indirect regulator
	Ethical process
	The process of joint force of the regulator
	The process of educating metaverse in schools
Law (H4)	Legislation related to all dimensions of the usage
	Laws will affect the daily lives of users
	Laws in Thailand cover foreign metaverse systems
	Laws should be as comprehensive as possible for users, service providers and regulators
	Laws with good cooperation from international government agencies
	Issuing notices in addition to the existing main law
Role (H5)	Defines a body specifically responsible for overseeing laws
	Defines an organization responsible for providing knowledge
	Educational institutions should be responsible for educating
	Government agencies should work with other
	The National Cyber Security Board should be central of all action and oversight of all aspects
	Establishment of the Virtual World Specially Agency

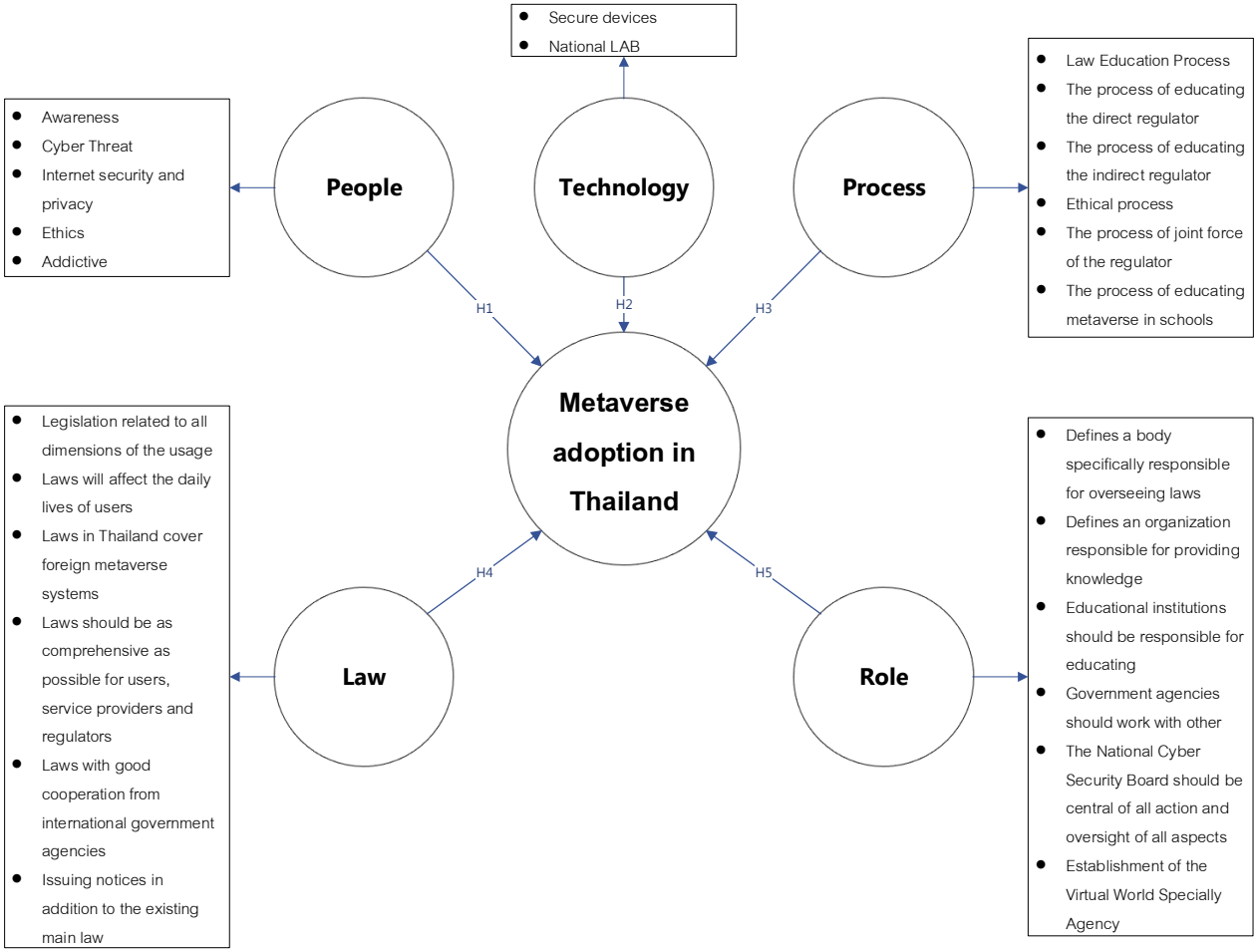

Figure 2. Metaverse adoption model

6. Conclusion

Based on the research and its results, it can be concluded that conducting electronic focus groups via the Zoom application, in addition to utilizing open-ended online questionnaires with Google Forms, aided in the collection of more comprehensive information from specialists. As a result of time constraints and the opinions of specialists in the electronic focus group, many of them utilized the open-ended online questionnaires to express their views in greater detail. The research team also greatly benefited from the recorded responses in the open-ended online questionnaire.During the data analysis of the closed-ended questionnaires, a 7-level estimation scale was used to query the specialists with a computer program based on the Fuzzy Analytic Hierarchy Process. This approach yielded clear analytical results that helped the specialists confirm their opinions on the factors contributing to the security and privacy factors for metaverse adoption in Thailand. All factors analyzed passed the acceptance criterion of 0.91 and were deemed suitable for use as security and privacy factors for metaverse adoption in Thailand.The research team found that using electronic focus groups via Zoom application, coupled with open-ended online questionnaires with Google forms, was an effective way to collect more complete information from specialists. Despite time constraints and limited opportunities for feedback during the electronic focus groups, many specialists were able to express their views extensively through the open-ended online questionnaires. Additionally, the research team found the recording of these questionnaires to be a valuable resource.

The research conducted to determine the security and privacy factors that influence the adoption of Metaverse in Thailand led to the identification of five components with a total of 25novel factorsare:

1. **People (H1)**- consisting of 5 factors as follow: Awareness, Cyber Threat, Internet security and privacy, Ethics, and Addictive.
2. **Technology (H2)** - consisting of 2 factors as follow: Secure devices, and National LAB.
3. **Process (H3)** - consisting of 6 factors as follow: Law Education Process, The process of educating the direct regulator, The process of educating the indirect regulator, Ethical process, The process of joint force of the regulator, and The process of educating metaverse in schools.
4. **Law (H4)**- consisting of 6 factors as follow: Legislation related to all dimensions of the usage, Laws will affect the daily lives of users, Laws in Thailand cover foreign metaverse systems, Laws should be as comprehensive as possible for users, service providers and regulators, Laws with good cooperation from international government agencies, and Issuing notices in addition to the existing main law.
5. **Role (H5)** - consisting of 6 factors as follow: Defines a body specifically responsible for overseeing laws, Defines an organization responsible for providing knowledge, Educational institutions should be responsible for educating, Government agencies should work with other, The National Cyber Security Board should be central of all action and oversight of all aspects, and Establishment of the Virtual World Specially Agency.

The research utilized electronic focus groups via the Zoom application coupled with open-ended online questionnaires using Google Forms. These methods proved to be effective in collecting more complete information from specialists. Additionally, data analysis was conducted using a computer program based on the Fuzzy Analytic Hierarchy Process and a 7-level estimator was used to query specialists, resulting in clear analytical results. All factors passedthe acceptance criterion at 0.91, confirming their use as security and privacy factors for Metaverse adoption in Thailand.

The novelfactors found are consistent with the National Cyber Security Strategy 2017-2021 (2017), Sumaporn (Srisoonthorn) Manasan (2021), Jin Kim (2021), Jon Radoff (2021), L.-H. Lee, T. Braud, P. Zhou, L. Wang, D. Xu, Z. Lin, A. Kumar, C. Bermejo, and P. Hui (2021), Leenes, R. E (2008, 2009), Noppadon Ratanavaraha, Chetneti Srisa-An (2023), and Skinner, Geoff & Han, Song & Chang, Elizabeth (2006).

7. Suggestion

The researchers should conduct a corroborative study with a large population of relevant individuals to confirm the results of this study and find research methods for identifying the key factors affecting Metaverse adoption in Thailand.

References

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

ETDA. (2021). ICT Law Center. Retrieved from https://ictlawcenter.etda.or.th

EverydayMarketing. (2022). Retrieved from https://www.everydaymarketing.co/trend-insight/insight-thailand-digital-stat-2022-we-are-social/

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

Jin Kim. (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

Jittipong L. (2021). Metaverse Metaverse ในอดีต-ปัจจุบันและอนาคตของเมตะเวิร์สคืออะไร. Marketing Tech Thailand. Retrieved from https://www.martechthai.com/technology/what-is-metaverse/

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

Joo-Eon JEON. (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

Ketkanok Urwongse. (2019). Focus group discussion: Effective qualitative data collection technique. Retrieved from https://so05.tci-thaijo.org/index.php/edjour_stou/article/view/182081

Kim J. L. Nevelsteen. (2018). Virtual world, defined from a technological perspective and applied to video games, mixed reality, and the Metaverse. Retrieved from https://onlinelibrary.wiley.com/doi/pdf/10.1002/cav.1752?casa_token=z8u_UbP4MUwAAAAA:fu_OX_VyBwjmV3BoMSfDghbnIXAKvj8Byzak3jSPXDEkkZ5rdU7N9QzuLQwNiVNfGYAdm1NWmPrm

Kultida T. (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.

L.A. Zadeh. (1965). Fuzzy sets, Information and Control, Volume 8, Issue 3, 1965, Pages 338-353, ISSN 0019-9958. Retrieved from https://www.sciencedirect.com/science/article/pii/S001999586590241X

L.-H. Lee, T. Braud, P. Zhou, L. Wang, D. Xu, Z. Lin, A. Kumar, C. Bermejo, and P. Hui. (2021) All one needs to know about metaverse: A complete survey on technological singularity, virtual ecosystem, and research agenda, arXiv preprint arXiv:2110.05352.

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.

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.

Marisol Hernández Hernández, Luis Alfonso Bonilla Cruz, Samuel Olmos Peña. (2022).Technology and Innovation in Organizations Using Fuzzy Systems.TEM Journal, 11(4), 1460-1468.Hill/publication/328146802_Metaverse_libraries_Communities_as_resources/links/5bbb89854585159e8d8c429b/Metaverse-libraries-Communities-as-resources.pdf

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

Natalia Poddubnaya , Tatyana Kulikova , Alexander Ardeeva and Polina Alekseeva. (2020). Formation of Digital Literacy of Students by Means of Virtual and Augmented Reality Technologies. 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

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

Noppadon Ratanavaraha, Chetneti Srisa-An. (2023). Critical Factors of Readiness Model for Metaverse Security and Privacy Adoption. Retrieved from https://www.eurchembull.com/uploads/paper/95883774fdca3d7bc0cd203fd69dbe18.pdf

Silvana Trimi, Sanggun Lee, Mincheol Kang. (2011). Innovation and imitation effects in Metaverse service adoption. Retrieved from https://www.academia.edu/26901253/Innovation_and_imitation_effects_in_Metaverse_service_adoption.

Skinner, Geoff & Han, Song & Chang, Elizabeth. (2006). Defining and Protecting Meta Privacy: A New Conceptual Framework Within Information Privacy. 101 - 101. 10.1109/ICDEW.2006.46.

Sumaporn (Srisoonthorn) Manasan. (2021). Metaverse: Law and Future in a Parallel World. Retrieved from https://www.bangkokbiznews.com/columnist/973315

Thongchai P. (2012). Development of criteria for selection of research consultants, Research Methodology & Cognitive Science, (9)2, 30-40.