Egyptian Informatics Journal 24 (2023) 303–311

Contents lists available at ScienceDirect

Egyptian Informatics Journal

journal homepage: www.sciencedirect.com

Design of security management model for communication networks in digital cultural consumption under Metaverse – The case of mobile game

Wei Gao [a,*], Lin Li [a], Yingchun Xue [b], Yan Li [a,*], Jinlong Zhang [a]

[a] Central China Normal University, National Research Center of Cultural Industries, No. 152 Luoyu Road, Hongshan District, Wuhan City, Hubei Province 430079, China
[b] Nantong University, Xinglin College, NO.1, Nanhai Road, Qidong Hi-tech Industrial Development District, Nantong City, Jiangsu Province 226236, China

ARTICLE INFO

Article history:
Received 30 August 2022
Revised 26 December 2022
Accepted 7 May 2023
Available online 12 May 2023

Keywords:
Communication networks
Security management model
Digital cultural consumption
Metaverse
Mobile game
Design

ABSTRACT

Under Metaverse, security management of communication networks in digital cultural consumption has attracted more and more attention. As we know, security risks of communication networks caused by non-human factors are becoming weaker and weaker due to technology optimization. Meanwhile, players play significant and increasing role in communication networks. Taking mobile games as an example, this paper designed and applied the security management model to improve security management of communication networks in digital cultural consumption under Metaverse. The results show that: (1) The physiological, psychological, pathological, pharmacological, physical and psychosocial factors exert tremendous influence on communication networks. The psychosocial factors are more prominent. (2) There is security threshold in communication networks. It means that the security state can be entered if security threshold is crossed. This paper designs security threshold as the III level ($5.5 \leq P < 6.5$). (3) This paper proposes 3E rules (That is, engineering, education, enforcement). It is beneficial to deal with security risks in communication networks. (4) After two security evaluations, the result is G2 = 6.70 > G 1 = 5.01. This confirms the effectiveness of the security management model.

1. Introduction

The past years have witnessed that cultural consumption of Chinese residents is undergoing digital transformation. For example, traditional cultural consumption with newspapers and books as carrier is gradually changing from offline to online. Digital cultural consumption is a new form that communication networks are deemed as channel to consume digital cultural products or services. The typical digital cultural consumption includes mobile games, digital animation, digital music, and online literature [1]. The prominent feature of digital cultural consumption is the close interaction between players [2]. This requires strong communication networks to provide technical support [3]. Communication networks are mainly divided into traditional communication networks and modern communication networks. The traditional communication networks (that is, telephone exchange network) are composed of three major parts: transmission, exchange and terminal [4]. Transmission is the medium for transmitting information. Exchange (mainly refers to switch) is the intermediary for various terminals to exchange information. Terminals refer to telephones, mobile phones, fax machines and computers. Modern communication networks can be considered as systemic services. Professional organizations provide individuals with the sum of various communication services depending on communication equipment (hardware) and applications (software).

The concept of Metaverse came from science fiction novel "Avalanche" written by American writer Neil Stephenson in 1992 [5]. There is no unified definition about Metaverse at present. Some scholars have summarized basic characteristics of Metaverse, such as new generation of information technology [5], and integration of virtual and reality [6]. In 2021, the Metaverse rapidly and widely became important driving force for upgrade and development of digital cultural consumption [7,8]. In Metaverse, the content of digital cultural consumption is not supplied by merchants centrally and uniformly, and is designed and consumed by different players according to their own needs [5]. That is to say, players are both consumers and producers of digital cultural content. The important reason lies in communication networks. With the help of Metaverse, communication networks can provide efficient and extensive channels for players to upload commands and downloads materials [3,6]. As a result, the relationship between players and

* Corresponding authors.
E-mail addresses: vsengao@163.com (W. Gao), 158036274@qq.com (Y. Li).

https://doi.org/10.1016/j.eij.2023.05.004
1110-8665/

communication networks is getting closer and closer under Metaverse (Fig. 1). Because of the increasing relationship, the impact of players on communication networks is also becoming more and more obvious. For example, operational errors resulted from player may lead to data congestion and information confusion in communication networks.

Mobile game is typical digital cultural consumption that relies on communication networks frequently [9]. Along with the ever-accelerating intelligentization and popularization of mobile phones are the ever-mounting mobile games. The ubiquity of mobile phones makes mobile game more dependent on communication networks [10]. For example, communication networks have allowed mobile game players to enjoy games in different places and at different times. With continuous penetration of Metaverse, more and more mobile game players produce and consume game content (Fig. 2) with the help of communication networks. The behavior of players also affects the efficiency of communication networks directly. Due to differences characteristics of players in physiological, physical, psychological, and pathological aspects, it is very easy to cause security problems in communication networks. Security problems in communication networks caused by players mainly include privacy leaks, information eavesdropping, system tampering, data forgery, virus software, invalid IP addresses, system vulnerabilities, etc. For example, physiological factors such as fatigue, intoxication, or pathological factors such as sleeping pills and sedatives, can decrease the perceptual awareness of players' brains. The weakening of perceptual awareness will lead to security problems in communication networks, such as privacy data leakage and tampering of critical information. In particular, most mobile game players are teenagers at present. These groups are still unstable and immature in terms of physiology and psychology. These instabilities and immaturities may lead to the serious security problems in communication networks. Based on the above analysis, this paper takes mobile game as an example, and tries to design the security management model of communication networks from perspective of players.

The significant limitations of research work are mainly in three aspects: (1) This paper tries to find out human factors affecting communication networks of mobile games, but human factors are too complex and dynamic to find overall and atypical human factors. (2) Due to influence of Metaverse, communication networks of mobile games will become more complicated in the future. The applicability of security management model also needs to be adjusted accordingly. (3) This paper invites experts to conduct security evaluation. The evaluation process may have subjective factors of experts. Therefore, this paper reduces subjective influence of experts as much as possible, such as inviting experts from different regions and different specialties.

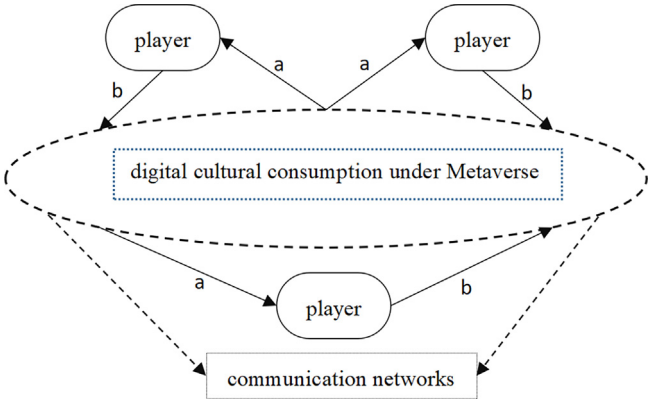

Fig. 1. The relationship between players and communication networks. Source: hand drawn by the author. The dotted ellipses represent communication networks. "a" represents that the player takes communication network to obtain materials. "b" represents that the player transmits the digital cultural content.

2. Literature review

With continuous popularity of mobile games, scholars have done a lot of valuable research on security management of communication networks.

Before Metaverse was incorporated into mobile games, scholars mainly discussed players mobility, network protocols, and network structures. For instance, Li et al. (2016) believed that player mobility increased the complexity of security management of communication networks. They proposed adaptive trusted request and authorization model (ATRA) to improve the security level of communication networks [11]. Kim et al. (2019) considered that the compatibility of different network protocols in the large-scale mobile game environment makes the risk of communication networks more obvious. They proposed mobile game optimization state update scheme based on event locking and analysis model [12]. Weifeng et al. (2020) argued that heterogeneity of network structure in different communication networks can easily lead to data leakage. Taking into account psychological structure and social attributes of mobile users, they constructed the security management patterns [13]. Su and Xu (2021) considered that the growing size of mobile networks and the amounting number of mobile players make security resources inadequate. They propose the security resource allocation scheme to ensure operation of communication networks [14].

Current scholars have done a lot of research on security management system in Metaverse. These researches mainly focus on communication protocols, information encryption and management system. For example, Zhang et al. (2022) proposed relevant techniques to improve the authenticated key exchange (AKE) protocol [15]. This improves security management system of communication networks in Metaverse. Kwon et al. (2022) designed the hybrid Quantum kernels approach to optimize security of virtual reality, augmented reality and other applications [16]. Ryu et al. (2022) proposed security system that can guarantee secure communication and transparently manage user identification data in Metaverse environments [17]. Park et al. (2022) proposed grouping algorithm that focuses on securing various bridgehead strategies to maintain security in Metaverse [18].

After Metaverse was incorporated into mobile games, scholars have mainly studied upgrade of communication networks, optimization of network protocols, allocation of network security resources, and ethical concepts. For example, Jeon et al. (2021) believed that current game is transferred from computer to mobile. The original communication networks need to be updated and adjusted under Metaverse. They proposed the game protection mechanism to deal with vulnerabilities in communication networks [9]. Park and Kim (2022) pointed out that the Metaverse brings deep immersive experience for different mobile game players. They called for network protocol optimization to prevent hacker attacks [19]. Chiang et al. (2022) argued that fifth-generation mobile networks can enhance communication networks. Specifically, relying on optimally splitting the spectrum, mobile game players can enjoy better quality of services under Metaverse [20]. Lee et al. (2022) argued that deep machine learning is helpful for resource allocation in communication networks. They proposed the joint learning framework that facilitates resource allocation for mobile games in wireless networks to improve security management of communication networks [21]. Harborth (2022) considered that mobile games are becoming more and more popular with the support of augmented reality technology. But privacy leakage in communication networks has become

Fig. 2. The auxiliary equipment of mobile games under Metaverse. Source: Baidu Gallery.

an important concern in Metaverse. They proposed ethical reviews to optimize security management in communication networks [22].

Scholars have done a lot of research on network protocol, network architecture, geographical factors, vulnerability factors of communication network. These research have very strong reference significance for security management of communication networks in mobile games and digital cultural consumption. However, existing research focuses more on technical optimization, hardware transformation. Few research discusses security management of communication network in mobile games from perspective of players. Under Metaverse, players have gradually become dominant force in mobile games and digital cultural consumption. It is urgent to study security management of communication networks with players as the core.

3. Security management model

Common factors that affect security management of communication networks include network structure, network protocols, regional factors, operating systems, and user factors [23–25]. With continuous minimization of technical errors related to communication networks, the influence of non-human factors on security management is becoming weaker and weaker. For example, network structure and network protocols show significant compatibility and coordination under the support of technical upgrade. As non-human factors gradually weaken, human factors become more and more important in communication networks [26]. In particular, core players of mobile games are teenagers. The instability and immaturity of these groups, such as irritability and unruly awareness, make the influence of players on the communication network more prominent. As the Metaverse integrates into digital cultural consumption, supporting technology of relevant communication networks in mobile games is further upgraded and optimized. The negative constraints caused by non-human factors on the communication network are minimized. Because more and more players have engaged in designing and consuming digital cultural content through communication networks, the influence and importance of players on security management of the communication are more and more prominent under Metaverse.

System security theory believes that the most important reason of security problems is due to human errors. That is, player's behavior deviates from specified goal or exceeds acceptable limit [27]. For reasons of human errors, scholars consider that there are three main reasons [27–28]: (1) overload pressure beyond human ability. (2) irregular response to external stimuli. (3) unknowing correct method or deliberately taking inappropriate behavior. In order to further analyze factors behind reasons, this paper summarizes factors from six dimensions based on player interviews (mainly interviewed core groups of mobile games, namely teenagers; also interviewed some middle-aged and elderly groups) and literature analysis [27,29]. That is, physiological, physical, pathological, pharmacological, psychological and psychosocial factors.

- Physiological: fatigue, lack of sleep, intoxication, and hunger, can weaken the level of consciousness in the brain. Temperature, lighting, noise and vibration in the environment, shift work and biological rhythms, can also affect the physiological state.
- physical: vision, hearing, and limb sensitivity can limit range of motion, operational strength, perception levels, and response capability.
- pathological: disease, mental disorder and epilepsy can affect the consciousness of the brain.
- Pharmacological: drugs such as sleeping pills, sedatives, antiallergic drugs can decrease the level of consciousness in the brain.
- Psychological: overconfidence, overheating and panic can hinder information processing process in the brain.
- Psychosocial: social awareness, group behavior, and levels of experience can affect normal information processing.

Based on above analysis, this paper designs the security management model (Fig. 3). The architecture of model consists of two main sections, namely factors and countermeasures. In the factors section, human factors that affect communication networks of mobile games are summarized, mainly including physiological, physical, pathological, pharmacological, psychological and psychosocial factors. In the countermeasures section, main countermeasures are proposed, involving engineering, education, and enforcement. Connecting factors and countermeasures is security thresholds. How does this model work? To begin with, The first security evaluation is to determine whether risks arising from human factors are below the security threshold or not. If it is below the security threshold, it means that the security state has not been achieved and countermeasures should be taken. After countermeasures are taken, the second security evaluation is performed to determine whether security threshold is reached. If security threshold is not reached, countermeasures and security evaluation should be continued until security threshold is reached or exceeded.

The work flow of security management model is as follows:

First, designing evaluation indicators from physiological, physical, pathological, pharmacological, psychological and psychosocial

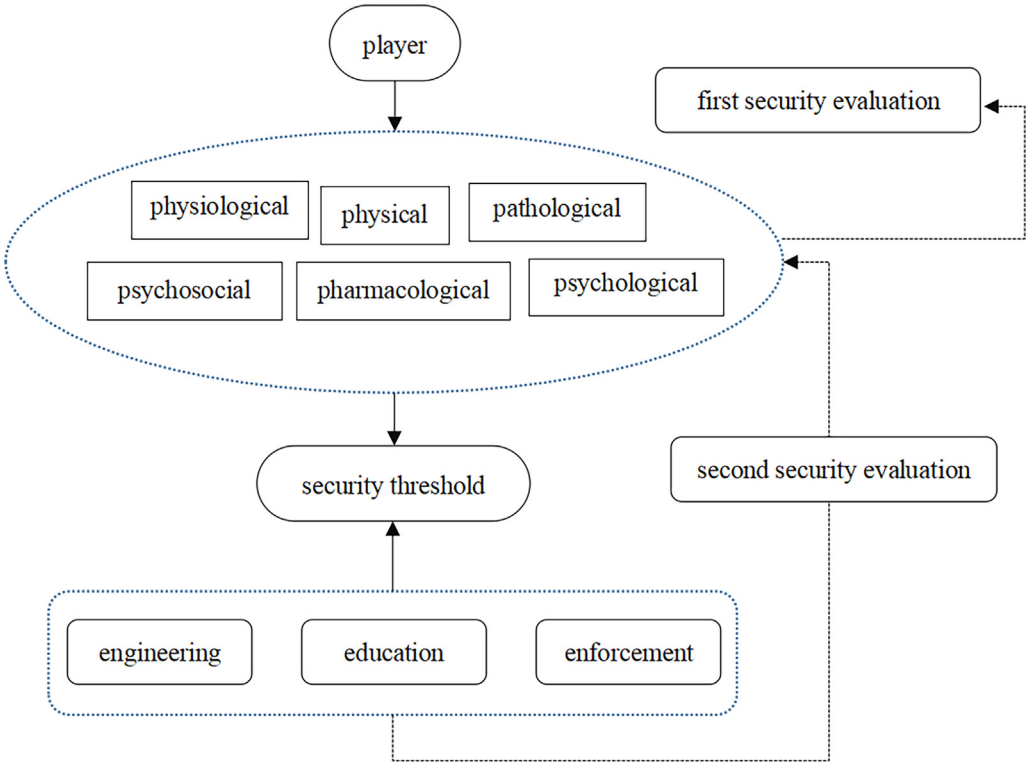

Fig. 3. The security management model. Source: hand drawn by the author.

dimensions. Why design evaluation indicators in the first place? There are two reasons as follows: (1) To find out the human factors (human errors) affecting the security management of communication networks from different dimensions. (2) Security evaluation usually relies on indicators. Reasonable indicators are strong support of scientific, accurate and rigorous security evaluation.

Second, after completing design of evaluation indicators, the security threshold needs to be set, which is the core of security management model. Security threshold is standard to determine whether current risks have negative impact on mobile games' communication networks. That is, whether risks arising from physiological, physical, pathological, pharmacological, psychological and psychosocial factors may endanger effective operation of communication networks.

Third, taking first security evaluation to judge whether risks arising from human factors are below the security threshold or not. If the security threshold is far from being achieved, corresponding measures need to be taken. According to behavioral science theory, human behavior is dominated by motivation, and human errors can be effectively prevented through management of human motivation [30]. Main method of managing human motivation is the well-known 3E rule [27].

- Engineering: using engineering techniques to eliminate unsafe factors and achieve physical security.
- Education: using various forms of education and training to enhance security awareness and master the necessary knowledge and skills of mobile games.
- Enforcement: restricting player's behavior with necessary administrative and legal systems.

After carrying out security management in accordance with 3E rule, indicators should be re-evaluated to judge whether security threshold is achieved. If security threshold is not achieved, the 3E rule and security evaluation need to continue.

4. Research design

4.1. Identify indicators

According to the safety management model, evaluation indicators involve physiological, physical, pathological, pharmacological, psychological and psychosocial dimensions. Based on field research and literature analysis [27–30], these evaluation indicators are decomposed into nearly 40 s-level indicator indicators. To further improve and optimize second-level indicators, this paper invites 20 experts and players to revise them. Three rounds of revision were carried out. After each revision, it is modified according to opinions and suggestions of experts and players. Finally, 27 s-level indicators are obtained in Table 1.

4.2. Indicator weight

The indicator weight is related to status and role of indicators. This paper takes the entropy weight method (EWM) to design indicator weight. The entropy weight method measures the amount of data information through information entropy, and designs the weight of each indicator accordingly [31]. Compared with Analytic Hierarchy Process (AHP) and other methods, it has stronger objectivity. The main calculation steps are as follows.

First, collect original data to construct matrix C.

$$C = \begin{bmatrix} c11 & c12 & \dots & c1n \\ c21 & c22 & \dots & c2n \\ \dots & \dots & \dots & \dots \\ cn1 & cn2 & \dots & cnn \end{bmatrix} \quad (1)$$

Second, data should be standardized and information entropy (R_i) is calculated according to the entropy formula.

Table 1
Evaluation indicators.

First-level indicators	Second-level indicators
Physiological (F1)	excessive fatigue (F11)
	excessive drunkenness (12)
	hunger and low blood sugar (F13)
	lack of sleep (F14)
Psychological (F2)	fluke mentality (F21)
	lazy mentality (F22)
	rebellious mentality (F23)
	impatient and negative (F24)
	grumpy and moody (F25)
	panic and restless (F26)
Pathological (F3)	Headache (F31)
	mental disorder (F32)
	sequelae of traumatic brain injury (F33)
	unconsciousness and coma (F34)
	Epilepsy (F35)
Pharmacological (F4)	long-term use of sleeping pills (F41)
	long-term use of anti-allergy drugs (F42)
	long-term use of sedatives (F43)
Physical (F5)	Eyesight (F51)
	Hearing (F52)
	Height (F53)
	Weight (F54)
	limb sensitivity (F55)
Psychosocial (F6)	skilled skills (F61)
	work experience (F62)
	social emotions (F63)
	social thought (F64)

$$Ri = -k\sum_{i=1}^{n} P\ln(P) \tag{2}$$

Among them, $K = \frac{1}{\ln(n)} > 0$, P is the weight after standardization.

Third, weight coefficient (g_i) is calculated according to information entropy (R_i).

$$gi = \frac{1 - Ri}{\sum_{i=1}^{m}(1 - Ri)} \tag{3}$$

Finally, calculate the weight (w) based on information entropy (R_i)

$$W = (g_1, g_2, g_3 \cdots g_n) \tag{4}$$

4.3. Data sources

The data sources mainly include primary data and secondary data. The primary data is scores provided by experts (including technical workers in enterprises, teachers in colleges, experts in associations, etc.). This paper collected nearly 70 relevant experts based on voluntary registration, direct invitation, authoritative recommendation. In order to reflect the professionalism, authenticity and impartiality, secondary assessment and screening were conducted. Finally, 60 experts were obtained (Table 2).

Setting reasonable parameters is the basis of expert scoring. Before setting parameters, it is necessary to clarify evaluation process. Firstly, experts are invited to score the second-level indicators (Table 1). Then, the entropy weight method (EWM) is used to determine indicator weights (weights of first-level indicators and second-level indicators) based on experts' scores. Finally, scores of first-level indicators and the overall score are obtained based on experts' scores and indicator weights. As we know, if scores come from experts, it is necessary to set parameters of indicators. The function of parameters is mainly to provide the basis for experts to judge and score. Since experts directly score second-level indicators, parameters are set for second-level indicators in the first place. In order to improve scientificity and convenience of parameters, this paper quantifies parameters of second-level indicators (Table 1). The parameters of second-level indicators in physical and psychosocial dimensions were divided from 1 to 10 (That is, scores from 1 to 10). The higher the score, the smaller the risks on communication networks. The parameters of second-level indicators in physiological, psychological, pathological and pharmacological dimensions were divided from 10 to 1 (That is, scores from 10 to 1). The smaller the score, the smaller the risks. How do experts score indicators of quantified parameters? Taking indicator F11 (excessive fatigue) as an example. The parameter range of indicator F11 is from 1 to 10 (That is, scores from 1 to 10). The higher the score, the smaller the risks on communication networks. Experts can determine the risk level of indicator F11 based on practical experience and external information. Then, experts choose the corresponding score value from parameter range. In order to ensure uniformity and computability in the calculation process, the parameters were processed with the same trend in statistics (The method of min–max standardization [32]). Finally, the scores of parameters tend to be the same as second-level indicators in physical and psychosocial dimensions. That is, the higher the score, the smaller the risks. Similarly, parameters of first-level indicators are the same as their second-level indicators.

The secondary data mainly comes from the "Statistical Yearbook" published by the National Bureau of Statistics, the government's annual bulletin, the official websites of the Ministry of Industry and Information Technology, and the Communication Networks Association. Secondary data is used as reference standard when experts evaluate indicators.

Table 2
Evaluation levels and security threshold.

Level	Value	Explanation
I	$8.5 \le P \le 10$	The lowest risk of security management
II	$6.5 \le P < 8.5$	Lower risk of security management
III	$\mathbf{5.5 \le P < 6.5}$	**General risk of security management (security threshold)**
IV	$3.5 \le P < 5.5$	Higher risk of security management
V	$0 \le P < 3.5$	The highest risk of security management

4.4. Security threshold

According to security management model, the design of security threshold is critical step. As we know, security threshold is reasonable standard for achieving security state [33]. The system security theory argues that security state is not absolutely safe, but the risk is controlled within security range [27]. When the security threshold is reached or exceeded, it means that security state is achieved; If the security threshold is not reached, it means that the security state is not implemented.

In the operational process, security threshold needs to be further quantified in order to improve accuracy and convenience of evaluation process. First, according to the principle of normal distribution, literature analysis [27,33] and field research, this paper divided results of indicator evaluation into five levels. These five levels represent risks of security management. Each level has its own range of values. These values are derived from above evaluation results (That is, calculated from expert scores). In order to test whether the division of five levels is scientific, effective and reasonable, this paper invited 20 authoritative experts and 20 experienced players to conduct reviews. The results show that 82% think it is reasonable, 16% think it needs to refine the range, and 2% think it is unclear. According to review results, this paper revised five levels. Second, identifying turning point. The turning point is significant turnaround about negative impact of risks on communication networks. As we know, higher risks mean farther away from security state, and lower risks mean closer to security state. This paper invited 20 authoritative experts and 20 experienced players

to conduct three preparatory tests. The result shows that 92% of them thought the III level might be the turning point. The main reasons are as follows: (1) when evaluation results are at the I level and II level, security state of communication networks is better. That is, communication networks of mobile games can operate normally, efficiently and securely. (2) When evaluation result is at the IV level and V level, security state of communication networks is far from our expectation. That is, communication networks of mobile games have many problems such as privacy data leakage, information tampering, system vulnerability. (3) When evaluation result is at the III level, security state of communication networks is at the turning point. For example, the III level is similar to pivot point of the seesaw. The security state changes dramatically when it exceeds or falls the III level. Third, Determining security threshold. This paper sets the III level as the security threshold. The main reasons are as follows: (1) Security threshold represents reasonable standard for achieving security state. The turning point (the III level) is the standard that whether security state is achieved. So the turning point (the III level) can be set as security threshold. (2) Security threshold means that security state is reached, but some risks still exist at this time. These risks can be offset by themselves during operational process, and it is difficult to have negative impact on communication networks. The turning point (the III level) represents turnaround in terms of negative impact of ricks on communication networks, and it also contains some ricks. But, these ricks hardly have any negative impact on communication networks.

5. Empirical analysis

5.1. Determine the research object

In order to verify whether the security management model is effective, this paper selected research object for empirical analysis. In consideration of representativeness and validity of research object, this paper sets selection rules: (1) The popularity and download of mobile games rank among the top 10 in mobile application malls. (2) This mobile game is highly dependent on communication networks. More than 50% of its functions rely on communication networks. (3) Players' physical, psychological and other factors produce more than 50% influence on communication networks in mobile games. (4) In this mobile game, technical factors affecting communication networks produce little impact on security management; (5) This mobile game is typical representative of digital cultural consumption, and ranks in the top 10 of the digital cultural consumption lists; (6) The mobile game has completed transformation and upgrade of Metaverse ecology. Based on the above requirements, this paper selected game A as the research object.

5.2. Results of the first evaluation

The overall score is 5.01 (G1 = 5.01, formula 5). This means that communication network has not yet achieved security threshold. It needs to be optimized and adjusted according to 3E rule.

$$\begin{aligned} G1 &= 0.22 * 4.90 + 0.28 * 5.17 + 0.25 * 4.98 + 0.17 * 5.02 \\ &\quad + 0.01 * 5.98 + 0.06 * 4.58 \\ &= 5.01 \end{aligned} \tag{5}$$

Specifically, the score of psychosocial (F6) is 4.58, ranking at the bottom and behind the security threshold. Scores of physiological (F1), psychological (F2), pathological (F3) and pharmacological (F4) are 4.90, 5.17, 4.98, 5.02, and 4.68 respectively. They are all behind the security threshold. Score of physical (F5) is 5.98, which is above the security threshold. These results show that risks arising from physiological, pathological, pharmacological, psychological and psychosocial factors pose serious threat to security management of communication networks. This requires corresponding countermeasures. In particular, psychosocial factors should be further strengthened. The results are shown in Table 3.

5.3. Safety management measures under 3E rules

The core idea of 3E rules is to take corresponding countermeasures according to results of the first evaluation. It is mainly divided into three steps. The first step is to find indicators below security threshold based on results of the first security evaluation. The second step is to take corresponding measures against these indicators according to 3E rules. The third step is to check whether implementation of measures is complete. Meanwhile, according to practice situation, it is necessary to summarize experience and enrich content of 3E rules.

There are many specific countermeasures to deal with results of the first evaluation. For example, in terms of engineering techniques, cloud technology should be used to strengthen the supervision of player errors in mobile games; The linkage mechanism should be optimized to achieve harmless accidents. That is, when player errors lead to accidents, measures should be immediately taken to stop or slow down digital cultural consumption; Error-resistant designs should be added for hardware buttons or software programs in mobile games. In terms of education, education and training should be standardized for players. It is necessary to emphasize that errors should not be ignored; The digital cultural consumption content should prevent fatigue or decrease psychological tension; If players are taking medicine or are sick, it is recommended to play mobile games reasonably. In terms of enforcement, it is best to design certification system for game competitions; For players who often cause accidents related to communication networks, it is best to interview the reasons or form blacklist management system. In short, there are many countermeasures under the 3E rules, But these countermeasures should not violate public order, good customs and legal systems. These better not hinder players from enjoying digital cultural consumption.

The criteria to fix the threshold value from 3E rules is very critical and important. 3E rules are mainly three operational steps and the focus is on the execution of the steps. However, how can the security threshold be reached during execution? Based on the security management model, this paper proposes the second security evaluation. The purpose of second security evaluation is to check whether 3E rules meet the security threshold. The second security evaluation is usually conducted after the third step of the 3E rules. Therefor, it can be concluded that the criteria to fix the threshold value from 3E rules depends on the result of second security evaluation.

5.4. Results of the second evaluation

The overall score is 6.70 (G2 = 6.70, formula 6). This means that with the help of 3E rules, the security threshold has been exceeded. It also means that communication network in the mobile game has been improved.

$$\begin{aligned} G2 &= 0.22 * 6.68 + 0.32 * 6.93 + 0.33 * 6.11 + 0.12 * 7.62 \\ &\quad + 0.01 * 7.47 + 0.01 * 7.55 \\ &= 6.70 \end{aligned} \tag{6}$$

Specifically, the scores of physiological (F1), psychological (F2), pathological (F3), pharmacological (F4), physical (F5), and psychosocial (F6) are 6.68, 6.93, 6.11, 7.62, 7.47, 7.55 respectively.

Table 3
Results of the first evaluation.

first-level indicators	Weight	value	second-level indicators	Weight	value
F1	0.22	4.90	F11	0.25	5.23
			F12	0.22	5.30
			F13	0.19	5.23
			F14	0.34	4.20
F2	0.28	5.17	F21	0.19	5.17
			F22	0.16	4.87
			F23	0.14	5.30
			F24	0.12	5.20
			F25	0.20	5.37
			F26	0.19	5.13
F3	0.27	4.98	F31	0.22	4.73
			F32	0.15	5.70
			F33	0.21	5.07
			F34	0.19	4.93
			F35	0.24	4.73
F4	0.17	5.02	F41	0.33	5.10
			F42	0.39	4.57
			F43	0.28	5.57
F5	0.01	5.98	F51	0.22	5.83
			F52	0.18	6.02
			F53	0.19	6.10
			F54	0.21	6.08
			F55	0.20	5.88
F6	0.06	4.58	F61	0.27	4.65
			F62	0.25	4.40
			F63	0.21	5.02
			F64	0.27	4.32

They exceed or reach the security threshold. This confirms that security management model can improve security management of communication networks in mobile games. The results are shown in Table 4.

This paper compares results of security management model with the latest publications in this domain. The latest publications selected are related to security management of communication networks. According to results of the latest publications, this paper finds that current research focuses on technical aspects, such as blockchain technology, key management, communication protocols. The security management model proposed in this paper mainly studies physiological, physical, pathological, pharmacological, psychological and psychosocial factors. Results emphasize the importance of human factor. Results of this paper are complementary to the current research. In addition, security threshold is designed and quantified. The security threshold may set the standard for our security management of communication networks (Table 5).

Table 4
Results of the second evaluation.

first-level indicators	Weight	value	second-level indicators	Weight	value
F1	0.22	6.68	F11	0.28	6.60
			F12	0.17	7.77
			F13	0.36	5.77
			F14	0.19	7.60
F2	0.32	6.93	F21	0.17	6.93
			F22	0.14	7.43
			F23	0.23	6.10
			F24	0.14	7.43
			F25	0.15	7.27
			F26	0.17	6.93
F3	0.33	6.11	F31	0.27	5.43
			F32	0.19	6.60
			F33	0.08	8.43
			F34	0.19	6.60
			F35	0.27	5.43
F4	0.12	7.62	F41	0.29	7.93
			F42	0.32	7.77
			F43	0.39	7.27
F5	0.01	7.47	F51	0.20	7.52
			F52	0.20	7.67
			F53	0.21	7.43
			F54	0.19	7.25
			F55	0.20	7.48
F6	0.01	7.55	F61	0.26	7.52
			F62	0.24	7.50
			F63	0.25	7.62
			F64	0.25	7.55

Table 5
Comparison table with the latest publications.

Researchers	Main content	Key point
Benzaïd et al. (2020) [34]	From perspective of defenders, criminals and victims, the paper examines how AI will affect the security of communication networks	Emphasize the role of artificial intelligence
Sun et al. (2021) [35]	The paper mainly studies the intelligent information terminal network security technology based on the mobile Internet of Things	Key management for the mobile Internet of Things
Khanna et al. (2022) [36]	The paper proposes blockchain-based security enhancement and spectrum sensing approach for spectrum management	Blockchain technology for communication networks
Pothumart et al. (2021) [37]	The paper presents lightweight cryptographic method which can improve the security level of communication	Key management scheme and mutual authentication protocol
Su et al. (2017) [14]	The paper proposes security perception resource allocation scheme based on match league game	Communication networks resource allocation
Jeon et al. (2021) [9]	The paper proposes game protection mechanism based on ARM trust zone, which can protect confidentiality and integrity of mobile games	Game protection mechanism based on ARM trust zone

6. Discussion

(1) The influence of players on security management of communication networks is becoming more and more obvious under Metaverse. Driven by the Metaverse, players become the focus of digital cultural consumption [5]. This means that players both design and consume digital cultural content through communication networks. In addition, communication networks with better compatibility and interoperability may have very few technical errors. For example, security errors of communication networks caused by hardware technology is getting smaller and smaller. The final result is that the influence of players on security management of communication networks is becoming more and more obvious.

(2) The physiological, psychological, pathological, pharmacological, physical and psychosocial factors play significant role in security management of communication networks. According to the security management model, the reasons why players have significant impact on security management of communication networks are the players' errors. Direct causes of players' errors are related to physiological, psychological, pathological, pharmacological, physical and psychosocial factors [27]. Above factors may alone cause errors, or work together. These errors may be random errors, systematic errors and sporadic errors. These errors also manifest themselves in phenomena such as forgetting things, doing wrong things, and performing extraneous acts.

(3) Security management model has designed security threshold. System security theory considers that there is threshold for security management [27]. According to the security management model, this paper chooses the III level ($5.5 \leq P < 6.5$) as security threshold. The security threshold allows risks to be controlled within the security range. When the threshold is crossed, the security state will be entered. For example, in the process of digital cultural consumption, when security threshold is reached, security state can be considered suitable for players to enjoy entertainment and consumption.

(4) The security management model has proposed 3E rules to deal with security risks. 3E rules optimize players' physiological, psychological, pathological, pharmacological, physical and psychosocial factors in terms of hardware modification and ideological improvement. According to results of the second evaluation, 3E rules have optimized factors and promoted communication networks to achieve security threshold. Generally speaking, when applying 3E rules, first engineering technical measures, then education and enforcement [27]. For example, we take engineering and technical measures to reduce and control unsafe factors. Then education and training maybe used to regulate and avoid errors.

7. Conclusion

This paper takes mobile games as an example, and designs the security management model from perspective of players. The relevant conclusions are as follows: (1) Under Metaverse, security management of communication networks in digital cultural consumption is increasingly influenced by players. In other words, the importance of physiological, physical, pathological, pharmacological, psychological and psychosocial factors is becoming more and more prominent. (2) Security threshold is the key of security management model. This paper has designed the security threshold (at the III level, $5.5 \leq P < 6.5$). This is useful attempt to quantify the security threshold. (3) Relying on two evaluations, the security management model determines whether security management reaches or exceeds security threshold. The results show that $G2 = 6.70 > G1 = 5.01$. It means that security threshold has been exceeded after the second security evaluation. This also confirms the validity of security management model. (4) The management of risks in communication networks is crucial. This paper designs 3E rules, involving technology optimization, administrative regulations, personal management. This manifests certain practical significance for the management of risks.

CRediT authorship contribution statement

Wei Gao: Investigation, Project administration, Validation, Formal analysis, Conceptualization, Data curation, Methodology, Resources, Visualization, Writing - original draft, Writing - review & editing. **Lin Li:** Conceptualization, Supervision. **Yingchun Xue:** Investigation, Funding acquisition. **Yan Li:** Investigation, Validation, Writing - original draft. **Jinlong Zhang:** Investigation, Software.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

Thanks to the research team for careful exploration and research. Thanks to editors and reviewers for their hard work and dedication.

Consent for publication

Written informed consent for publication was obtained from all participants. All the authors agreed to publish.

Funding

This achievement is supported by Excellent Engineering Project of Social Science Applied Research in Jiangsu Province, China (Project No.: 22SYB-124; Project Leader: Xue Yingchun).

References

[1] Dey BL, Yen D, Samuel L. Digital consumer culture and digital acculturation. Int J Inf Manag 2020;51:102057.
[2] Cochoy F, Licoppe C, McIntyre MP, Sörum N. Digitalizing consumer society: equipment and devices of digital consumption. J Cult Econ 2020;13(1):1–11.
[3] Bisht S, Kumar A, Goyal N, Ram M, Klochkov Y. Analysis of network reliability characteristics and importance of components in a communication network. Mathematics 2021;9(12):1347.
[4] Jia W, Jiang T. Information-defined networks: a communication network approach for network studies. China Commun 2021;18(7):197–210.
[5] Mystakidis S. Metaverse. Metaverse Encyclopedia 2022;2(1):486–97.
[6] Chen SC. Multimedia research toward the metaverse. IEEE MultiMedia 2022;29(1):125–7.
[7] Ge J, Gupta A. Multiple influences of intelligent technology on network behavior of college students in the metaverse age. J Environ Public Health 2022;2022:1–7.
[8] Dahan NA, Al-Razgan M, Al-Laith A, Alsoufi MA, Al-Asaly MS, Alfakih T. Metaverse framework: a case study on e-learning environment (ELEM). Electronics 2022;11(10):1616.
[9] Jeon S, Kim HK. TZMon: improving mobile game security with ARM trustzone. Comput Secur 2021;109:102391.
[10] Agrawal R, Faujdar N, Romero CAT, Sharma O, Abdulsahib GM, Khalaf OI, et al. Classification and comparison of ad hoc networks: a review. Egypt. Informat. J. 2022.
[11] Li ZY, Liu L, Chen RL, Bi JL. An adaptive secure communication framework for mobile peer-to-peer environments using Bayesian games. Peer-to-Peer Networking Applications 2016;9(6):1005–19.
[12] Kim HY, Kim KJ. Optimized state update for mobile games in cloud networks. Clust Comput 2019;22(1):1035–41.
[13] Weifeng Lu, Mingqi Z, Jia Xu, Siguang C, Lijun Y, Jian Xu. Cooperative caching game based on social trust for D2D communication networks. Int J Commun Syst 2020;33(9):e4380.
[14] Su Z, Xu Q. Security-aware resource allocation for mobile social big data: a matching-coalitional game solution. IEEE Trans Big Data 2017;7(4):632–42.
[15] Zhang X, Huang X, Yin H, Huang J, Chai S, Xing B, et al. LLAKEP: a low-latency authentication and key exchange protocol for energy internet of things in the metaverse era. Mathematics 2022;10(14):2545.
[16] Kwon HJ, El Azzaoui A, Park JH. MetaQ: A Quantum Approach for Secure and Optimized Metaverse Environment. Human-Centric Computing and Information Sciences; 2022. p. 12.
[17] Ryu J, Son S, Lee J, Park Y, Park Y. Design of secure mutual authentication scheme for metaverse environments using blockchain. IEEE Access 2022;10:98944–58.
[18] Park WH, Siddiqui IF, Qureshi NMF. AI-enabled grouping bridgehead to secure penetration topics of metaverse. Comput Mater Continua 2022;73(3):5609–24.
[19] Park SM, Kim YG. A metaverse: taxonomy, components, applications, and open challenges. IEEE Access 2022;10:4209–51.
[20] Chiang JK, Lin CL, Chiang YF, Su Y. Optimization of the Spectrum splitting and auction for 5th generation mobile networks to enhance quality of services for IoT from the perspective of inclusive sharing economy. Electronics 2021;11(1):3.
[21] Lee HS, Lee DE. Resource allocation in wireless networks with federated learning: network adaptability and learning acceleration. ICT Express 2022;8(1):31–6.
[22] Harborth D. Human autonomy in the era of augmented reality—a roadmap for future work. Information 2022;13(6):289.
[23] Rai P, Ghose MK, Sarma HKD. Game theory based node clustering for cognitive radio wireless sensor networks. Egypt Informat J 2022;23(2):315–27.
[24] Mukherjee S, Biswas GP. Networking for IoT and applications using existing communication technology. Egypt Informat J 2018;19(2):107–27.
[25] Dureja R, Rozier KY. Formal framework for safety, security, and availability of aircraft communication networks. J Aerosp Inform Syst 2020;17(7):322–35.
[26] Paolucci A, Sangiorgi S, Mariani MG. Non-technical skills in social networks: the spread of safety communication and teamwork in a warehouse. Int J Environ Res Public Health 2021;18(2):467.
[27] Chen BZ, Zhang PH. Safety Principles. Metallurgical Industry Press; 2016.
[28] Morag I, Chemweno P, Pintelon L, Sheikhalishahi M. Identifying the causes of human error in maintenance work in developing countries. Int J Ind Ergon 2018;68:222–30.
[29] Soltanzadeh A, Sadeghi Yarandi M, Mirzaei Aliabadi M, Mahdinia M. Modeling cause-and-effect relationships among predictive variables of human error based on the fuzzy multi-criteria decision-making method. Theor Issues Ergon Sci 2021:1–18.
[30] Yee DM, Braver TS. Interactions of motivation and cognitive control. Curr Opin Behav Sci 2018;19:83–90.
[31] Joshi D, Kumar S. Intuitionistic fuzzy entropy and distance measure based TOPSIS method for multi-criteria decision making. Egypt Informat J 2014;15(2):97–104.
[32] Nogueira AL, Munita CS. Quantitative methods of standardization in cluster analysis: finding groups in data. J Radioanal Nucl Chem 2020;325(3):719–24.
[33] Snyman D, Kruger H. Behavioural threshold analysis: methodological and practical considerations for applications in information security. Behav Inform Technol 2019;38(11):1088–106.
[34] Benzaïd C, Taleb T. AI for beyond 5G networks: a cyber-security defense or offense enabler? IEEE Netw 2020;34(6):140–7.
[35] Sun N, Li T, Song G, Xia H, Chen C-H. Network security technology of intelligent information terminal based on mobile Internet of Things. Mob Inf Syst 2021;2021:1–9.
[36] Khanna A, Rani P, Sheikh TH, Gupta D, Kansal V, Rodrigues JJ. Blockchain-based security enhancement and spectrum sensing in cognitive radio network. Wirel Pers Commun 2022;127(3):1899–921.
[37] Pothumarti R, Jain K, Krishnan P. A lightweight authentication scheme for 5G mobile communications: a dynamic key approach. J Ambient Intell Hum Comput 2021:1–19.