CRITICAL FACTORS OF READINESS MODEL FOR METAVERSE SECURITY AND PRIVACY ADOPTION

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

Article History: **Received:** 12.12.2022 **Revised:** 29.01.2023 **Accepted:** 15.03.2023

Abstract

Metaverse adoption has increased recently while security and privacy concerns have also grown simultaneously. Currently, there is no readiness model for Metaverse security and privacy adoption. EFA, CFA, and Fuzzy logic techniques were applied. The purpose of this research is to identify critical factors of readiness model for Metaverse security and privacy adoption. According to a survey, our experiment was developed based on 4 main categories. From those categories, first found 20 important factors. Secondly, defined the top ten important factors called "critical factors". The total weight of critical factors is 56.46%. Finally, the formula equation of the readiness model is defined.

Keywords: Metaverse, Security, Privacy, Readiness Model.

[1] School of Digital Innovation Technology, Rangsit University, Pathumthani, Thailand
[2] School of Digital Innovation Technology, Rangsit University, Pathumthani, Thailand

Email:[1]noppadon.r64@rsu.ac.th, [2]chetneti@rsu.ac.th

DOI: 10.31838/ecb/2023.12.s3.250

1. Introduction

Thailand' s social media technology market value statistics in February 2021 showed that the number of online shopping is very high for all ages (EverydayMarketing., 2022). Social media technology's temptation of business value attracted more people to join the market. Due to digital disruption, digital transformation, and especially the COVID-19 crisis, the behavior of people has changed in the use of social media technology around the world. People must therefore be prepared to cope with the new way of life (New normal) and to adapt to the uncertainty of future crises.

Facebook (FB) is a famous application that can connect the whole world for decades. The drawback of the application is the user's real experience. AR and VR are two promising technologies for user real experience but still lack of platform. Second life launched in 2003 was the first online multimedia platform that gives a realistic user experience. The disadvantage of using second life is a technical issue in terms of speed and realism. The readiness of Metaverse recently can outcomes many problems including user experience, realism, speed, platform, and hardware limitations. Moreover, Metaverse allows humans able to interact with each other in digital form in their virtual world.

It can be seen that COVID-19 is a major catalyst for new media usage (EverydayMarketing., 2022). With the social distancing policy, people turn their attention to the form of Metaverse virtual events because they meet the needs of a live atmosphere. Metaverse was invented since 1992 from a novel "snow crash". This word drew attention again in 2021 when Facebook CEO changed company name to 'Meta'. His vision is to create a digital platform on the internet that let people can do things they can't do in the physical world. Metaverse combines two words "META" (Beyond) and "VERSE" (Universe). Metaverse Virtual activities are popular because they can attract people to participate. They are creating a sub-community group with modern features that allow participants to use their creativity and create new challenges. These activities allow people to build connections with others. The application has been adopted since announcement by Mark Zuckerberg; however, new threads of Metaverse are security and privacy issues.

From the global cybersecurity index (Global Cybersecurity Index., 2017) by the International Telecommunication Union (ITU), ITU measures commitment in five areas. Thailand ranks 7th in Asia-Pacific and 22nd among ITU member countries. Both for personal and business use; Therefore, Thailand must focus on formulating a national cybersecurity policy that is clear and practical. Lead to an efficient and timely response to cyber threats in domestic management and cooperation with foreign countries. The uses of cyberspace as a tool to commit crimes in various forms are increasing day by day. Cyber threats have been happening around the world. For example, a hack into the central bank of Bangladesh using SWIFT malware resulted in over $81 million in losses. A Survey by the Electronic Transactions Development Agency (Thailand) showed average Thai population spends 41.4 hours per week using the Internet. Misuse of cyberspace, such as using online media as a tool to spread extremist ideas or recruit members of groups to commit crimes or acts of terrorism. On the same token, Metaverse's concern about security and privacy also increased

According to H. Ning., H. Wang., Y. Lin., W. Wang., S. Dhelim., F. Farha., J. Ding., and M. Daneshmand. (2021), an important open issue on Metaverse is security and privacy. Therefore, worry about security and privacy on Metaverse since there is no standards on security and privacy. Skinner., Geoff & Han., Song & Chang., Elizabeth. (2006) also emphasized that there is a privacy risk issue in Metaverse. According to H. Ning. et al. (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), and Skinner., Geoff & Han., Song & Chang., Elizabeth. (2006), they all stated that security and privacy issues exist on Metaverse.
According to Statistics, Thailand have more than 50.05 million Thais use Facebook, representing 71.5% of the total Thai population (EverydayMarketing., 2022). Therefore, this research presents the novel Critical Factors of Readiness Model (CFRM) on 1129 survey samples in Thailand.
In another section of this paper, researchers presented related work in section II and then describe the methodology and results in sections III, IV and V. Finally, discussion and conclude in Section VI and VII respectively.

2. Literature Review

H. Ning., et al. (2021) stated that there are five open issues of metaverse including interaction problem, computation issues, Ethical issues, Security and privacy issue, and standard and compatibility.
Skinner., et al. (2006) defined a new terminology named "meta-information. It is metadata that contains identity or personal information and is classified as a Privacy Risk. Second Life is one of the pioneers Metaverse applications.
Leenes, R. E. (2008) exhibited certain privacy characteristics of Second Life. D. Grider. and M. Maximo. (2021) describe the virtual cloud economies of Metaverse and Web 3.0.
L.-H. Lee., et al. (2021) illustrated there is no privacy standard on metaverse yet. They urged that Privacy

threats should be protected in metaverse. Leenes, R. E., (2008) stated some of the privacy aspects of Metaverse (Case study of Second Life). Leenes also mentioned that the different forms of government, governance and policy make more privacy issues in metaverse.

Mufti., Yusuf & Niazi., Mahmood & Alshayeb., Mohammad & Mahmood., Sajjad. (2018) developed a model to assess security readiness levels for organizations. Their model consists of 12 categories and 76 best practices of security requirements.

L.-H. Lee., et al. (2021) urged to play attention to privacy issues in an early stage. They also stated that organizations should start from scratch in the designing stage on privacy issues for metaverse.

Q. Yang., Y. Zhao., H. Huang., and Z. Zheng., (2022) illustrated the powerful blockchain applications for an office work, social networks, NFT, finance games, etc. He also raises a real example of the blockchain-based game named "Axie Infinity" (Axie infinity., 2021). The game allows playing in real money transactions and trade in metaverse.

H. Duan., J. Li., S. Fan., Z. Lin., X. Wu., and W. Cai. (2021) proposed and developed a new metaverse prototype named CUHKSZ Metaverse using blockchain- technology. They illustrated that blockchain technology will move forward to the next era of metaverse.

W. Y. B. Lim., Z. Xiong., D. Niyato., X. Cao., C. Miao., S. Sun. and Q. Yang. (2022) proposed their surveys on metaverse adoption. Their research survey the key components including communication and networking, computation, and blockchain aspects. Alessandro Acquisti., and Ralph Gross. (2006) did research on privacy concerns on Facebook (FB). They found that some students are able to manage their privacy on FB while others cannot.

J. D. N. Dionisio., W. G. B. III., and R. Gilbert. (2013) stated that a metaverse can create the first complete virtual work because of four areas 1)immersive realism, 2) the ubiquity of access and identity, 3) interoperability and 4) Scalability.

Irfan., M., Putra., S. J., & Ramdhani., M. A. (2019) proposed an IT implementation readiness model for higher education. Their model consists of seven variables and 50 indicators. The purpose of their research is to find what are the successful factors of the readiness model on IT project implementation.

Mufti., et al., (2018) proposed a novel software engineering readiness model named " Security Requirements Engineering Readiness Model (SRERM) ". They claimed that the model demonstrated the readiness levels of Security Requirements Engineering in the software industry.

Sardjono . W. (2019) presented the methodology to develop readiness model and their equation. Jon Radoff. (2021) gave an interesting idea of the structure of Metaverse, dividing Metaverse into seven layers as follows 1)Infrastructure, 2)Human Interface, 3)Decentralization, 4)Spatial Computing, 5)Creator Economy, 6)Discovery, and 7)Experience.

Kim J. L. Nevelsteen., (2018) has defined Metaverse that will support the real-time operations. Thus, Metaverse will be infused with elements of the Internet that exist in the real World.

Silvana Trimi., Sanggun Lee., Mincheol Kang., (2011) who conducted research on Innovation and imitation effects in Metaverse service adoption, gave a clear definition of Virtual Worlds, Mirror Worlds, Augmented Reality, and Life logging. Metaverse roadmap. (2016) provides the first picture of Metaverse Scenarios by choosing from two main factors : 1) Identity focused, and 2) World-focused. There are four key areas of metaverse scenario as follows : 1)Augmentation, 2)Simulation, 3)Intimate and, 4)External.

Jin Kim. (2021) has analyzed data protection and found that the Virtual Reality user experience using Metaverse can be combined with education to achieve better learning outcomes.

Natalia Poddubnaya.,Tatyana Kulikova.,Alexander Ardeeva.,and Polina Alekseeva. (2020) from North Caucasus Federal University conducted a research study Formation of Digital Literacy of Students by Means of VR and AR Technologies.

Joo-Eon JEON. (2021), the research was founded on attractiveness, novelty, usability, interaction with Metaverse Platform, relevance to Virtual Worlds, Mirror Worlds, Augmented Reality, and Lifetime Recordings was impacted innovation on identity.

According to Sebastian, G. (2023) addressed the high level of metaverse cybersecurity risks, controls, and framework. This research gives the important cyber risks as follows 1) Data privacy issues, 2) Access risk, 3) Blockchain based NFT, Crypto currency vulnerabilities, 4) Platform/Application code vulnerabilities, 5) Algorithmic fairness, 6) API/Sensor security, 7) Data center/Cloud security, and 8) Network security. Finally, present the mitigating controls of those risks.

2. Methodology

This research is a mix methodology including both qualitative and quantitative. There are 3 steps for building the proposed CFRM. Firstly, the effective factors for CFRM are produced with qualitative using e-focus group. Secondly, the important factors are obtained with quantitative using questionnaire. Lastly, the critical factors are acquired in order to create a novel readiness formula.

Qualitative research with e-focus group.

3.1.1 Population and Sample were divided into 4 groups with total of 15 experts. Group 1 contains 2 members of the National Cyber Security Committee (NCSC). Group 2 Cybersecurity expertise in the private sector 4 persons. Group 3 University

professors or experts who are University lecturers or experts in Artificial Intelligence, Digital forensics, and Information Technology related to Virtual Reality 5 persons. Group 4 Metaverse experts by being involved in the development, and business related to Metaverse in Thailand 4 persons.

3.1.2 Research Tool used to collect data for this research was an e-Focus Group. (Ketkanok Urwongse., 2019) Data was collected through the Zoom application with careful planning to invite experts and prepare leading questions, main questions, and conclusion questions for these discussions to get answers to research. An e-Focus group must be a moderator who is responsible for ensuring that the group discusses the specific factors. Data were collected by an e-Focus Group with 15 experts, which will be analyzed by fuzzy set theory and the results will be used for the quantitative data in the next step.

3.1.3 Data Collection. The researchers collected data using an e-focus group from 15 experts via the zoom application. It takes time to process and collect data for a period of 3 months, starting from April to June 2022.

3.1.4 Data analysis uses the fuzzy set theory to sets and the uncertainty of members of a set. The ambiguity and uncertainty of the data from the answers to the opinion questionnaire from 15 experts can be examined by extracting only the relevant factor and indicator with an acceptance criterion of 0.83. It helps increase efficiency in selecting factors and indicators to match the decision of the researchers as much as possible and is suitable for multi-criteria decision-making. It helps resolves conflicting feeling among experts in scoring and fully help enable each expert to perform comments to measure the consensus of the expert group to be more accurate and complete. (Marisol Hernández Hernández., Luis Alfonso Bonilla Cruz., Samuel Olmos Peña., 2022), (Thongchai P., 2012) The step of the Fuzzy methodology as follows 1) Calculate the Fuzzy Score 2) Score Conversion 3) Select the best Factors and indicators. Table 1 shows the language variables and fuzzy number values in weighting.

Table 1. The language variables and fuzzy number values in weighting.

Linguistic	**Fuzzy numbers**
Very Important(VI)	(0.9, 1.0,1.0)
Important(I)	(0.7,0.85, 1.0)
Above Moderate(AM)	(0.5,0.7,0.9)
.Moderate(M)	(0.3,0.5,0.7)
Below Moderate(BM)	(0.1,0.3, 0.5)
Low Important(LI)	(0, 0.15,0.3)
Very Low Important(VLI)	(0, 0, 0.1)

To convert opinions on the Likert. The scale to be a member of fuzzy is based on the fuzzy average method $\frac{l+m+u}{3}$ of combining expert opinion. In this study, the researchers set a threshold of 0.83. Questions equal to or greater than 0.83 will show accepted and will be used. If it does not reach 0.83, it will be rejected and will not be used.

Quantitative research by collecting online questionnaires.

3.2.1 Population and Sample of this research were 66,300 members of the Thailand System Admin Group, 42,200 members of Metaverse Thailand, and 2233 members of the National CERT NCSA. (December 15, 2021) The sample of this research was 1129 members of the Thailand System Admin Group, Metaverse Thailand, and National CERT NCSA living in Thailand by simple random sampling.

3.2.2 Research Tools used to collect data for this research was an Online Questionnaire in which the researchers researched various research textbooks, Literature related to the opinion of 15 experts were collected and used to create a questionnaire with 7 Likert scale indicator.

3.2.3 Data Collection be sharing an online questionnaire via the Facebook page of the Thailand System Admin Group, Metaverse Thailand, and Sharing an Online Questionnaire via Line Application at LINE official Account of the National CERT NCSA group. Starting from August to October 2022 with a total questionnaire collection period of 3 months with 1129 respondents and checking the accuracy of all 1129 data that will be used for further statistical analysis.

3.2.4 Data Analysis.

1) General Data, analyzed by frequency and percentage.
2) Rating of opinions on various components of CFRM. EFA was performed using the principal component analysis method and the orthogonal rotation with the Varimax rotation method. Indicators with a component weight less than 0.4 or cross-loading more than 1 will be discarded and the indicators that remain in the model must have an Eigen Value greater than 1.0 as (Hair, J., Black,

W., Babin, B., Anderson, R. and Tatham, R., 2006), (Rangsungnoen G., 2011) which was suggested in the EFA.

3) Component analysis to validate CFRM with empirical data. 1st order CFA and 2nd order CFA were used by using factor analysis application. Parameters were estimated using the Maximum Likelihood (ML) method by considering the following statistical measures, Chi-square (X^2), Relative chi-square (X^2/df), Comparative Fit Index (CFI), Incremental Fit Index (IFI), Tucker-Lewis Index (TLI) and Root Mean Square Error of Approximation (RMSEA) to determine whether the component confirmatory development of model it consistent with empirical data. (Rangsungnoen G., 2011)

3.3 Develop the model.

Use the results from 3.2 to find the proportion of the relationship between main factors and other factors that affect to CFRM then develop the model. (Sardjono . W., 2019)

Experiment

4.1 Literature review and research conceptual framework.

Researchers have synthesized the data from the literature review which is related to the CFRM with a total of 51 factors and can be written in relation to the four main elements of metaverse as shown in Figure 1 and the conceptual framework as shown in Figure 2.

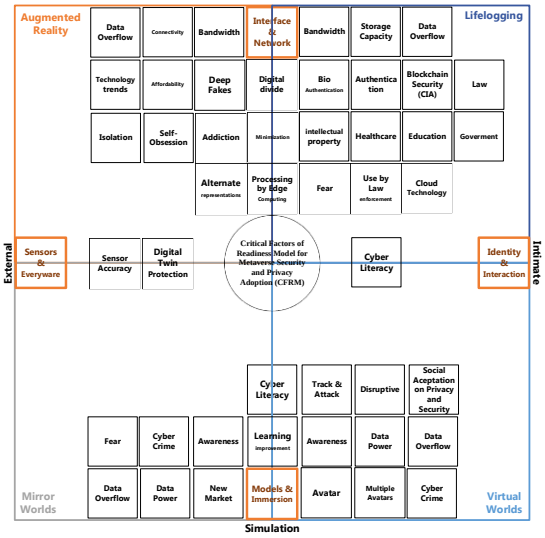

Figure 1. The four elements of Metaverse and security, privacy concerns from literature review.

Figure 2. CFRM conceptual framework.

4.2 Qualitative research with e-Focus group.

The e-Focus group was performed with 15 experts on April 23, 2022, and do not have any problems or errors. Before the e-focus group researchers designed 25 discussion factors after the e-focus group researchers found 131 factors in total. Metaverse knowledge has 32 factors, Technology Knowledge 13 factors, Knowledge process 13 factors, Law and Regulation 30 factors, and Role and Responsibility 43 factors concerned with CFRM. From the results, researchers design the Online questionnaire for quantitative research in 5 nodes with 64 factors, General information with 4 factors, Metaverse knowledge (KPE) with 15 factors, Technology knowledge (KTE) with 11 factors, Knowledge process (KPR) with 10 factors, Law and Regulation (LAW) 12 factors and Role and Responsibility (ROL) 12 factors. The online questionnaire was sent to 15 experts to confirm their opinion after getting the questionnaire back the fuzzy test was performed. The results of the fuzzy analysis show that all factors were accepted and used for quantitative research (Threshold=0.83, Max=0.939, Min=0.838, Avg.=0.903).

4.3 Quantitative Research with online questionnaire.

4.3.1 General information results were 540 female respondents, 586 males, and 3 alternative genders, representing 47.83%, 51.90%, and 0.26% respectively. Most of them were between the ages of 21-30 years old, 1011 people, followed by 31-40 years old, 55 people, representing 89.54% and 4.87% respectively. Most of the respondents were members of the Thailand System Admin Group, 38.6% followed by 27.5% of Metaverse Thailand members, and the third was a member of National CERT NCSA 18.6% and not a member of any group 15.2%.

4.3.2 EFA, results of testing the suitability of the study variable set. By analysis Kaiser-Meyer-Olkin (KMO) measure of Sampling Adequacy were found to be equal to 0.902, which is greater than 0.80, indicating that this set of variables is very suitable for component analysis according to Kim and Mueller's criteria. Bartlett's Test of Sphericity found that the variables There was a statistically significant correlation at the 0.000 level, indicating that the variables can be used to analyze components as shown in Table 2.

Table 2. EFA KMO and Bartlett's test results.

KMO		0.902
Bartlett's Test	Approx. Chi-Square	9971.306
	Df	190
	Sig.	0.000

The findings revealed that the studied variables could be analyzed as 4 factors which were Metaverse knowledge, Role and Responsibilities, Knowledge process, and Law and Regulation. The cumulative variance can explain up to 60.191% as shown in Table 3.

Table 3. EFA Rotated component Varimax method results.

Factor	**Component**			
	1	2	3	4
KPE11	0.749	0.035	0.238	-0.010
KPE12	0.728	0.055	0.200	-0.033
KPE13	0.812	-0.050	-0.031	0.213
KTE2	0.809	-0.014	-0.070	0.262
KTE3	0.809	0.007	-0.091	0.261
KTE4	0.786	0.031	-0.149	0.254
KTE5	0.748	0.000	-0.147	0.292
KPR1	0.027	0.393	0.587	0.028
KPR2	-0.005	0.221	0.759	0.116
KPR3	-0.018	0.252	0.756	0.035
KPR4	-0.014	0.356	0.609	0.090
LAW3	0.340	0.109	0.124	0.711
LAW4	0.262	0.098	0.059	0.815

LAW5	0.258	0.090	0.096	0.781
ROL2	-0.016	0.587	0.184	-0.075
ROL5	0.046	0.649	0.194	0.158
ROL6	0.012	0.655	0.244	-0.013
ROL7	-0.026	0.661	0.254	0.041
ROL9	0.031	0.667	0.041	0.249
ROL10	0.019	0.732	0.159	0.030
Eigenvalues	5.520	4.189	1.294	1.034
% of Variance	27.601	20.947	6.471	5.172
Cumulative %	27.601	48.548	55.019	60.191

When the factors are arranged in a single component and have a descriptive name corresponding to the components in order to correspond with the CFRM. The details are shown in Table 4.

Table 4. Assign factors to new component and assign component name.

Component	**Factor**
Metaverse Knowledge	1. Ethics in virtual world.
	2. Addiction in virtual world.
	3. Law and Regulation concerned with Metaverse.
	4. Secure devices for use with Metaverse.
	5. Devices that are privacy compatible with Metaverse.
	6. Monitoring the efficiency of data collection of used devices.
	7. Availability of devices and applications for privacy inspection.
Role and Responsibility	1. Designate a specific agency responsible for providing knowledge related to social media and metaverse.
	2. Schools should be responsible for educating them about social media and metaverse.
	3. Government agencies should work with other agencies such as safety, mental health, department of industrial promotion, etc. to provide comprehensive social media and metaverse services.
	4. The Ministry of Education should play a role in setting up educational curriculum and providing knowledge related to social media and metaverse in schools.
	5. The National Cyber Security Agency (NCSA) should be the center of action and oversight of all aspects of social media and metaverse.
	6. Set up a Thai Virtual World Security Agency (TVWSA) committee to be the center of operations and oversight of social media and metaverse in all dimensions.
Knowledge process	1. Education process for using Metaverse.
	2. Education process in term of concerned Law and Regulation.
	3. The process of educating the Regulators directly related to Metaverse.
	4. The process of educating the Regulators that are indirectly related to Metaverse.
Law and Regulation	1. The existing Laws related to metaverse are fully covered.
	2. The existing Laws related to metaverse are cover foreign metaverse systems.
	3. Laws related to metaverses of foreign countries are comprehensive and suitable for users.

4.3.3 1st order CFA to analyze the harmonization of CFRM with empirical data. The analysis results show that Metaverse Knowledge (KNW), Knowledge Process (KPR), Law and Regulation (LAW), and Role and Responsibility (ROL) measurement models consisted of 20 observed variables before model modification, there were still unqualified model fit indices (χ^2//df=5.455), which suggests that the model has not yet harmonized with the empirical data. Therefore, the model was modified by allowing 8 pairs of variances between the errors to be correlated. The results appeared after the model modification the measurement models are thus harmonized with empirical data. The model fit indices are as follows: χ^2//df=2.227, CFI=0.981, IFI=0.981, TLI=0.976, and RMSEA=0.033, all indices meet the specified criteria. The 1st-order CFRM is shown in Figure 3.

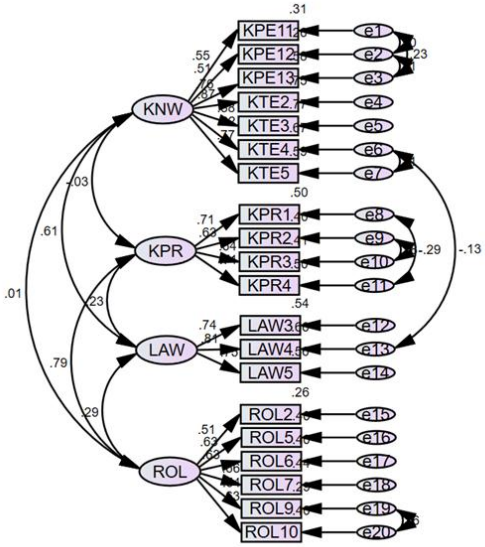

Figure 3. 1st order CFA CFRM fit indices results.

4.3.4 2nd order CFA of CFRM developed with empirical data. The analysis results show that Metaverse Knowledge (KNW), Knowledge Process (KPR), Law and Regulation (LAW), and Role and Responsibility (ROL) measurement models consisted of 20 observed variables before model modification, there were still unqualified model fit indices ($\square^2$/df=8.501, CFI=0.871, IFI=0.872, TLI=0.855, RMSEA=0.082), which suggests that the model has not yet harmonized with the empirical data. Therefore, the model was modified by allowing 53 pairs of variances between the errors to be correlated. The results appeared after the model modification the measurement models are thus harmonized with empirical data. The model fit indices are as follows : $\square^2$/df=2.994, CFI=0.977, IFI=0.977, TLI=0.962 and RMSEA=0.042, all indices meet the specified criteria. The 2nd order CFRM shown in Figure 4.

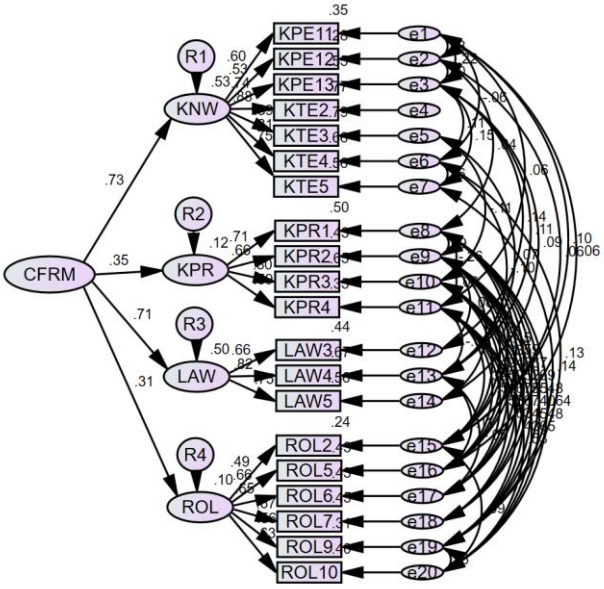

Figure 4. 2nd order CFA CFRM fit indices results.

The analysis of latent variables CFRM model Metaverse Knowledge (KNW), Knowledge Process (KPR), Law and Regulation (LAW), and Role and Responsibility (ROL). It turns out that the observed variables can be used to measure or explain the variance of these latent variables with statistical significance at the 0.001 level.

Latent variable KNW, Observer variables KPE11, KPE12, KPE13, KTE2, KTE3, KTE4, and KTE5 had standard component weights (λ) = 0.595, 0.530, 0.739, 0.878, 0.887, 0.812, and 0.747 respectively, which could explain (R^2) 35.4, 28.1, 54.6, 77.1, 78.7, 65.9, and 55.8 percent of the variance of latent

variable KNW, respectively. The constituent and the extracted mean-variance. (AVE) of KNW latent variables were 0.898 and 0.565, respectively, indicating that all 7 observational variables of latent variable KNW had good internal consistency and were suitable for measuring latent variable KNW.

Latent variable KPR, Observer variables KPR1, KPR2, KPR3, and KPR4 had λ=0.708, 0.656, 0.805, 0.594 respectively, which R^2 50.1, 43.0, 64.8, 35.3% respectively. CR and AVE were 0.787, 0.483 respectively, indicating that all 4 observational variables of latent variable KPR had good internal consistency and were suitable for measuring latent variable KPR.

Latent variable LAW, Observer variables LAW3, LAW4, and LAW5 had λ= 0.662, 0.821, 0.746 respectively, R^2 43.8, 67.4, 55.7% respectively. CR and AVE were 0.789, 0.556 respectively, indicating that all 3 observational variables of latent variable LAW had good internal consistency and were suitable for measuring latent variable LAW.

Latent variable ROL, Observer variables ROL2, ROL5, ROL6, ROL7, ROL9 and ROL10 had λ=0.487, 0.659, 0.652, 0.671, 0.559, 0.633 confidence (CR) respectively, which R^2 23.7, 43.4, 42.5, 45.0, 31.2, 40.1% respectively. CR and AVE were 0.782, 0.377 respectively, indicating that all 6 observational variables of latent variable ROL had good internal consistency and were suitable for measuring latent variable ROL.

Structural validity of each latent variable it turns out that latent variable 1) Metaverse Knowledge 2) Knowledge Process 3) Law and Regulation 4) Role and Responsibility is base on structural integrity in all respects as follows.

1) The weight of standard component is greater than 0.5 and is statistically significant (except ROL2).
2) The confidence coefficients of the observer variables were greater than 0.5 (except KPE11, KPE12, KPR2, KPR4, LAW3, ROL2, ROL5, ROL6, ROL7, ROL9, ROL10).
3) The component reliability of latent variables is greater than 0.7 and
4) The extracted mean variance of latent variables was greater than 0.5 (except KPR, ROL).

4.4 Critical factors of readiness model for Metaverse security and privacy adoption.

From 4.3 research results, CFRM consists of four main categories: 1) Metaverse Knowledge, 2) Knowledge process, 3) Law and Regulation, and 4) Role and Responsibility. Totally, there are 20 important factors that have an effect on CFRM in Figure 5. This research tries to find top 10 factors known as "critical factor".

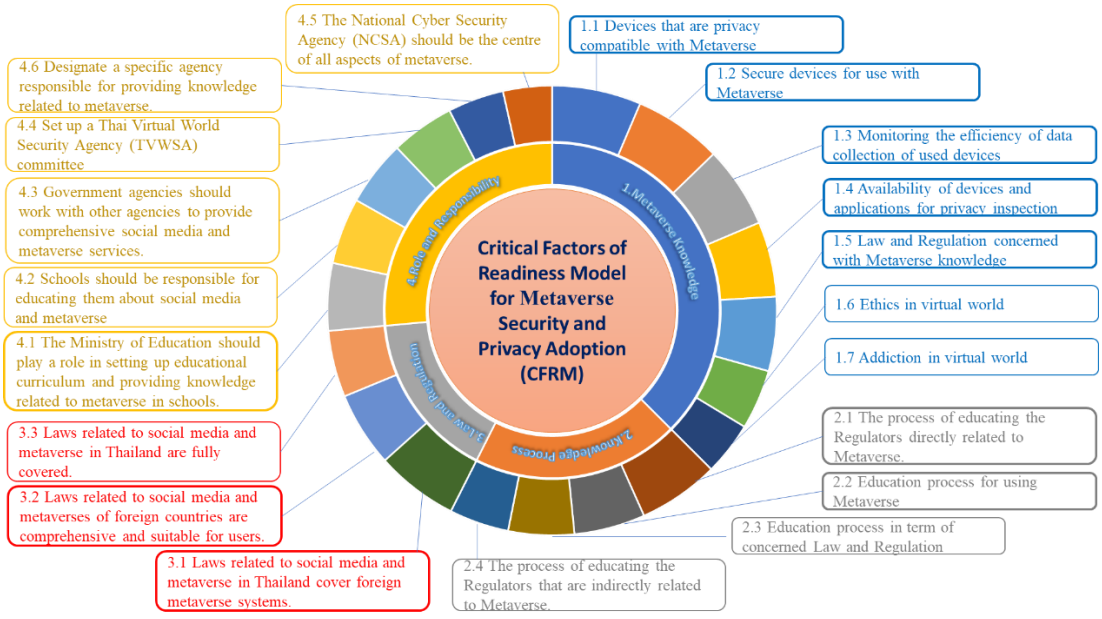

Figure 5. Developed the important factors of readiness model for Metaverse security and privacy adoption.

3. Experiment Result

In this study, researchers developed the critical factors of the readiness model for Metaverse security and privacy adoption (CFRM). The purpose of the CFRM is to assist Governance, Organizations measure their Metaverse security and privacy adoption readiness level. This framework is expected to improve users' security and privacy readiness and reduce their cyber and physical risk in the real world and virtual world.

From Figure 5, researchers concluded that critical factors of the readiness model as shown in Figure 5 consist of four main factors including 1. Metaverse Knowledge 2. Knowledge process 3. Law and Regulations and 4. Role and responsibility as shown in Table 5.

Table 5. 4 main factors and feature importance weight impact to CFRM.

CFRM		
Main Factors	**Description**	**Weight (%)**
1. Metaverse Knowledge	Miscellaneous related knowledge about Metaverse.	37.48
2. Knowledge Process	Law and Regulation related to Metaverse.	19.96
3. Law and Regulation	Process of Knowledge distribution in organizations.	16.10
4. Role and Responsibility	Role and responsibility of Organization, Agency, Regulator, etc., related to Metaverse.	26.45

1) Metaverse Knowledge main factor consists of 7 different factors as shown in Table 6.

Table 6. Metaverse Knowledge's factors and feature importance weight impact to CFRM.

1. Metaverse Knowledge	
Factors	**Weight (%)**
1.1 Devices that are privacy compatible with Metaverse	6.41
1.2 Secure devices for use with Metaverse	6.34
1.3 Monitoring the efficiency of data collection of used devices	5.87
1.4 Availability of devices and applications for privacy inspection	5.40
1.5 Law and Regulation concerned with Metaverse	5.34
1.6 Ethics in virtual world	4.30
1.7 Addiction in virtual world	3.83

2) Knowledge process main factor consists of 4 different factors as shown in Table 7.

Table 7. Knowledge process's factors and feature importance weight impact to CFRM.

2. Knowledge Process	
Factors	**Weight (%)**
2.1 The process of educating the Regulators directly related to Metaverse.	5.82
2.2 Education process for using Metaverse	5.12
2.3 Education process in term of concerned Law and Regulation	4.74
2.4 The process of educating the Regulators that are indirectly related to Metaverse.	4.29

3) Law and regulation main factor consist of 3 different factors as shown in Table 8.

Table 8. Law and regulation's factors and feature importance weight impact to CFRM.

3. Law and Regulation	
Factors	**Weight (%)**
3.1 Laws related to metaverse cover foreign metaverse systems.	5.93
3.2 Laws related to metaverses of foreign countries are comprehensive and suitable for users.	5.39
3.3 Existing Laws related to metaverse are fully covered.	4.78

4) Role and responsibility main factor consisting of 6 different factors as shown in Table 9.

Table 9. Role and responsibility's factors and feature importance weight impact to CFRM.

4. Role and Responsibility	
Factors	**Weight (%)**
4.1 The Ministry of Education should play a role in setting up educational curriculum and provides knowledge related to social media and metaverse in schools.	4.85
4.2 Schools should be responsible for educating them about social media and metaverse.	4.76
4.3 Government agencies should work with other agencies such as safety, mental health, department of industrial promotion, etc. to provide comprehensive social media and metaverse services.	4.71
4.4 Designate a Thai Virtual World Security Agency (TVWSA) committee to be the regulator of social media and metaverse.	4.57

4.5 The National Cyber Security Agency (NCSA) should be responsible for social media and metaverse.	4.04
4.6 Designate a specific agency responsible for providing knowledge related to social media and metaverse.	3.52

The top 10 out of 20 most important factors that are critical factors for Metaverse security and privacy adoption are as follows.

Factors 1, 2, 4, 6, 8 (29.40%): Metaverse devices and applications not secure, and privacy compatible. The data collected from each device to Metaverse should have been monitored. Devices and applications should have security and privacy inspection before a permit to use. And Laws and Regulations concerned with Metaverse must be educated.

Factors 3, 7 (11.3%): Laws and regulations concerned with Metaverse is not cover foreign metaverse systems and are suitable for users.

Factors 5, 9 (10.9%): There is no training standard course for Regulators on Metaverse knowledge. Government and private organizations do not have a process of education about Metaverse usage and all related laws for civil citizens.

Factor 10 (4.8%): The Ministry of Education should play a role in setting up an educational curriculum and providing knowledge related to social media and metaverse in schools.

The summation of the impact to CFRM of the top ten factors is 56.46%. That is why organizations should be aware of those factors before adopting Metaverse.

Figure 6 proposed critical factors of Readiness model (CFRM).

1) The first factor, Devices that are privacy compatible with Metaverse, has a readiness score of 0.064 which indicates the effectiveness of the knowledge concerned with Metaverse security and private adoption.
2) The second factor, Secure devices for use with Metaverse, has a readiness score of 0.063 which indicates the effectiveness of the knowledge concerned with Metaverse security and private adoption.
3) The third factor, monitoring the efficiency of data collection of used devices, has a readiness score of 0.059 which indicates the effectiveness of the knowledge concerned with Metaverse security and private adoption.
4) The fourth factor, the Availability of devices and applications for privacy inspection, has a readiness score of 0.059 which indicates the effectiveness of the knowledge concerned with Metaverse security and private adoption.
5) The fifth factor, Law and Regulation concerned with Metaverse, has a readiness score of 0.058 which indicates the effectiveness of the knowledge concerned with Metaverse security and private adoption.
6) The sixth factor, the process of educating the Regulators directly related to Metaverse, has a readiness score of 0.054 which indicates the effectiveness of the education concerned with Metaverse security and private adoption.
7) The seventh factor, the Education process for using Metaverse, has a readiness score of 0.054 which indicates the effectiveness of the education concerned with Metaverse security and private adoption.
8) The eighth factor, Existing Laws related to metaverse cover foreign metaverse systems, has a readiness score of 0.053 which indicates the effectiveness of the Laws concerned with Metaverse security and private adoption.
9) The ninth factor, Laws related to metaverses of foreign countries are comprehensive and suitable for users, and have a readiness score of 0.051which indicates the effectiveness of the Laws concerned with Metaverse security and private adoption.
10) The Tenth factor, The Ministry of Education should play a role in setting up educational curriculum and providing knowledge related to social media and metaverse in schools, has a readiness score of 0.048 which indicates the effectiveness of the Role and Responsibility concerned with Metaverse security and private adoption.

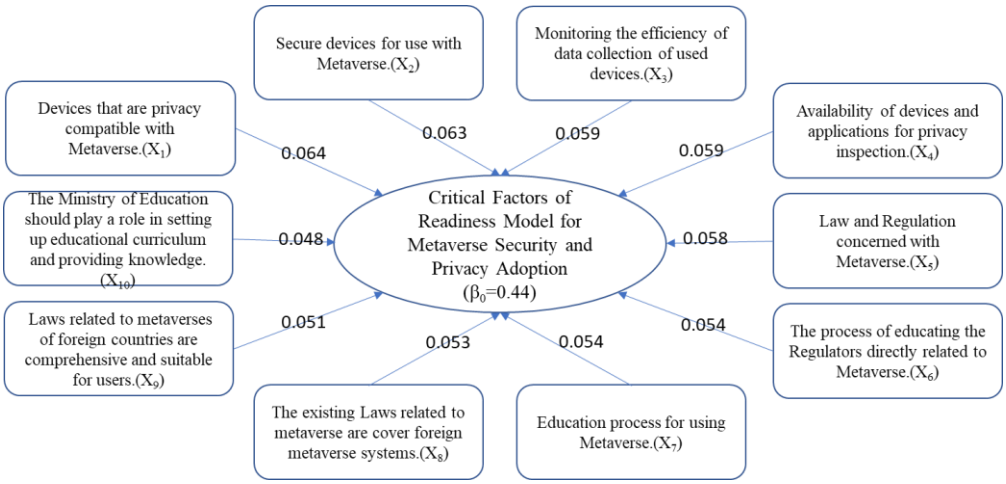

Figure 6. The proposed critical factors of Readiness model (CFRM).

$$R_{score} = 0.44 + 0.064X_1 + 0.063X_2 + 0.059X_3 + 0.059X_4 + 0.058X_5 + 0.054X_6 + 0.054X_7 + 0.053X_8 + 0.051X_9 + 0.048X_{10} \ldots.(eq\ 1)$$

An equation 1(eq1) shows a novel formula of readiness model.

R_{score} show the readiness score of organization. $\{X_1, X_2, X_3, X_4, X_5, X_6, X_7, X_8, X_9, X_{10}\}$ is range of 0 or 1.

4. Discussion

The proposed CFRM is built upon using the mixed methods research combined and integrated qualitative and quantitative research methods within a single study to present the framework, which is the same direction as Sardjono . W., (2019) and Chimmanee, K. & Jantavongso, S. (2021). Four critical factors of CFRM (Devices privacy, Secure devices, Data monitoring, and Privacy inspection) are the same way as Sebastian, G., (2023). The rest six critical factors (Law and regulation, Process of Regulators educating, Education process, Existing Laws, Suitable of Laws of foreign countries, Role of The Ministry of Education) are the same idea with further research of Sebastian, G., (2023). For the proposed equation (1), this equation is used for the readiness score, which is the same direction as Sardjono. W., (2019).

5. Conclusion

In this study, the readiness model for Metaverse security and private adoption was developed. This model was to identify critical factors of readiness based on 4 main categories of 20 important factors. The "critical factors" was then defined from the top ten important factors. The critical factor includes as follows. 1) Devices that are privacy compatible 2) Secure devices for use with Metaverse 3) Monitoring the efficiency of data collection of used devices 4) The availability of devices and applications for privacy inspection 5) Law and Regulations concerned with Metaverse 6) The process of educating the Regulators directly related to Metaverse 7) The Education process for using Metaverse 8) Existing Laws related to metaverse cover foreign metaverse systems 9) Laws related to metaverses of foreign countries are comprehensive and suitable for users and 10) The Ministry of Education should play a role in setting up educational curriculum and providing knowledge related to social media and metaverse in schools. Finally, the formula equation of the readiness model is defined.

6. References

Alessandro Acquisti and Ralph Gross. (2006). Imagined communities: awareness, information sharing, and privacy on the facebook. In Proceedings of the 6th international conference on Privacy Enhancing Technologies (PET'06). Springer-Verlag, Berlin, Heidelberg, 36–58. https://doi.org/10.1007/11957454_3.

Axie infinity. (2021). Play to earn. Retrieved from https://axieinfinity.com/, December 16, 2021.

Chimmanee, K. & Jantavongso, S. (2021). Practical mobile network planning and optimization for Thai smart cities: Towards a more inclusive globalization. Research in Globalization, Volume 3, 2021, 100062, ISSN 2590-051X, https://doi.org/10.1016/j.resglo.2021.100062.

D. Grider and M. Maximo. (2021). The metaverse: Web3.0 virtual cloud economies. Accessed: Nov. 1, 2021. [Online]. Available: https://grayscale.com/

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

Fabrigar, L. R., Wegener, D. T., MacCallum, R. C., & Strahan, E. J. (1999). Evaluating the use of exploratory factor analysis in psychological research. Psychological Methods, 4(3), 272–

299. https://doi.org/10.1037/1082-989X.4.3.272.

Global Cybersecurity Index. (2017). Retrieved from https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

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

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.

Hair, J., Black, W., Babin, B., Anderson, R. and Tatham, R. (2006) Multivariate Data Analysis. 6th Edition, Pearson Prentice Hall, Upper Saddle River.

Irfan, M., Putra, S. J., & Ramdhani, M. A. (2019). The readiness model of information technology implementation among universities in Indonesia. In Journal of Physics: Conference Series (Vol. 1175, No. 1, p. 012267). IOP Publishing.

J. D. N. Dionisio, W. G. B. III, and R. Gilbert. (2013). 3D virtual worlds and the metaverse: Current status and future possibilities, ACM Computing Surveys (CSUR), vol. 45, no. 3, pp. 1–38, Jul. 2013.

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.

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/abs/10.1002/cav.1752.

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. (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.

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

Mufti, Yusuf & Niazi, Mahmood & Alshayeb, Mohammad & Mahmood, Sajjad. (2018). A Readiness Model for Security Requirements Engineering. IEEE Access. PP. 1-1. 10.1109/ACCESS.2018.2840322.

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: Retrieved from http://ceur-ws.org/Vol-2861/paper_36.pdf.

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

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

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. , 15(1), 1-14. http://doi.org/10.4018/IJSPPC.315591

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.

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

W. Y. B. Lim, Z. Xiong, D. Niyato, X. Cao, C. Miao, S. Sun, and Q. Yang. (2022). Realizing the metaverse with edge intelligence: A match made in heaven, arXiv preprint arXiv:2203.05471.

Williams B, Onsman A, Brown T. (2022). Exploratory factor analysis: A five-step guide for novices . Australasian Journal of Paramedicine [Internet]. 2010 Aug.2 [cited 2022Nov.19];8(3). Available from: https://ajp.paramedics.org/index.php/ajp/article/view/93