Hindawi
Wireless Communications and Mobile Computing
Volume 2020, Article ID 8888296, 11 pages
https://doi.org/10.1155/2020/8888296

Research Article

Research on Privacy Security Risk Assessment Method of Mobile Commerce Based on Information Entropy and Markov

Tao Zhang,[1] Kun Zhao,[1] Ming Yang,[1] Tilei Gao,[1] and Wanyu Xie[2]

[1] *School of Information, Yunnan University of Finance and Economics, Kunming 650221, China*
[2] *Personnel Department, Kunming Metallurgy College, Kunming 650033, China*

Correspondence should be addressed to Ming Yang; yangming@ynufe.edu.cn

Received 31 May 2020; Revised 11 June 2020; Accepted 17 June 2020; Published 7 July 2020

Academic Editor: Yin Zhang

To obtain precise personalized services in mobile commerce, the users have to disclose their personal information to the operator, which constitutes a potential threat to their privacy security. In this paper, a mobile commerce privacy security risk assessment model is established based on information entropy and Markov chain, and effective security risk measurement, and assessment method is put forward. Our method can provide accurate and quantitative results in assessing privacy disclosure risk to guide the users' selection of safe mobile commerce applications and protect their privacy security.

1. Introduction

In the mobile internet age, mobile commerce (m-commerce for short) has gained a high market share by virtue of its portable characteristics, and various precise services like web access, e-shopping, tourism consumption, and near-field payment are rendered to the public. With the popularization of m-commerce, the users can access more and more precise services, but meanwhile, their privacy and security are facing serious threats [1]. To obtain and enjoy more precise personalized services, the users have to disclose more personal information to the service operator, and the operator requires more details of such information to maintain the operation of the commercial platform and render the so called diverse personalized services. Then, the private information of users may be disclosed, abused, stolen, or exposed to other risks when being acquired, used, transmitted, and stored by the operator, and multiple data, including social security number, credit card number, protected health information, and user name, may be disclosed unintentionally. Meanwhile, the private information can also be stolen via internal theft, external hacking, employee negligence, or in other ways. As learned by the Identity Theft Resource Center and the US Department of Health and Human Services, the top 10 data breaches of 2019, where more than 137 million records were leaked, were all related to the government, medical institutions, and corporate websites or apps [2]. The academia and industry are paying more attention to the security risk of users' private information in mobile commerce.

At present, most researchers focus on the risk assessment of private information in information system, cloud computing, and big data, and the risk assessment of user private information disclosure in m-commerce is rarely studied. Given the vital importance of risk assessment for information security to the ecosystem and sustainable development of m-commerce platform [3], the risks of users' private information in m-commerce are explored in this paper from the perspective of private information disclosure. Compared with the traditional information system security risk factors, the risk hierarchy structure of users' privacy information in m-commerce is more complex. These risks include traditional information system security risk, user behavior risk, third-party application risk, and special risks of m-commerce services, like the risk in location-based services in mobile networks [4]. Therefore, in this paper, various risk factors are comprehensively analyzed by reference to some literature, and a risk indicator system for user private information disclosure in m-commerce is built based on the security model of information system [5]. Moreover, the privacy security of users is still assessed, and effective risk assessment model is built based on the theories of information entropy and Markov chain, to provide accurate risk assessment results to the users and protect their privacy security in m-commerce.

This paper can divided into the following parts: in Section 1, the background, content, and significance of the research are presented; in Section 2, we summarize and discuss the privacy security risk index, measurement and assessment methods in m-commerce are summarized and expounded, and the existing problems in the current researches on privacy security of m-commerce are revealed; in Section 3, we apply information entropy and Markov chain in the research of privacy security risk of m-commerce users, the user privacy security is described based on the information entropy, and the random state of privacy security risk of m-commerce is restored in accordance with Markov chain; in Section 4, a risk assessment model for m-commerce user privacy disclosure is established based on information entropy and Markov chain, effective assessment method is put forward, and the whole assessment process is specified; in Section 5, a detailed case study is carried out by substituting the proposed model into a specific m-commerce application, and the quantitative assessment results for three applications are presented and compared with each other. And finally, in Section 6, the research of this paper is summarized, and the future research direction is pinpointed.

2. Related Work

Recent researches on privacy security risk of m-commerce can be generally classified into two aspects, identification of risk factor and method development for risk assessment.

2.1. Research on Risk Factors of User Privacy Disclosure. Risk assessment depends on the identification of risk factors. In order to properly define the privacy risks of m-commerce users, we conclude the risk factors that have been widely studied by researchers in Table 1.

Table 1: Classes and factors of privacy risks of m-commerce users.

Risk classes	Risk factors
Technology risk	Data encryption; intrusion detection; authorization and authentication; access control; anonymisation; trajectory information hiding
Platform environmental risk	Data contribution agreement; secure routing protocol; legal or institutional requirements; diversity of privacy laws; mobile advertising attack; location service
Operator management risk	Privacy management mechanism; regulatory and disciplinary systems; insider threat; third party information collection
User vulnerability risk	Privacy awareness; privacy invasion experience; privacy association setting; simple password setting
Mobile terminal device risk	Sensitive data protection; taint tracking; privilege manage; detection of malicious events

2.1.1. Technology Risk. Shirazi and Iqbal [6] studied the community clouds in m-commerce and pointed out that the privacy security of users in m-commerce mainly relies on data encryption, intrusion detection, identity management, security awareness, privacy protocol, privacy principle, privacy practice, and effective database utilization. Erfan et al. [7] suggested that anonymous technology could help reduce the personal privacy risk of m-commerce users. Zhang et al. [8] proposed a security policy based on identity authentication and access control to protect private information stored in the edge cloud. Yosef and Mahmoud [9] analyzed the security issues at various levels of the cyber physical system (CPS) architecture and pointed out that to improve its safety, attention should be paid to the influence of relevant technologies, such as authentication, access control, data encryption, environment monitoring, security routing protocol, network access control, attack detection mechanism, and user authentication and authorization.

2.1.2. Platform Environmental Risk. According to literature [10, 11], location information was extremely sensitive in m-commerce, and the exposure of location information might cause the risk of information abuse in m-commerce. In reference [12], it was found that advertisements in m-commerce were intrusive to the users' privacy, for the users' location, and other information may be mandatorily acquired. Reference [13] reveals that users are required to accept some privacy clauses before using some m-commerce applications and have no autonomy over whether to share their own information in utilization.

2.1.3. User Vulnerability Risk. Ampong et al. [14] noted that privacy awareness, privacy concerns, and privacy intrusion experiences were important factors that affected the disclosure of user privacy. Reference [15] conducted a qualitative analysis of the privacy risk factors of social networks in the big data environment and suggested that privacy association setting, spatial location sharing, information behavior negligence, and simple password setting constituted the major user behavior risk factors.

2.1.4. Operator Management Risk. Tian et al. [16] believed that the privacy risks in the management of mobile apps included rigid legal or institutional requirements, imperfect standards for disclosure of privacy information, lack of regulatory and disciplinary systems, and malicious disclosure by internal personnel. In line with the Risk Evaluation Specification for Information Security (GB-T20984-2007) and the behavior characteristics of m-commerce users, Xiang et al. [17] incorporated into their risk evaluation index system such related factors as privacy management mechanism, platform privacy protection input, information sharing risk, third party information collection, and privacy legal differences.

2.1.5. Mobile Terminal Device Risk. In addition to the risk factors mentioned above, potential privacy risk may arise from the mobile terminal as well. Therefore, corresponding measures, including sensitive data protection [18, 19], smear

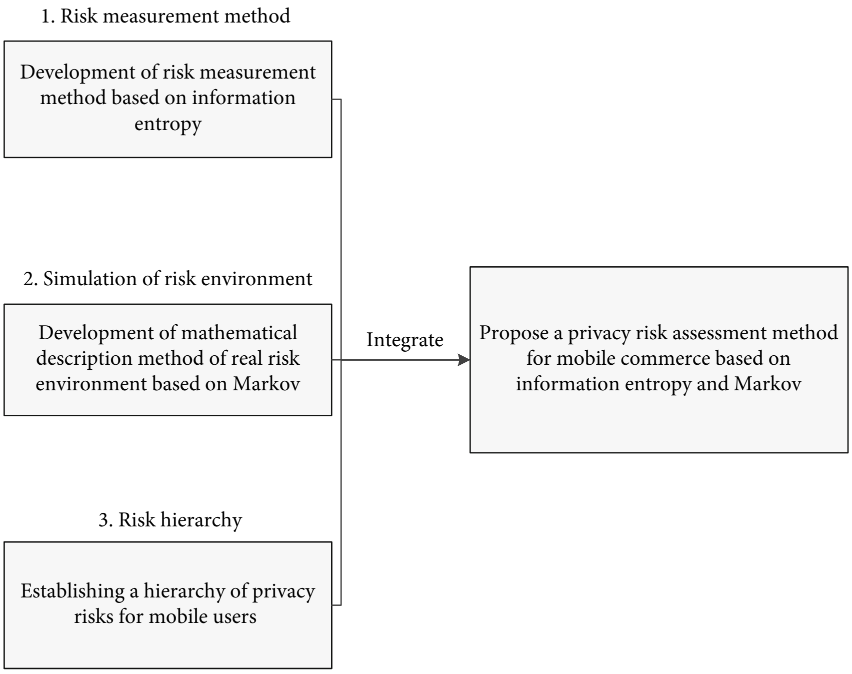

1. Risk measurement method
Development of risk measurement method based on information entropy
2. Simulation of risk environment
Development of mathematical description method of real risk environment based on Markov
3. Risk hierarchy
Establishing a hierarchy of privacy risks for mobile users
Integrate
Propose a privacy risk assessment method for mobile commerce based on information entropy and Markov

Figure 1: Framework of our research in developing risk assessment method.

tracking [20], authority management [21], and malicious event monitoring [22], need to be taken to ensure the security at the mobile terminal.

2.2. Research on Assessment Method for Privacy Security Risk. At present, fruitful achievements have been made in the research of risk assessment, but only a few researches focus on privacy risk assessment, and researches on privacy assessment for m-commerce applications are rare. In references [23–26], the risks were evaluated based on the concept of information entropy; a feasible program was proposed for the assessment of security risk in cloud computing, but the privacy security was not analyzed. In reference [27], a privacy-considered information security assessment model was built with the risk recommendation system based on the identifiability, context of use, quantity, sensitivity, and freshness of the personal identity information data. The likelihood of risk evaluation was calculated taking into account the impact assessment of existing control measures and risks, and privacy security was evaluated from the perspective of the frequency of risk occurrence. Oetzel and Spiekermann [28] proposed a system approach for privacy impact evaluation, and divided the entire privacy impact assessment (PIA) process into seven steps, namely, characterization of the system, definition of privacy objectives, evaluation of protection requirements, identification of threats, identification and recommendations of controls, evaluation of residual risks, and PIA documentation. Taking into account the new challenges of user privacy management, Lo et al. [29] worked out LRPdroid, a user privacy analysis framework for the Android platform, to detect the information leak and evaluate user privacy leak and privacy risks for applications installed on android-based mobile devices. These methods have significant reference value for the risk assessment of this paper. However, only a certain class of privacy security risk was evaluated with above methods, taking into account neither the interaction between various risks nor the risk characteristics of m-commerce applications.

In order to be able to put forward an effective m-commerce privacy security assessment method, this paper will collate relevant risk factors, establish a multilevel and multiangle assessment model, which constructs the hierarchy analysis model of privacy risk, uses information entropy to describe privacy risks, simulates and analyses a real risk environment of m-commerce application based on Markov chain, and realizes the effective assessment of the privacy security of m-commerce users. The privacy security risk assessment method proposed in this paper aim to provide a comprehensive method for the accurate and quantitative evaluation of privacy disclosure risk in real risk environment of m-commerce application.

3. Method Development for Risk Assessment Based on Information Entropy and Markov Chain

For the purpose of risk assessment, this paper proposes to integrate information entropy and Markov chain into the privacy risk assessment of m-commerce users; the framework of our work is shown in Figure 1.

As shown in Figure 1, our proposed assessment method is developed to integrate the works on the three parts.

3.1. Development of Risk Measurement Method Based on Information Entropy. Information entropy was proposed by Shannon in 1948. In Shannon's theory, information entropy

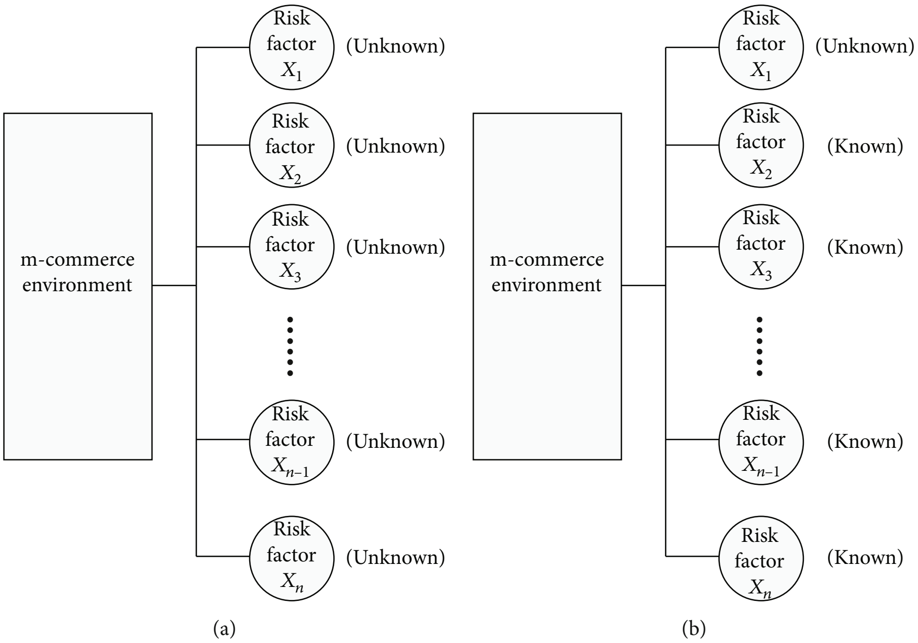


Figure 2: Comparison of two extreme risk factors in m-commerce environment.

is measured by the well-known formula $H(X) = -\sum_{i=1}^{n} P(X_i) \log_2 P(X_i)$, where X_i is the information source variable and $P(X_i)$ is the probability of the information source. In information theory, information entropy is used to represent the amount of information content and quantify the uncertainty of things.

Privacy security is not so objective to be easily measured. However, with the method of information entropy, it can be described from the perspective between known to unknown, the two opposite extremes. That is, the privacy risks of users are described with the characteristics of information entropy uncertainty, as shown in Figure 2.

Figure 2(a) shows the mobile business environment with n unknown risks X_i, i.e., $X = \{X_1, X_2, \cdots, X_n\}$; according to the information entropy theory, its entropy value $H(X)$ will reach its maximum, $H(X) = \log_2 n$, when all the risks occur with the same probability, that is $P(X_1) = P(X_2) = , \cdots, = P(X_n)$. This idea also suggests that the higher the user privacy risk uncertainty, the lower the controllability of the risks, and the lower the security.

Figure 2(b) shows the opposite case, when there is only one unknown risk in the m-commerce environment and the other risks are controllable, the entropy value $H(X)$ will reach its minimum according to the information entropy theory, indicating that the lower the privacy security risk uncertainty of the application, the higher the security, namely, the risk is substantially controllable.

3.2. Simulation of Risk Environment Based on Markov Chain. Markov chain [30, 31] is a discrete time random process of continuous transition from one state to another in the finite state space. It can describe the state space of the change of state of things and calculate the probability of occurrence of each random state of things by establishing Markov chain transfer matrix.

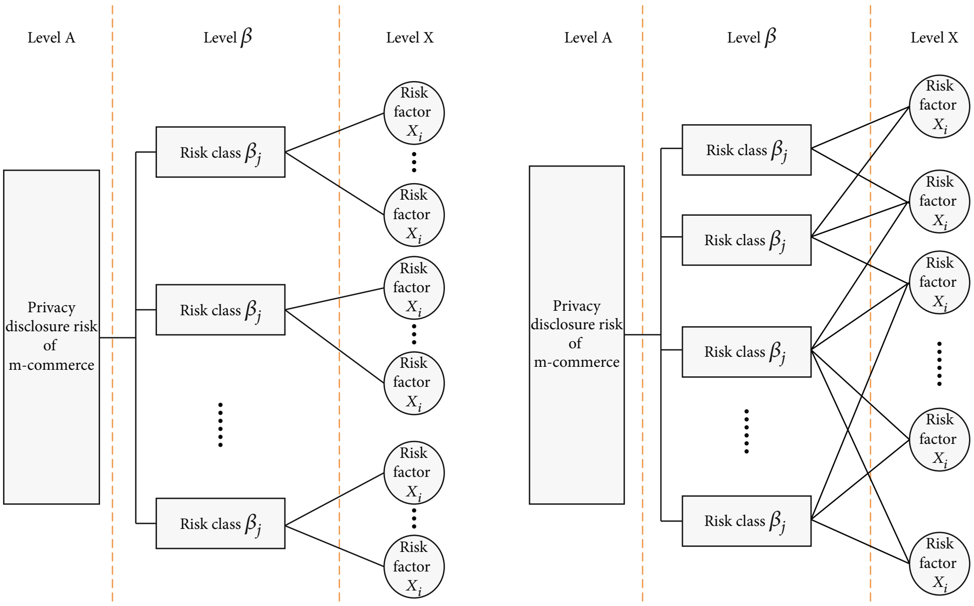
In addition to effective risk measurement method, the user privacy disclosure risk of m-commerce still needs to be assessed, and the random state in the practical application shall be analyzed, so as to ensure the validity of the assessment results. Therefore, the complex environment of user privacy disclosure risk in m-commerce is described in line with Markov chain, to achieve effective assessment of the user privacy security based on the practical conditions.

Assuming that there are n risk factors X_i in an m-commerce environment, according to Markov chain, this complex risk environment can be described as the following matrix taking into account the mutual influence between every two factors:

$$R = \begin{bmatrix} X_{11}X_{12} & & \cdots & X_{1n} \\ X_{21} & X_{22} & & X_{2n} \\ \vdots & & \ddots & \vdots \\ X_{n1} & X_{n2} & \cdots & X_{nn} \end{bmatrix}. \quad (1)$$

Matrix R is an m-commerce privacy risk matrix, where the elements X_{ii} on the diagonal line represent the separate occurrence of risk factors X_i, and X_{ij} represent simultaneous occurrence of risk factors X_i and X_j in the actual application process. The matrix R represents the complex privacy risk environment of m-commerce users by mathematical method, which provides a guarantee for the simulation analysis of this paper.

3.3. Construction of Risk Hierarchy. In the above discussions, we outline a method for descripting the privacy risk based



Traditional hierarchy of user privacy risk analysis

The hierarchy of privacy risk of mobile commerce users

Figure 3: The hierarchy of privacy risk of m-commerce users.

Table 2: Risk categories β_1 and β_2 and the risk factors they contain.

Risk class	Risk factors included risk class
β_1	X_1, X_2, X_3
β_2	X_3, X_4

on information entropy, and we develop a Markov matrix to simulate the complexity of risk environment for m-commerce. In our framework, it is still necessary to further establish a risk hierarchy to allow for multidimensional and multilevel simulation analysis of m-commerce user privacy risk, which is shown in Figure 3.

This hierarchy consists of three levels, target level A, risk class level β, and risk factor level X. Each risk class β_j includes multiple risk factors X_i. Different from the traditional user privacy risk analysis, our proposed analyzing framework presents a cross relationship between risk factors and risk class, which is more consistent with the real risk environment of m-commerce.

3.4. Development of the Proposed Assessment Method. A bottom-up process is used to the hierarchy in our method. In the following discussions, we use $P(X_i)$ to represent the probability of occurrence of risk X_i at level 3, and normalization process is carried out based on the classified categories, to calculate the probabilities $P(X_{ij})\ i, j = 1, 2, \cdots, n$ of risk occurrence under different categories, which are substituted into the matrix R to further obtain the state transition matrix $P(R)$ of the m-commerce privacy.

The calculation process is as shown in the following example: it is assumed that there are two risk classes, namely, β_1 and β_2, which include risk factors as shown in Table 2.

As shown in Table 1, class β_1 includes particular risk factor X_1, class β_2 includes particular risk factor X_4, while risk factor X_3 is included in both β_1 and β_2, then their transition state matrix can be derived through calculation.

$$P(R) = \begin{bmatrix} P(\beta_{11}) & P(\beta_{12}) \\ P(\beta_{21}) & P(\beta_{22}) \end{bmatrix} = \begin{bmatrix} \dfrac{1}{\sum_{i=1}^{3} P(X_i)} P(X_1) + P(X_2) & \dfrac{1}{\sum_{i=1}^{3} P(X_i)} P(X_3) \\ \dfrac{1}{\sum_{i=3}^{4} P(\alpha_i)} P(X_3) & \dfrac{1}{\sum_{i=3}^{4} P(\alpha_i)} P(X_4) \end{bmatrix}. \tag{2}$$

Similarly, according to formula (2), it is assumed that there are m risk classes β_i and n risk factors X_i in an m-commerce, then the privacy risk transfer matrix $P(R)$ for this m-commerce application can be derived based on the classified classes.

$$P(R) = \begin{bmatrix} P(X_{11}) & P(X_{12}) & \cdots & P(X_{1m}) \\ P(X_{21}) & P(X_{22}) & & P(X_{2m}) \\ \vdots & & \ddots & \vdots \\ P(X_{m1}) & P(X_{m2}) & \cdots & P(X_{mm}) \end{bmatrix}. \tag{3}$$

It is assumed that in the long utilization, the steady-state probability of class β_i is $\widehat{P}(\beta_i), \mathrm{i} = 1, 2, \cdots, m$. It is a

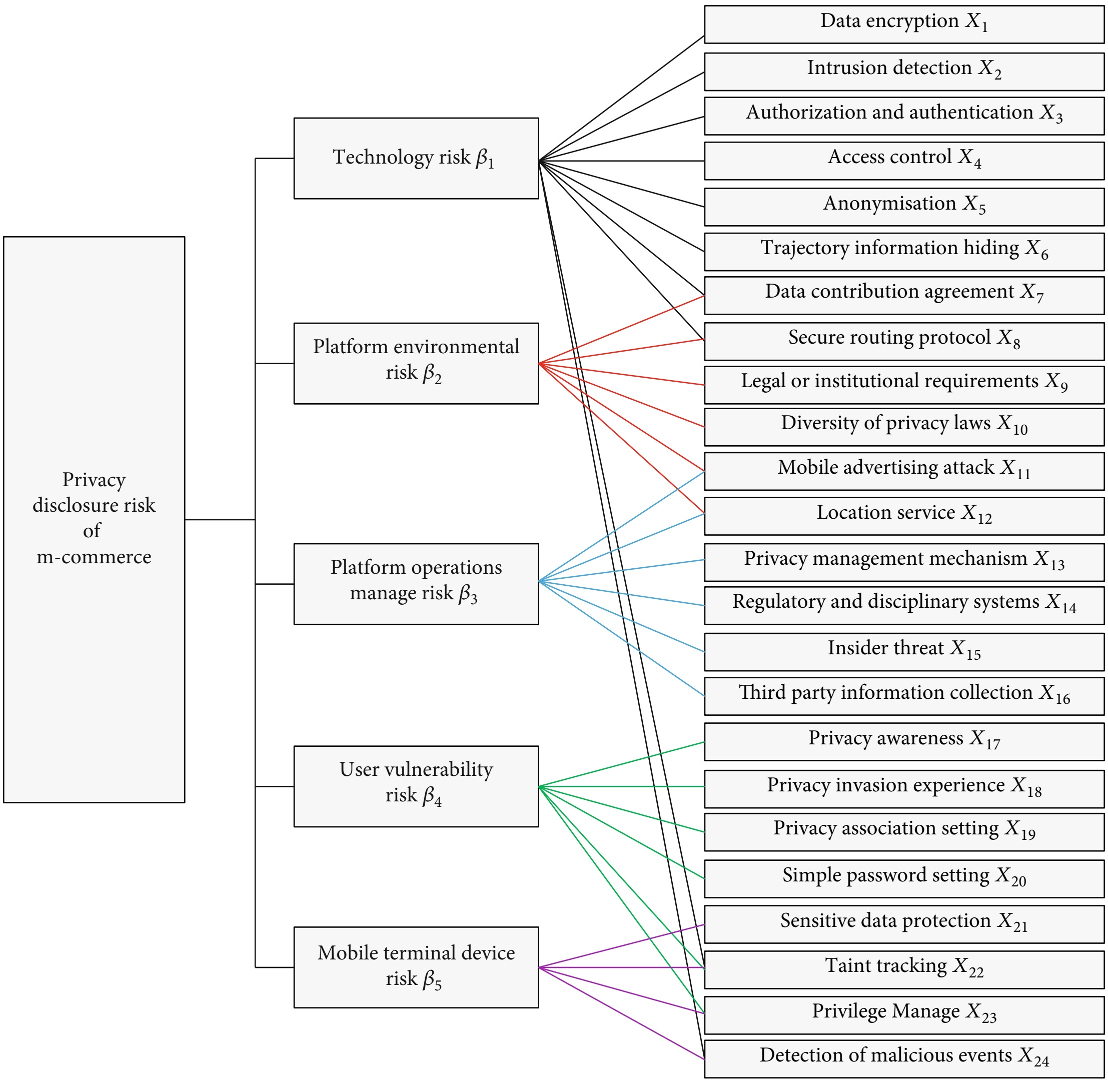

Privacy disclosure risk of m-commerce
Technology risk β_1
Platform environmental risk β_2
Platform operations manage risk β_3
User vulnerability risk β_4
Mobile terminal device risk β_5
Data encryption X_1
Intrusion detection X_2
Authorization and authentication X_3
Access control X_4
Anonymisation X_5
Trajectory information hiding X_6
Data contribution agreement X_7
Secure routing protocol X_8
Legal or institutional requirements X_9
Diversity of privacy laws X_{10}
Mobile advertising attack X_{11}
Location service X_{12}
Privacy management mechanism X_{13}
Regulatory and disciplinary systems X_{14}
Insider threat X_{15}
Third party information collection X_{16}
Privacy awareness X_{17}
Privacy invasion experience X_{18}
Privacy association setting X_{19}
Simple password setting X_{20}
Sensitive data protection X_{21}
Taint tracking X_{22}
Privilege Manage X_{23}
Detection of malicious events X_{24}

Figure 4: Hierarchical attribute model of privacy disclosure risk in m-commerce.

possible probability of a certain risk class in the long stable utilization and a stable probability calculated by the Markov method. According to this method, the relation between $\widehat{P}(\beta_i)$ and sate transition matrix $P(R)$ satisfies the following equation:

$$\begin{cases} \widehat{P}(\beta_1) = P(X_{11})\widehat{P}(\beta_1) + \mathrm{P}(X_{12})\widehat{P}(\beta_2) + \cdots + \mathrm{P}(X_{1m})\widehat{P}(\beta_m) \\ \widehat{P}(\beta_2) = P(X_{21})\widehat{P}(\beta_1) + \mathrm{P}(X_{22})\widehat{P}(\beta_2) + \cdots + \mathrm{P}(X_{2m})\widehat{P}(\beta_m) \\ \widehat{P}(\beta_3) = P(X_{31})\widehat{P}(\beta_1) + \mathrm{P}(X_{32})\widehat{P}(\beta_2) + \cdots + \mathrm{P}(X_{3m})\widehat{P}(\beta_m) \\ \vdots \\ \widehat{P}(\beta_\mathrm{m}) = P(X_{m1})\widehat{P}(\beta_1) + \mathrm{P}(X_{m2})\widehat{P}(\beta_2) + \cdots + \mathrm{P}(X_{mm})\widehat{P}(\beta_m) \\ 1 = \widehat{P}(\beta_1) + \widehat{P}(\beta_2) + \cdots + \widehat{P}(\beta_m) \end{cases} . \quad (4)$$

The occurrence probability of various risks $\widehat{P}(\beta_i) = \{\widehat{P}(\beta_1), \widehat{P}(\beta_2), \cdots, \widehat{P}(\beta_m)\}, \sum_{i=1}^{m} \widehat{P}(\beta_i) = 1$ in the longstable utilization of the m-commerce application can be derived by solving the Equation (3).

Table 3: The level of probability of risk factors occurrence.

Level	Definition and description
(8, 10)	This factor has a great risk and a direct threat to the user's privacy
(6, 8)	This risk has a high probability of occurrence and exists in most m-commerce environments
(4, 6)	This risk is a common risk, which exists in some m-commerce
(2, 4)	This risk exists and only occurs when special conditions are met
(0, 2)	This factor has high security and hardly causes user privacy risk

Therefore, the privacy risk assessment results H of the entire m-commerce environment can be calculated by

Table 4: Scoring results of probability of occurrence of underlying risk factors.

Company	Risk factor x_i	Level	$P(x_i)$	Risk factor x_i	Level	$P(x_i)$	Risk factor x_i	Level	$P(x_i)$
A	X_1	2	1.887%	X_9	2	1.887%	X_{17}	9	8.491%
	X_2	2	1.887%	X_{10}	2	1.887%	X_{18}	9	8.491%
	X_3	3	2.830%	X_{11}	7	6.604%	X_{19}	7	6.604%
	X_4	3	2.830%	X_{12}	7	6.604%	X_{20}	6	5.660%
	X_5	1	0.943%	X_{13}	2	1.887%	X_{21}	5	4.717%
	X_6	1	0.943%	X_{14}	3	2.830%	X_{22}	4	3.774%
	X_7	6	5.660%	X_{15}	2	1.887%	X_{23}	6	5.660%
	X_8	6	5.660%	X_{16}	7	6.604%	X_{24}	4	3.774%
B	X_1	2	2.000%	X_9	2	2.000%	X_{17}	9	9.000%
	X_2	7	7.000%	X_{10}	2	2.000%	X_{18}	8	8.000%
	X_3	3	3.000%	X_{11}	3	3.000%	X_{19}	9	9.000%
	X_4	2	2.000%	X_{12}	2	2.000%	X_{20}	1	1.000%
	X_5	2	2.000%	X_{13}	5	5.000%	X_{21}	5	5.000%
	X_6	2	2.000%	X_{14}	3	3.000%	X_{22}	4	4.000%
	X_7	4	4.000%	X_{15}	2	2.000%	X_{23}	7	7.000%
	X_8	4	4.000%	X_{16}	8	8.000%	X_{24}	4	4.000%
C	X_1	1	0.901%	X_9	2	1.802%	X_{17}	9	8.108%
	X_2	1	0.901%	X_{10}	2	1.802%	X_{18}	9	8.108%
	X_3	3	2.703%	X_{11}	2	1.802%	X_{19}	9	8.108%
	X_4	2	1.802%	X_{12}	9	8.108%	X_{20}	2	1.802%
	X_5	1	0.901%	X_{13}	8	7.207%	X_{21}	3	2.703%
	X_6	9	8.108%	X_{14}	3	2.703%	X_{22}	4	3.604%
	X_7	8	7.207%	X_{15}	2	1.802%	X_{23}	8	7.207%
	X_8	3	2.703%	X_{16}	7	6.306%	X_{24}	4	3.604%

substituting $\widehat{P}(\beta_i)$ into the following information entropy formula (5):

$$H = -\sum_{i=1}^{m} \widehat{P}(\beta_i) \log_2 \widehat{P}(\beta_i), \tag{5}$$

where H represents the entropy value for privacy security of the m-commerce users, and the greater its value, the lower the privacy security of the m-commerce. The entropy value of the risk class β_{i} can be derived by normalizing the occurrence probability of risk factors included in such class following the information entropy calculation method, and the greater this value, the lower the privacy security of this risk class.

4. Integration of the Assessment Method

4.1. Risk Attribute Model for Privacy Disclosure of m-commerce Users. According to the assessment method proposed in Section 3, 24 risk evaluation indicators for privacy information disclosure of m-commerce users are selected, and these indicators are divided into 5 classes, i.e., technology risk, platform environmental risk, platform operation manage risk, user vulnerability risk, and mobile terminal device risk. According to the hierarchical structure in Figure 3, a hierarchical attribute model for privacy disclosure risk is built, as shown in Figure 4.

4.2. Measurement and Assessment of Privacy Disclosure Risks. Based on the m-commerce user privacy risk attribute model in Figure 4 and in accordance with the assessment method proposed herein, the detailed calculation process is as follows:

Step 1. Table 3 “the level of probability of risk factors occurrence” is prepared, and the occurrence probability level of the lowest-level risk factors is obtained through scoring by experts, and the values of $P(X_i)$ obtained through normalization processing.

Step 2. Based on the hierarchical structure in Figure 4 and according to Markov chain, use Equation (2) to calculate the state transition matrix $P(R)$.

Table 5: The steady-state probability of risk class.

Company	β_i	$\widehat{P}(\beta_\text{i})$	Company	β_i	$\widehat{P}(\beta_\text{i})$	Company	β_i	$\widehat{P}(\beta_\text{i})$
A	β_1	0.159	B	β_1	0.119	C	β_1	0.135
	β_2	0.181		β_2	0.163		β_2	0.172
	β_3	0.190		β_3	0.203		β_3	0.192
	β_4	0.247		β_4	0.277		β_4	0.266
	β_5	0.228		β_5	0.247		β_5	0.242

Table 6: Comparison of evaluation results of three companies.

Company	Risk entropy H
A	2.307
B	2.270
C	2.288

Step 3. Use Equation (4) to calculate the stability probability $\widehat{P}(\beta_i)$ of various risks.

Step 4. Use formula (5) to calculate H, so as to evaluate the privacy security of the entire m-commerce environment.

Step 5. Normalize the probability of occurrence of these risk factors to obtain their weight coefficients $P(X_j, \beta_i)$ in different risk classes. Then, calculate various risk entropy $H(\beta_\text{i})$ in combination with the information entropy formula with the following.

$$H(\beta_\text{i}) = \frac{-\sum_{j=1}^{m} P(X_j, \beta_i) \log_2 P(X_j, \beta_i)}{\log_2 m}, \tag{6}$$

where m is the number of risk factors included in risk class β_i. The larger this value is, the more difficult it is to control such risks, and the greater the privacy security risk will be.

5. Case Study

5.1. Assessment Process. In order to verify the feasibility of the proposed method, three companies with different nature in m-commerce applications background are selected and assessed from bottom to top in details, where company A provides food delivery m-commerce service, company B provides financial m-commerce service, and company B provides map navigation service. The three applications all carry the users' privacy data like information of finance, identity, location, and device. The assessment is specifically carried out for these three companies as follows:

Step 1. First of all, the bottom risk factors x_i of three m-commerce applications are scored by a panel of 10 experts with AHP [32] method according to the definitions in Table 3. After the scoring is completed, the scores of 10 experts are summed up, averaged to obtain their level, and the level is further normalized to obtain the value of $P(x_i)$, and the results are shown in Table 4.

Table 7: Normalization results of risk factors contained in each risk class.

Risk class β_i	Risk factor x_j contained in β_i
β_1	$\{x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_{22}, x_{24}\}$
β_2	$\{x_7, x_8, x_9, x_{10}, x_{11}, x_{12}\}$
β_3	$\{x_{11}, x_{12}, x_{13}, x_{14}, x_{15}, x_{16}\}$
β_4	$\{x_{17}, x_{18}, x_{19}, x_{20}, x_{22}, x_{23}\}$
β_5	$\{x_{21}, x_{22}, x_{23}, x_{24}\}$

Step 2. Based on the hierarchical structure in Figure 4, the results of Table 4 are substituted into formula (2), to obtain the following state transition matrices $P^\text{A}(R)$, $P^\text{B}(R)$, and $P^\text{C}(R)$ for privacy disclosure risk of m-commerce users of the three companies.

$$\begin{aligned}
P^\text{A}(R) &= \begin{bmatrix} 0.375 & 0.375 & 0.000 & 0.000 & 0.250 \\ 0.400 & 0.133 & 0.467 & 0.000 & 0.000 \\ 0.000 & 0.500 & 0.500 & 0.000 & 0.000 \\ 0.000 & 0.000 & 0.000 & 0.756 & 0.244 \\ 0.211 & 0.000 & 0.000 & 0.526 & 0.263 \end{bmatrix}, \\
P^\text{B}(R) &= \begin{bmatrix} 0.529 & 0.235 & 0.000 & 0.000 & 0.235 \\ 0.471 & 0.235 & 0.294 & 0.000 & 0.000 \\ 0.000 & 0.217 & 0.783 & 0.000 & 0.000 \\ 0.000 & 0.000 & 0.000 & 0.711 & 0.289 \\ 0.200 & 0.000 & 0.000 & 0.550 & 0.250 \end{bmatrix}, \\
P^\text{C}(R) &= \begin{bmatrix} 0.472 & 0.306 & 0.000 & 0.000 & 0.222 \\ 0.423 & 0.154 & 0.423 & 0.000 & 0.000 \\ 0.000 & 0.355 & 0.645 & 0.000 & 0.000 \\ 0.000 & 0.000 & 0.000 & 0.707 & 0.293 \\ 0.211 & 0.000 & 0.000 & 0.632 & 0.158 \end{bmatrix}.
\end{aligned} \tag{7}$$

Step 3. The data in the above transition matrices are substituted into formula (4) to calculate the steady-state probability of various risks, as shown in Table 5.

Step 4. The calculated results of Table 5 are substituted into formula (5) to obtain the user privacy security evaluation results of three companies' m-commerce applications, as shown in Table 6.

Step 5. The risk factors included in different risk classes are further normalized. The known risk classes and the contained risk factors are shown in Table 7.

Based on the division of Table 7, the level-2 risk classes of three different m-commerce companies are evaluated in this paper, and the calculated entropy values of various risks are shown in Figure 5.

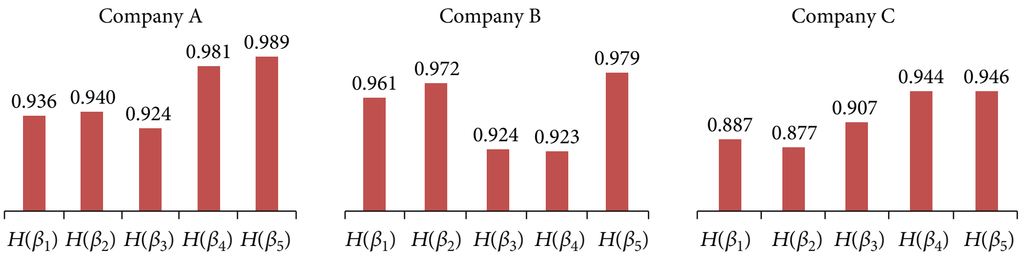


Figure 5: Comparison of entropy values of various risk class.

5.2. Analysis of Assessment Results. According to the results of the assessment and the proposed risk hierarchy, the analysis is carried out level by level:

5.2.1. Analysis of Top-Level Evaluation Results. The comparison of Table 6 shows that $H(\mathrm{A}) > H(\mathrm{C}) > H(\mathrm{B})$, indicating that the food delivery m-commerce application of company A has higher privacy risk compared with the other two applications; on the contrary, company B's financial m-commerce application enjoys the highest privacy security.

However, the privacy security evaluation results of the three companies are not very different in data size, indicating that on the whole, the three companies have similar privacy security performance and certain privacy and security factors.

5.2.2. Analysis of Middle-Level Evaluation Results

(1) Comparative Analysis of Steady-State Probability Results of Risk Classes. It is found in Table 5 that $\widehat{P}(\beta_4) > \widehat{P}(\beta_5) > \widehat{P}(\beta_3) > \widehat{P}(\beta_2) > \widehat{P}(\beta_1)$. This result shows that the three companies share one marked characteristic, namely, the value $\widehat{P}(\beta_4)$ is the greatest, indicating that compared with other risk classes, user vulnerability risk β_4 is most likely to occur in the long utilization of m-commerce application. Secondly, the value of $\widehat{P}(\beta_5)$ is great, which suggests that while user vulnerability risk can easily arise, the terminal device often causes security problems. On the contrary, the value of the technical risk $\widehat{P}(\beta_1)$ is the smallest, which indicates that technology risk is not the main cause of the user's privacy information security problem, and compared with other risk classes, it is not likely that the privacy security problems are caused by technology risk.

Thus, it can be seen that when m-commerce users disclose personal information in pursuit of personalized services provided by the m-commerce platform, there are mainly problems such as low awareness of privacy risks, numerous privacy association settings, insufficient experience in privacy invasion, and simple password setting, etc. The above situation poses a great threat to user privacy. Users should strengthen their awareness of privacy protection and improve their ability to deal with risks. While enjoying the convenience brought by m-commerce, users should also understand the risks and avoid excessive disclosure of their private information.

(2) Analysis of Comparison Results of Entropy Value of Risk Classes. Figure 5 shows that the $H(\beta_5)$ values of the three companies are the greatest, indicating that it is most difficult to control the mobile terminal device risk.

Moreover, the evaluation results show high $H(\beta_4)$ of company A and company C, indicating that when utilizing the m-commerce applications of these two companies, the users could hardly control their own privacy risk, giving rise to privacy security issues in these applications (take-away catering, map navigation). By contrast, the value of financial application $H(\beta_4)$ is low, which suggests that the users' behavior and operation are strictly regulated in such application, and its user risk is easier to control compared with other applications. This comparison shows that platform environment risk $H(\beta_2)$ should be mainly blamed for the leakage of such application privacy information.

5.2.3. Analysis of Bottom-Level Evaluation Results. The above comparison shows that the user vulnerability risk β_4 has the highest probability of occurrence. There is an observation of the bottom factors of such risk class that the security problems of m-commerce applications are mainly caused by the users' weak privacy risk awareness x_{17}, excessive privacy association settings x_{18}, the lack of privacy invasion experience x_{19}, and simple password setting x_{20} and so on.

In the financial application, the platform environment risk β_2 has the greater probability of occurrence, it is affected by x_7, x_8, x_9, and so on. This result shows that the privacy security problem is mainly caused by the platform environment risk factors such as the data sharing agreement with the users x_7, the security routing agreement x_8, the formulation of privacy law x_9, and so on.

5.3. Suggestions and Remarks. It is well known that it is not feasible to only improve the privacy security of m-commerce users by the use of technique tools. The current risk problems mainly arise from the weak privacy security awareness of users, and the security issues of m-commerce applications will not be effectively solved until the users are more aware of and better understand the privacy security issues. For this purpose, the operator should more diligently remind the users on privacy security in the utilization of m-commerce applications, standardize their relevant operation as much as possible, and urge them to take security protection measures. On the other hand, for some financial applications, more explicit confidentiality agreement shall be signed with the users, the access to the users' permission shall be reduced, relevant responsibilities shall be clarified, and guarantee the information security of the users through laws and regulations.

6. Conclusions

In this paper, the risk factors of user privacy disclosure in m-commerce are reviewed, the magnitude of risks is measured based on information entropy, to provide effective data support for risk assessment. We have detailed discussed the complexity of user privacy risk in the real environment, and a complete assessment model for user privacy disclosure risks is established, and reasonable risk measurement and assessment methods are proposed based on Markov chain. In addition, a detailed comparative analysis is carried out based on the actual application that can provide practical reference for the protection of the privacy security of m-commerce users, and enrich and improve the relevant research theory of user privacy security. In the future research, with the update of the m-commerce application service, it is necessary to keep track of the latest research theories and further improve the attribute model of the user privacy risk. Moreover, the risks can be divided in line with actual application into more classes, which can be selected based on relevant risk factors, to realize more accurate assessment and research on user privacy security.

Data Availability

The expert scoring data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work was supported by the National Natural Science Foundation Project (No. 71462036), Yunnan Basic Applied Research Program (No. 2017FD130), the Scientific Research Foundation of Yunnan Education Department (No. 2020J0377, No. 2020J0392, and No. 2020J0378), and School-level Project of Yunnan University of Finance and Economics (No. 2017D29, No. 2018B07, and No. 2018B08).

References

[1] C. Cao and X. Zhu, “Strong anonymous mobile payment against curious third-party provider,” *Electronic Commerce Research*, vol. 19, no. 3, pp. 501–520, 2019.

[2] Y. Lei, “The top 10 data breaches of 2019,” *Computer Networks*, vol. 46, no. 2, pp. 46-47, 2020.

[3] Y. Z. Xu, J. L. Zhang, Y. Hua, and L. Y. Wang, “Dynamic Credit Risk Evaluation Method for E-Commerce Sellers Based on a Hybrid Artificial Intelligence Model,” *Sustainability*, vol. 11, no. 19, 2019.

[4] Y. Zhang, R. Wang, M. S. Hossain, M. F. Alhamid, and M. Guizani, “Heterogeneous Information Network-Based Content Caching in the Internet of Vehicles,” *IEEE Transactions on Vehicular Technology*, vol. 68, no. 10, pp. 10216–10226, 2019.

[5] Y. Wu, G. Feng, N. Wang, and H. Liang, “Game of information security investment: Impact of attack types and network vulnerability,” *Expert Systems with Applications*, vol. 42, no. 15-16, pp. 6132–6146, 2015.

[6] F. Shirazi and A. Iqbal, “Community clouds within M-commerce: a privacy by design perspective,” *Journal of Cloud Computing*, vol. 6, no. 1, 2017.

[7] E. Aghasian, S. Garg, and J. Montgomery, “A Privacy-Enhanced Friending Approach for Users on Multiple Online Social Networks,” *Computers*, vol. 7, no. 3, article 7030042, 2018.

[8] Y. Zhang, Y. Qian, M. S. H. Di Wu, A. Ghoneim, and M. Chen, “Emotion-Aware Multimedia Systems Security,” *IEEE Transactions on Multimedia*, vol. 21, no. 3, pp. 617–624, 2019.

[9] Y. Ashibani and Q. H. Mahmoud, “Cyber physical systems security: Analysis, challenges and solutions,” *Computers and Security*, vol. 68, pp. 81–97, 2017.

[10] H. Zhu, C. X. J. Ou, W. J. A. M. van den Heuvel, and H. Liu, “Privacy calculus and its utility for personalization services in e-commerce: An analysis of consumer decision-making,” *Information and Management*, vol. 54, no. 4, pp. 427–437, 2017.

[11] M. Fodor and A. Brem, “Do privacy concerns matter for Millennials? Results from an empirical analysis of location-based services adoption in Germany,” *Computers in Human Behavior*, vol. 53, pp. 344–353, 2015.

[12] V. M. Wottrich, E. A. van Reijmersdal, and E. G. Smit, “The privacy trade-off for mobile app downloads: The roles of app value, intrusiveness, and privacy concerns,” *Decision Support Systems*, vol. 106, pp. 44–52, 2018.

[13] A. Gutierrez, S. O'Leary, N. P. Rana, Y. K. Dwivedi, and T. Calle, “Using privacy calculus theory to explore entrepreneurial directions in mobile location-based advertising: Identifying intrusiveness as the critical risk factor,” *Computers in Human Behavior*, vol. 95, pp. 295–306, 2019.

[14] G. Ampong, A. Mensah, A. Adu, J. Addae, O. Omoregie, and K. Ofori, “Examining Self-Disclosure on Social Networking Sites: A Flow Theory and Privacy Perspective,” *Behavioral Sciences*, vol. 8, no. 6, pp. 58–75, 2018.

[15] G. Zhu, M. N. Feng, Y. Chen, and J. Y. Yang, “Research on Fuzzy Evaluation of Privacy Risk for Social Network in Big Data Environment,” *Information Science*, vol. 34, no. 9, pp. 94–98, 2016.

[16] B. Tian, Y. S. Zheng, P. Y. Liu, and C. H. Li, “The evaluation index and empirical study on risk of privacy information disclosure of mobile APP users,” *Library and Information Services*, vol. 62, no. 19, pp. 101–110, 2018.

[17] M. M. Xiang, X. W. Wang, R. N. Jia, and L. Wang, “Research on the Risk Evaluation of Consumers' Privacy Information Disclosure in Mobile Commerce,” *Library and information service*, vol. 62, no. 18, pp. 34–44, 2018.

[18] Y. Nan, Z. Yang, M. Yang et al., “Identifying User-Input Privacy in Mobile Applications at a Large Scale,” *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 3, pp. 647–661, 2017.

[19] Y. Zhang, X. Ma, J. Zhang, M. S. Hossain, G. Muhammad, and S. U. Amin, "Edge Intelligence in the Cognitive Internet of Things: Improving Sensitivity and Interactivity," *IEEE Network*, vol. 33, no. 3, pp. 58–64, 2019.

[20] H. Li, B. Wang, W. Zhang, Q. Tang, and Y. L. Zhang, "X-Decaf : Detection of Cache File Leaks in Android Social Apps," *Journal of Electronics & Information Technology*, vol. 39, no. 1, pp. 66–74, 2017.

[21] Y. A. Tan, Y. Xue, C. Liang et al., "A root privilege management scheme with revocable authorization for Android devices," *Journal of Network and Computer Applications*, vol. 107, pp. 69–82, 2018.

[22] A. Ruiz-Heras, P. García-Teodoro, and L. Sánchez-Casado, "ADroid: anomaly-based detection of malicious events in Android platforms," *International Journal of Information Security*, vol. 16, no. 4, pp. 371–384, 2017.

[23] T. L. Gao, T. Li, R. Jiang, M. Yang, and R. Zhu, "Research on cloud service security measurement based on information entropy," *International Journal of Network Security*, vol. 21, no. 6, pp. 1003–1013, 2019.

[24] M. Yang, R. Jiang, T. L. Gao, W. Y. Xie, and J. Wang, "Research on cloud computing security risk assessment based on information entropy and Markov chain," *International Journal of Network Security*, vol. 20, no. 4, pp. 664–673, 2018.

[25] G. Tilei, L. Tong, Y. Ming, and J. Rong, "Research on a Trustworthiness Measurement Method of Cloud Service Construction Processes Based on Information Entropy," *Entropy*, vol. 21, no. 5, 2019.

[26] J. Wang, J. Liu, and H. Zhang, "Access Control Based Resource Allocation in Cloud Computing Environment," *International Journal of Network Security*, vol. 19, no. 2, pp. 236–243, 2017.

[27] Y. C. Wei, W. C. Wu, G. H. Lai, and Y. C. Chu, "pISRA: privacy considered information security risk assessment model," *The Journal of Supercomputing*, vol. 76, no. 3, pp. 1468–1481, 2020.

[28] M. C. Oetzel and S. Spiekermann, "A systematic methodology for privacy impact assessments: a design science approach," *European Journal of Information Systems*, vol. 23, no. 2, pp. 126–150, 2019.

[29] N.-W. Lo, K.-H. Yeh, and C.-Y. Fan, "Leakage Detection and Risk Assessment on Privacy for Android Applications: LRPdroid," *IEEE Systems Journal*, vol. 10, no. 4, pp. 1361–1369, 2016.

[30] W. J. Stewart, *Introduction to the numerical solutions of Markov chains*, USA:Princeton University Press, Princeton, 1994.

[31] W. J. Stewart, *Probability, Markov Chains, Queues, and Simulation: the Mathematical Basis of Performance Modeling. Princeton*, Princeton University Press, Princeton,USA, 2009.

[32] M. Yang, T. B. Li, R. Jiang, T. L. Gao, and J. Wang, "Research on Model of Big Data Usability and Mining Strategy Based on AHP," *Computer Technology and Development*, vol. 28, no. 5, pp. 51–58, 2018.