scientific reports

Check for updates

OPEN

Comprehensive assessment of privacy security of financial services in cloud environment

Dongri He[1], Ming Yang[1]✉, Rong Jiang[1,2], Tiebing Li[1] & Jia Wang[1]

In recent years, the financial industry has become a disaster area for information leakage, which has serious implications for user privacy security. In the absence of risk identification and assessment, the risk will be difficult to prevent, and once the risk occurs it will directly cause serious losses. Therefore, this study plans to construct a comprehensive assessment framework combining fuzzy analytic hierarchy process (FAHP) and Dempster-Shafer (D-S) theory, aiming at assessing the weights and risk levels of the privacy security risks of financial services. (Privacy security risks refer to integrated factors in management, security, or other aspects that may lead to user privacy leakage, and they are considered an integrated concept.) The case study illustrates that the model and method proposed in this paper are effective and feasible. Finally, a comparison with the current mainstream privacy security assessment methods demonstrates that the method proposed in this paper is more capable of objectively and quantitatively reflecting the real privacy risks, providing users with more perspectives of the assessment results, and helping users to reasonably manage their personal privacy information, so as to effectively prevent and control the privacy risks.

Keywords Financial services, Assessment, Risk levels, Weight

In June 2022, the World Bank released data from its latest Global Financial Inclusion Survey (The Global Findex Database 2021)[1]. The database is based on a 3-year period. The data show that the proportion of people with bank accounts is growing globally, and account ownership in China has reached nearly 90%. 76% of respondents globally said that they have an account, an increase of 8% points from 2017. In China, the figure stood at 89%, representing an increase of 9% points compared to 2017. The significant increase in account ownership means that demand for financial inclusion and financial services continues to grow globally, highlighting the growing reliance of individuals worldwide on financial services to manage their finances, access banking services and participate in the economy.

With the development of the Internet and the financial industry, a large number of users enjoy the convenience and efficiency brought by financial technology services. But as financial markets continue to grow, an increasing number of users are facing more and more serious financial privacy security issues. Even though nowadays there are cryptography, double authentication (2FA) and multiple authentication (MFA), biometrics, blockchain and smart contract decentralisation and privacy-preserving consensus mechanisms[2] as approaches to financial privacy security protection. The financial industry involves a large amount of sensitive information, such as funds, transactions, customer identity, etc. This reality places extremely high demand on information security. The development of financial public clouds is still facing more serious challenges, including security issues in terms of information asset security and privacy protection, and trusted services[3] .

Verizon released its 2023 Annual Data Breach Investigations Report in June[4], in which Verizon analyzed 16,312 incidents, of which 5,199 were identified as data breaches. This breach count spanned 11 industries, with public affairs (582 breaches), financial services (477 breaches), and information technology (380 breaches) experiencing the highest numbers. According to the data in the report, 74% of the security incidents proved to have a human element, which means that in the past year, enterprise employees are repeatedly making mistakes, including misuse of permissions, abuse of privileges, phishing attacks, identity leaks, use of stolen credentials, etc., which poses a huge threat to the security of users' personal information and privacy. These privacy security issues are not only caused by human factors, but are also caused by a combination of technical vulnerabilities, security risks of end devices, and the operating environment of the services provider.

In the research on enhancing data privacy security in the financial industry, Hazzazi et al.[5] introduced a new encryption algorithm based on Turbo code, which eliminates the need to send keys through a secure channel and

[1]School of Information, Yunnan University of Finance and Economics, Kunming 650221, China. [2]Yunnan Key Laboratory of Service Computing, Kunming 650221, China. ✉email: yangming@ynufe.edu.cn

instead generates keys with preexisting data to achieve confidentiality in information exchanges among financial institutions. Most of the research is focused on blockchain technology, Alenizi et al.[6] proposed a framework for integrating blockchain and artificial intelligence (IBAI), which enhances data protection and improves the accuracy of detecting suspicious behavior such as hacking. Su et al.[7] combined blockchain and proxy re-encryption techniques to achieve secure data sharing among users by re-encrypting sensitive data. Wang et al.[8] proposed a blockchain method combining Convolutional Neural Network and Transformer structure, which can effectively identify abnormal transaction behavior and ensure the security of user assets.

While many scholars have provided multiple ways to secure user privacy in conjunction with blockchain technology, it cannot prevent employees from leaking data through non-blockchain channels, or when the blockchain technology application costs are too high, enterprises may choose not to adopt this technology[9], making the risks difficult to prevent. At this point, it becomes particularly important to assess the privacy risks of financial services provided by enterprises. Therefore, this paper establishes a comprehensive risk identification and assessment method that serves as an effective tool for platforms or third-party assessment institutions. When financial service providers intend to list their services on a platform, they are required to disclose relevant risk indicators to the platform. For users, who access corresponding financial services through the platform, they can choose appropriate services based on the platform's assessment results. The main contributions of this paper can be summarized as follows:

(1) This paper proposes a comprehensive privacy security assessment method for financial services, which can provide users and financial institutions with comprehensive assessment results. This method helps financial institutions manage and mitigate privacy risks more effectively, and helps improve data protection across the financial services industry and user trust in the financial services industry.
(2) In this paper, we combine the Fuzzy Analytic Hierarchy Process (FAHP) method, Dempster-Shafer (D-S) theory and Fuzzy theory to establish a privacy risk model for financial services. Solving the problem of consistency testing of the AHP and the disagreement in the multi-expert evaluation process.
(3) Through case analysis and comparison with existing mainstream risk assessment methods, this study verifies that the method proposed in this paper has higher objectivity, comprehensiveness and scalability in evaluating privacy security in financial services.

Relevant studies

With the help of cloud computing technology, financial institutions can more easily access key information in all links of the industrial chain. However, the use of large-scale financial data comes with multiple potential risks. Zhao et al.[10] pointed out that security and privacy issues have become the main obstacles to the development of financial cloud, including confidentiality and integrity protection of data, regulatory and legal risks, moral risks, and exit risks of financial public cloud services providers, and pointed out that a financial cloud security system should be built. In order to assess the privacy risks of financial services and better protect users' financial privacy, different scholars have explored it from different perspectives.

In analyzing the causes leading to the leakage of users' financial privacy, Peng et al.[11] analyzed the reasons for the leakage of users' personal financial data in cross-border flow as hacker attacks, system infrastructure vulnerabilities, and sharing of consumer information with unaffiliated third parties, etc., and proposed that various types of risks in the cross-border flow of financial data should be assessed. Sun[12] pointed out that the illegal collection and use of users' personal information by insiders of financial institutions have led to the leakage of a large amount of users' personal privacy, and emphasized that the elemental governance of financial data should be strengthened and the classification and grading of data supervision should be done well. Liu[13] pointed out that big data financial algorithms may also cause the leakage of users' financial privacy, especially big data financial customer profiling algorithms are the hardest hit by privacy leakage. The algorithms, in order to obtain as much information as possible about their customers, may "extract" or "force" personal financial information through "overbearing terms" in e-commerce contracts, and it is suggested that big data financial algorithms must comply with the regulation of the law.

In terms of how to effectively protect users' financial privacy, Huo et al.[14] proposed a privacy protection model based on cloud computing, which provides four different levels of privacy protection measures according to the actual needs of users. Dhiman et al.[15] achieved good results in securing financial privacy data through a federated learning approach with homomorphic encryption. Xu et al.[16] developed an image-based financial services privacy-preserving blockchain model which is capable of storing users' financial services data as images. This improves the security of user privacy by ensuring that users can understand the content and preventing the data from being recognized by machines. Qiu et al.[17] propose a model called Privacy Preserving Smart Storage (PS2) that uses a novel distributed data storage method to prevent attacks based on massive data mining by financial institution insiders.

In terms of effective early warning and assessment of financial services risks, Zhong et al.[18] designed a sensor network-based early warning system for cloud data storage security and financial risk management, which introduces a financial risk control module that can help users with financial risk warning and management. Luo et al.[19] proposed a systematic financial risk assessment algorithm based on fuzzy clustering analysis of risk data. The financial systemic risk measurement method established in this study can identify risks to a certain extent and deepen the understanding of the nature of systemic financial risks, serving as a long-term mechanism for constructing systems to prevent and resolve systemic financial risks. Alqahtani and Moorsel[20] developed a risk assessment method for EMV trading systems. The method enhances the decision-making process by analyzing, modeling, and evaluating the risks that may occur during EMV payment transactions. Zhang et al.[21] constructed a risk assessment model using big data indicators and integrated big data opinion indicators into traditional corporate financial risk assessment indicators, which effectively corrected the defects of the original

assessment model and improved the risk assessment results. Ali-Eldin et al.[22] introduced an effective model to evaluate privacy risks, which offers practical strategies for avoiding and mitigating privacy risks associated with open data. Yang et al.[23–25] quantify and evaluate privacy risks by analyzing the information uncertainty based on information entropy method.

Although the above-mentioned methods provide valuable solutions for enhancing the privacy security of financial services, there are still some deficiencies. To more systematically and clearly present the perspectives and shortcomings considered by the current methods, we have organized them into a table, as shown in Table 1 below.

From the research in the above table, it can be seen that financial services face a complex risk environment regarding privacy security in the current cloud environment. Existing evaluation methods are one-dimensional and cannot fully meet the needs of assessing the risks and changes in financial services. At this point, there is a need for a method that can analyze privacy risks of financial services from multiple perspectives, quantify risk levels, and be widely applicable to better protect user privacy.

Therefore, this paper proposes an integrated evaluation method that combines FAHP, fuzzy theory, and D-S evidence theory. First, the FAHP method is used to construct a comprehensive risk attribute system and calculate the weights of each indicator, effectively highlighting the importance of risks. Second, by introducing fuzzy theory and D-S evidence theory, combined with two dimensions—risk frequency and severity of consequences—the method ranks different risks. This not only quantifies the impact of uncertain factors but also provides a comprehensive risk classification and identification of key risk elements, ensuring users receive clear and scientific risk level information. This method is applicable regardless of whether companies use blockchain, making it highly applicable in various scenarios. In addition, the method in this paper does not depend on user information but only requires considering enterprise risk indicators, thus avoiding the issue of directly identifying user identities. Secondly, our model design takes into account the flexibility and adaptability, and can timely update and adjust relevant indicators according to the latest laws and regulations, so as to ensure that they always comply with laws and regulations.

FAHP-based privacy risk weighting for financial services

In the process of financial services transactions, it is obvious that users' private information is frequently accessed. The process is shown in Fig. 1 below.

As can be seen from the figure above, user information can be at risk of privacy disclosure at all points in the transaction process, such as the three main bodies: apps, platforms, and financial services providers. In addition, there are risks in the transmission of data, as well as malicious external attacks on financial institutions. Therefore, this paper classifies privacy risks of financial services into five risk categories as follows.

(1) Platform risk β_1 is the risk arising within financial platforms.
(2) Technology risk β_2 is the risk from software or applications.
(3) External Attack Risk β_3 is the risk of malicious attacks from outside the financial platform.
(4) Services Provider Risk β_4 is the risk resulting from the services provider.
(5) Data transmission risk β_5 is the risk of data during transmission.

FAHP-based privacy risk attribute model for financial services

FAHP is a decision-making method that optimizes traditional analytic hierarchy process through fuzzy logic, effectively handling subjective ambiguity in evaluations. This study adopts this method to determine the weights

Reference source	Perspective	Method	Gaps
Huo et al.[9]	User financial privacy protection	Privacy protection model based on cloud computing	It relies on linear operation model, and its use scenario is limited
Dhiman et al.[10]	User financial privacy protection	Federated learning method based on homomorphic encryption	The cost is high and there is no way to prevent other aspects of privacy leakage
Xu et al.[11]	User financial privacy protection	Blockchain model for privacy protection of financial services based on image	The storage overhead is large, and the risk is difficult to prevent when the enterprise does not use blockchain
Qiu et al.[12]	User financial privacy protection	Privacy protection intelligent storage (PS2) model	The data recovery process is complex and does not prevent other aspects of privacy leakage
Zhong et al.[13]	Financial services risk warning	Cloud data storage security and financial risk control management early warning system based on sensor network	Real-time requirements are high and deployment costs are high
Luo et al.[14]	Risk assessment of financial services	Systematic financial risk assessment based on fuzzy clustering analysis of risk data	Can identify risks, but lack of quantification of risks
Alqahtani and Moorsel[15]	Risk assessment of financial services	Risk assessment method for EMV transaction system	Limited to the field of payment transactions, it is difficult to prevent other risks
Zhang et al.[16]	Risk assessment of financial services	Use big data indicators to build risk assessment model	The quality of public opinion data is uneven and the objectivity is insufficient
Shi et al.[17], Zhang et al.[18] and Yang et al.[19]	Risk assessment of financial services	Use information entropy method to estimate privacy risks	The scalability is low, and the index needs to be recalculated when it changes
Ali-Eldin et al.[20]	Risk assessment of financial services	Privacy risk assessment model	The accumulation of open data requires high requirements

Table 1. Summary of privacy security methods for financial services.

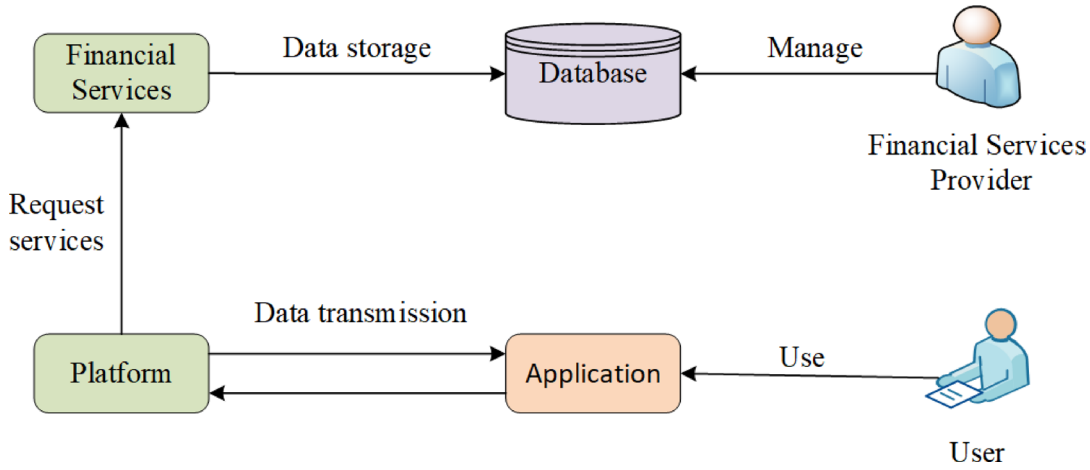


Fig. 1. Financial business transaction process.

Indicators	Significance	Example
I_1	Risk of privacy leakage due to malicious behavior of internal employees	Selling User Information
I_2	Security vulnerabilities in software or applications	Vulnerabilities in apps allow hackers to steal users' personal information
I_3	Abusive collection of permissions by third-party applications	User preferences collection
I_4	Data leakage due to internal system or platform errors	An error in the platform caused the services to shut down
I_5	Data Store or Server Authentication Vulnerability	Unauthorized users are able to access sensitive data
I_6	Insecure network connections during data transmission	Insecure WiFi connection, vulnerable to hacker interception to steal data
I_7	Privacy disclosure due to services providers data loss	Loss of storage device by the services provider
I_8	Vulnerabilities in operating systems or end devices	Malware exploits operating system vulnerabilities, leading to the theft of users' personal information
I_9	User rights not properly configured or managed by internal personnel	Incorrect authorization
I_{10}	Third-party application vulnerabilities posing a risk to user privacy	Third-party applications hacked
I_{11}	Risk of privacy leakage due to vulnerabilities in encryption mechanisms	Insecure encryption algorithms
I_{12}	Risk of privacy leakage resulting from inadequate key management	Information leakage due to lost keys or simple password settings

Table 2. Meaning of the 12 financial risk indicators.

of risk indicators, aiming to accurately quantify the relative importance of multi-dimensional indicators, reduce subjectivity in expert assessments, and provide a reliable basis for comprehensive assessment.

To construct the risk indicator system, this paper has collected and sorted out about 200,000 words of source data through forms such as literature review, report tracking, case analysis, and interview investigation. According to the Grounded theory[26], 3/4 of the data were used for data processing, and the remaining 1/4 was used to verify indicator integrity. 3/4 of the original data was first combed (First, the NVivo 15 tool was used to conduct unitization processing on the original text and decompose it into independent and complete semantic fragments; Subsequently, open coding was carried out. The initial concepts are extracted and similar terms are merged through sentence-by-sentence annotation) to get 265 initial concepts, and then refined again (First, axial coding was conducted to reclassify the scopes formed in the previous stage and to summarize them into higher-level scopes. Subsequently, selective coding was carried out to identify the core scope.) to get 12 indicators, as shown in Table 2 below.

Finally, in order to verify whether the indicators extracted in this paper are complete, the remaining 1/4 of the information was summarized in this paper. No new concepts or categories were found, indicating that the evaluation indicators constructed in this paper are complete.

To use FAHP method for assessment, it is necessary to first identify the target, scheme and indicator layer, and construct a hierarchical model based on them[27]. After sorting out the risk indicators in Table 2, taking into account the actual operation scenario, the relevant credible risk factors and each risk category are inseparable from each other, even if they are less related, they cannot be analyzed completely independently. Therefore, in order to maintain the objectivity of the assessment, this paper develops a cross-attribute model of privacy risks in financial services. The privacy risk model established is shown in Fig. 2 below.

The model has three layers, the first is the Target layer, which focuses on the evaluation of privacy risks in financial services; the second is the Scheme layer, which includes risk categories $\beta_1 \sim \beta_5$; The third layer is the Indicator layer, which contains risk indicators $I_1 \sim I_{12}$. After building the model, the corresponding weights can then be calculated, including weights for individual indicators, risk categories and overall service risk, thus helping the user to better select the target.

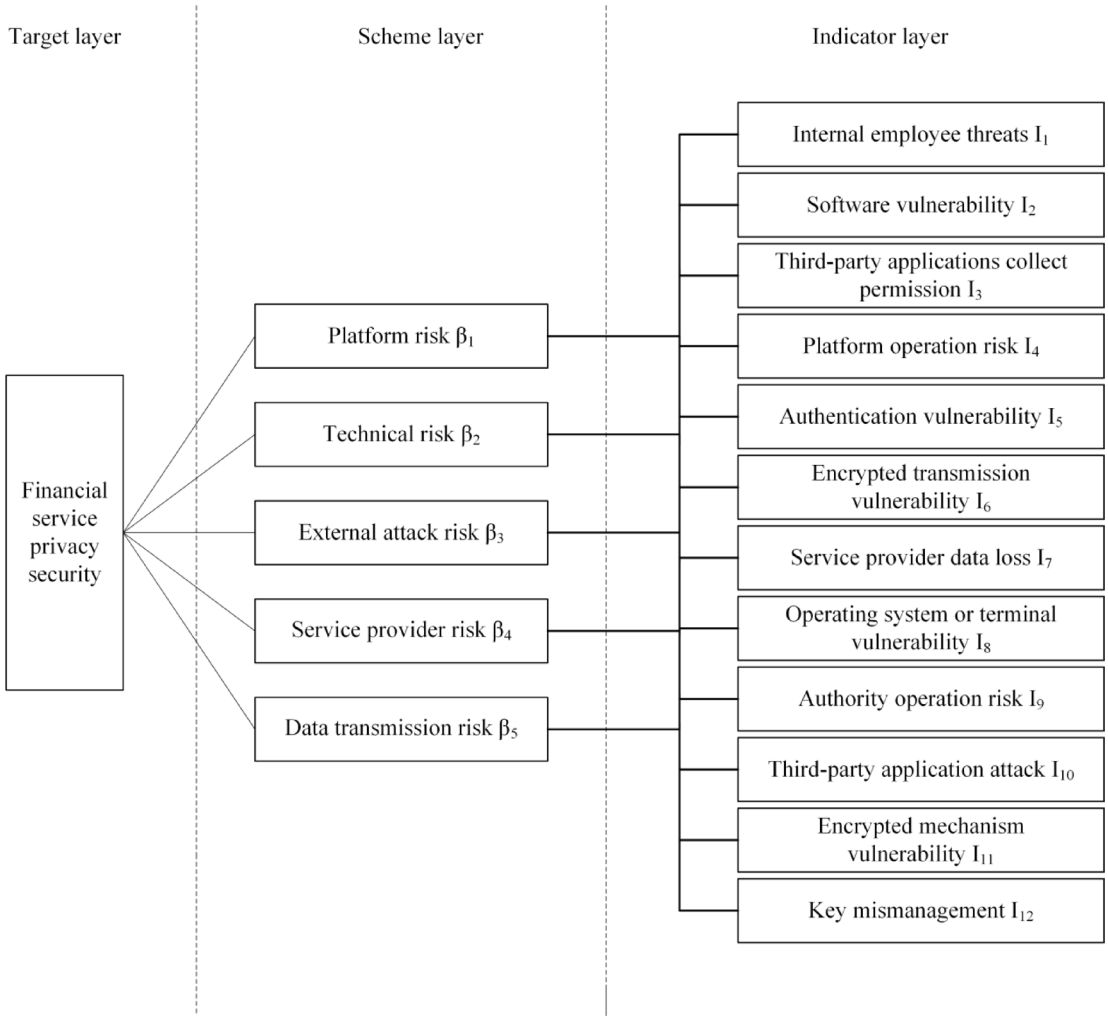


Fig. 2. Cross-attribute model of privacy risks in financial services.

Fuzzy consistency matrix-based risk weight assessment

The assessment of risk category risk indicator weights using the AHP method requires a pairwise comparison of the elements in each layer of the model in (Fig. 2). If there are M factors need to be assessed, comparing these factors pairwise would require a total of M(M-1)/2 judgments. When M is large, this will result in the experts to make more comparisons, potentially triggering inconsistencies in the judgment matrix that have been created. Additionally, if the judgment matrix is not consistent, experts must continuously adjust their evaluations to meet the matrix consistency.

To simplify the process of evaluating the AHP method, this paper employs a fuzzy consistency matrix for determining weights. This method not only reduces the influence of human subjective factors like the AHP method, but also effectively addresses inconsistencies[28].

Fuzzy consistency matrix construction process

Based on the concept of a fuzzy consistency matrix[29], the significance ratio $P(I_i, I_j)$ of element I_i and element I_j is shown as follows. This ratio reflects the relative importance of I_i compared to I_j as evaluated by experts.

(1) $0 \le P(I_i, I_j) < 0.5$ indicates I_j is more important than I_i, the smaller the value, the greater the ratio of the importance of I_j and I_i.
(2) $P(I_i, I_j) = 0.5$ indicates I_j and I_i are of equal importance.
(3) $0.5 < P(I_i, I_j) \le 1$ means I_i is more important than I_j, opposite to the meaning of (1).

According to the meaning of $P(I_i, I_j)$, the steps for constructing the fuzzy consistency matrix are as follows.

1. Constructing a judgment matrix between elements

$$(F_{ij})_{n*n} = \begin{pmatrix} P(I_i, I_1) & \cdots & P(I_i, I_n) \\ \vdots & \ddots & \vdots \\ P(I_n, I_1) & \cdots & P(I_n, I_n) \end{pmatrix}$$

2. The established fuzzy matrix $(F_{ij})_{n*n}$ will be converted into fuzzy consistency matrix using the follow formula.

$$\underline{P}(I_i, I_j) = \frac{\sum_{l=1}^{n} P(I_i, I_l)}{\sum_{l=1}^{n} (P(I_i, I_l) + P(I_j, I_l))} \tag{1}$$

3. $\underline{P}(I_i, I_j)$ is the weight ratio of the two elements. therefore, a fuzzy consistency matrix can be constructed, and this matrix $\left(\underline{F}_{ij}\right)_{n*n}$ has full consistency.

$$\left(\underline{F}_{ij}\right)_{n*n} = \begin{pmatrix} \underline{P}(I_i, I_1) & \cdots & \underline{P}(I_i, I_n) \\ \vdots & \ddots & \vdots \\ \underline{P}(I_n, I_1) & \cdots & \underline{P}(I_n, I_n) \end{pmatrix} \tag{2}$$

After constructing the matrix $\left(\underline{F}_{ij}\right)_{n*n}$, it is possible to calculate the weights of each element use the follow formula.

$$W_i = \frac{2\sum_{j=1}^{n} \underline{P}(I_i, I_j) - 1}{n(n-1)}, i = 1, 2, \ldots, n \tag{3}$$

W_i represents the weight of element i in the model. Based on the principle of pairwise comparison in FAHP[30], W_i has a certain degree of objectivity. A larger value of W_i indicates a greater influence of element i on the target evaluation in the model.

Assessment of privacy risk weight in financial services
According to the method in the previous section, and in conjunction with the model in Fig. 2, it is possible to construct the fuzzy consistency matrix from the bottom up.

(1) The weight calculation of the scheme layer relative to the target layer. By constructing a fuzzy consistency matrix, it is possible to calculate the weights $W\left(\beta_j\right)$ of risk categories within the entire privacy risk assessment. The larger the value of $W\left(\beta_j\right)$, the risk category β_j has a greater impact on the overall privacy risks of financial services.
(2) The weight calculation of the indicator layer relative to the scheme layer. As above, by constructing five fuzzy consistency matrices, it is possible to calculate the weights $W(I_i, \beta_j)$ of the 12 indicators in the indicator layer with respect to each risk category. The larger the value of $W(I_i, \beta_j)$, the indicator I_i has the greater impact on the risk category β_j.

After determining the assessment weights through the method mentioned above, this paper will next concentrate on the evaluation of risk levels in financial services.

Assessment of risk levels in financial services

FAHP-based risk weight evaluation only can evaluate the significant of elements. In order to offer more comprehensive information of financial services, a further assessment of the risk levels is necessary. Here, "risk levels" refers to the quantified classification of risk for each indicator in the assessment system, which is determined based on the actual situation of indicators and expert evaluations to reflect the degree of potential privacy risks in terms of occurrence frequency or loss severity.

Risk classification

In order to make the risk assessment process more concise and more distinguishable, this paper initially define four risk levels from two aspects: risk frequency and risk loss, as illustrated in the following Table.

Fuzzy and D-S theory based risk level assessment

While Table 3 divides the risks into four levels according to their frequency and degree of loss, it is not easy to precisely define the level of risk in reality. Meanwhile, experts' determination of risk levels may vary from person to person. To overcome this challenge, this paper applies fuzzy theory[31] to reclassify risk levels and uses D-S theory to integrate multiple expert opinions to improve the assessment results.

D-S evidence theory, as an artificial intelligence technique, was originally applied to the field of expert systems with the ability to deal with uncertain information[32]. The theory can effectively address the problem of conflicting results of multi-expert assessment and provide reasonable fusion results by calculation. In information fusion, a confidence level needs to be assigned to each expert's assessment results, and then fuse the results using appropriate formulas. In this paper, the risk levels of financial services are assessed as follows.

Risk frequency level	Significance
1	Risks are virtually non-existent
2	Risks are occasional
3	Risks are common and frequent
4	Risks are nearly unavoidable
Risk loss level	significance
1	Risks rarely threaten users' privacy
2	Risks may lead to the exposure of sensitive user information, including but not limited to personal interests, hobbies, and real-time location data
3	Risks can lead to the exposure of users' critical data, such as identification details, contact logs, and health status, among other private information
4	Risks will result in the exposure of critical private information of users, such as financial information

Table 3. Privacy risk classification.

Arbitrary set S	t_1 (S_1)	t_2 (S_2)	t_3 (S_3)
1	0	0	0
1–2	0.2	0.3	0.3
2	0.3	0.2	0.3
2–3	0.2	0.1	0.2
3	0.3	0.3	0.2
3–4	0	0.1	0
4	0	0	0

Table 4. Results of the expert assessment of risk levels.

This paper uses confidence level t(S) for describing the risk level, which indicates the probability of belonging to the set S, $0 \le t(S) \le 1$. S is a set containing all possible risk levels, including {1},{1,2},{2},{2,3},{3},{3,4},{4},and $\sum_{S \neq \varnothing} t(S) = 1$. This is illustrated in Table 4 below.

Table 4 shows an example of the results of the assessment by three experts, each of whom gave a different level of confidence. The next step is to fuse the assessment results of the three experts using the following formula.

$$\begin{aligned} t(S) &= (t_1 \oplus t_2 \oplus \cdots \oplus t_n)(S) \\ &= \frac{1}{k} \sum_{S_1 \cap S_2 \cap \ldots \cap S_n = S} t_1(S_1)\, t_2(S_2) \cdots t_n(S_n) \end{aligned} \tag{4}$$

Among them, k is a normalization factor, which can be calculated by the following two formulas.

$$k = 1 - \sum_{S_1 \cap S_2 \cap \ldots \cap S_n = \varnothing} t_1(S_1)\, t_2(S_2) \cdot \cdot \cdot t_n(S_n) \tag{5}$$

$$k = \sum_{S_1 \cap S_2 \cap \ldots \cap S_n \neq \varnothing} t_1(S_1)\, t_2(S_2) \cdot \cdot \cdot t_n(S_n) \tag{6}$$

Integrating expert evaluations requires dealing with various sets, making the computation quite complex. Therefore, this paper employs the Bayesian approximation method[33] to simplify set S. The specific methods are described as follows.

$$t(\underline{S}) = \frac{\sum_{\underline{S} \subseteq S} t(S)}{\sum_{A \subseteq \theta} t(S) * N} \tag{7}$$

In the above formula, the S is the reduced set of the S, which includes only {1},{2},{3},{4}. θ is the full set, and N is the number of levels included in the set S. Therefore, the evaluation results of the three experts can be calculated using the above formula with the following process.

$$t(\underline{1}) = \frac{t(1) + t(1,2)}{t(1) + t(1,2) * 2 + t(2) + t(2,3) * 2 + t(3) + t(3,4) * 2 + t(4)}$$

$$t(\underline{2}) = \frac{t(1,2) + t(2) + t(2,3)}{t(1) + t(1,2) * 2 + t(2) + t(2,3) * 2 + t(3) + t(3,4) * 2 + t(4)}$$

$$t(\underline{3}) = \frac{t(2,3) + t(3) + t(3,4)}{t(1) + t(1,2) * 2 + t(2) + t(2,3) * 2 + t(3) + t(3,4) * 2 + t(4)}$$

Arbitrary set S	t_1 (S_1)	t_2 (S_2)	t_3 (S_3)
1	0.1429	0.2000	0.2000
2	0.5000	0.4000	0.5333
3	0.3571	0.3333	0.2667
4	0.0000	0.0667	0.0000

Table 5. The calculated results of the expert assessment.

Arbitrary set S	t(S)
1	0.0396
2	0.7401
3	0.2203
4	0.0000

Table 6. The confidence level after fusion.

$$t(\underline{4}) = \frac{t(3,4) + t(4)}{t(1) + t(1,2) * 2 + t(2) + t(2,3) * 2 + t(3) + t(3,4) * 2 + t(4)} \tag{8}$$

The set S is calculated in Table 5 below.

After obtaining the data in the table above, the value of k is then calculated using formula (6), and finally put them into formula (4) to obtain the fused confidence level t(S), and the fused results in Table 6 below.

From Table 6, it can be seen that t(2) > t(3) > t(1) > t(4), which means that the risk level for this element is most likely to be level 2.By querying Table 3, it can be seen that the risk may occur occasionally, and the probability of belonging to level 4 is very low. Similarly, the confidence level of other elements can be calculated according to this method.

Comprehensive privacy security assessment for financial services

Comprehensive evaluation process

In Sect. 3, we introduce a FAHP-based risk weight evaluation method. Section 4 introduces a risk level evaluation method that combines fuzzy theory with D-S theory. These two methods together provide a comprehensive assessment of privacy risks in financial services. The detailed implementation process is shown in Fig. 3 below.

According to Fig. 3 and previous studies, the indicators' risk fuzzy level $f(I_i)$ and $l(I_i)$ obtained based on D-S theory can realize the effective assessment of the indicator layer, and combined with the indicator risk weights $W(I_i, \beta_j)$obtained based on the FAHP method can evaluate the risk category of the scheme layer, and finally realize the bottom-up assessment of financial services.

Assessment of the indicator layer

Firstly, we need to calculate the risk levels for each indicator I_i at the indicator layer, and the calculation formula is as follows.

$$Lv(I_i) = f(I_i) * l(I_i) \tag{9}$$

In the above formula, the $f(I_i)$ and $l(I_i)$ respectively denote the fuzzy level of risk frequency and risk loss of the indicator I_i . By multiplying $f(I_i)$ and $l(I_i)$, and combined with the risk matrix method[34], the comprehensive risk level $Lv(I_i)$ can be calculated in Table 7 below. Integrating risk frequency and loss severity through the risk matrix method makes the classification of risk levels more intuitive and objective.

In the above Table, the risk levels of financial services are divided into 4 levels. Level I means the element has high security and very low privacy risk; Level II indicates the element is relatively safe, but has a slight privacy risk that could reveal basic information such as the user's location and interests; Level III denotes the element has more serious privacy security issues, with the risk of leaking sensitive data such as the user's identity, health status, and so on; and Level IV indicates that the element has the most serious security risks, which may leak the critical information such as the user's financial and monetary information.

Assessment of the scheme layer

Based on the D-S theory, after calculating the $f(I_i)$ and $l(I_i)$ for the privacy risk attribute model indicator layer risk indicators in Fig. 2, the risk indicator weights $W(I_i, \beta_j)$calculated by FAHP method, $Lv(\beta_j)$ can be calculated using the following formula.

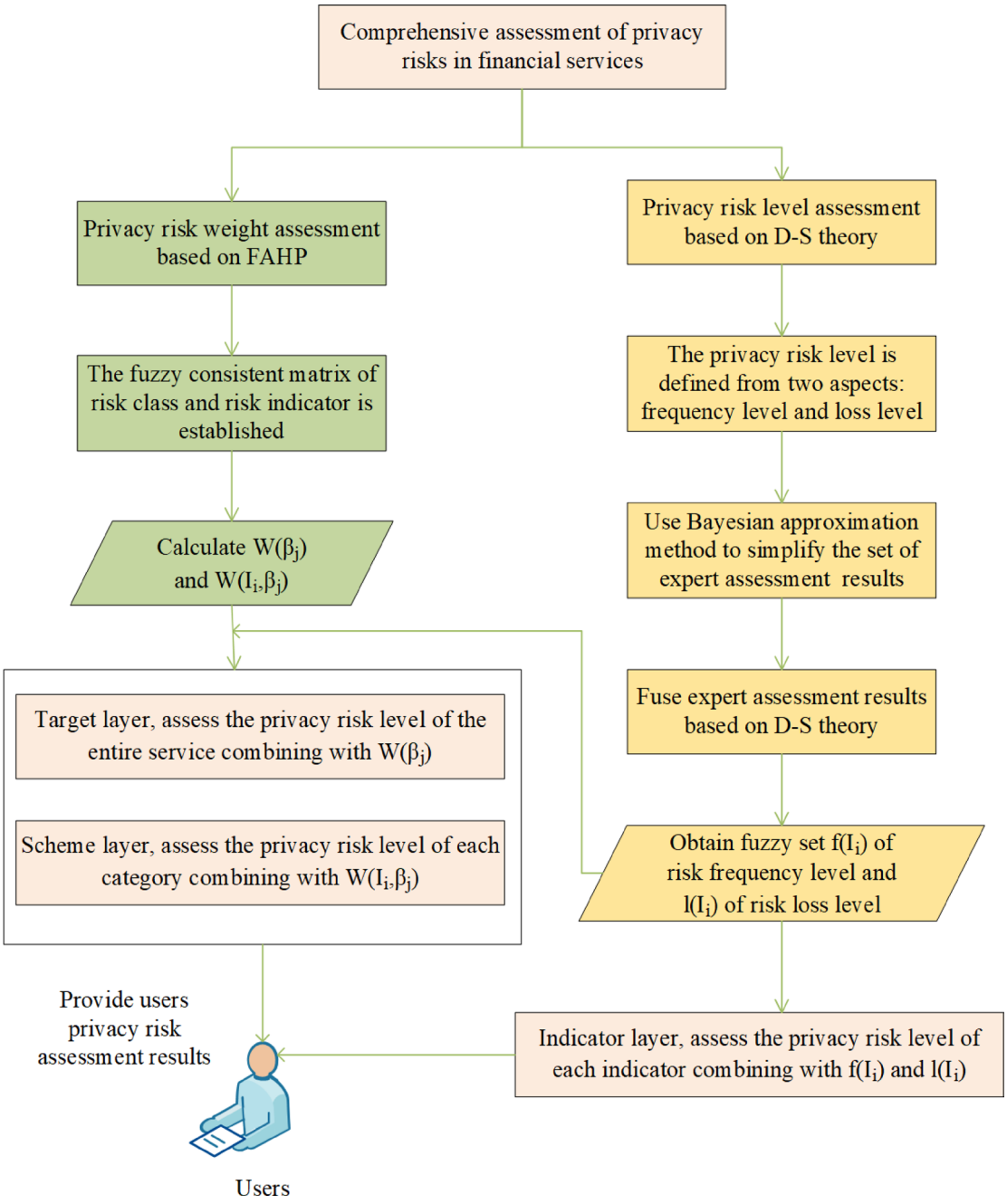


Fig. 3. Comprehensive assessment process of privacy risks in financial services.

Frequency / Loss	1	2	3	4
1	1/I	2/I	3/I	4/II
2	2/I	4/I	6/II	8/III
3	3/I	6/II	9/III	12/IV
4	4/II	8/III	12/IV	16/IV

Table 7. Comprehensive level of privacy risks based on the risk matrix Method.

$$Lv(\beta_j) = f(\beta_j) * l(\beta_j) = \left\{\sum_{i=1}^{12} f(I_i) * W(I_i, \beta_j)\right\} * \left\{\sum_{i=1}^{12} l(I_i) * W(I_i, \beta_j)\right\} \quad (10)$$

Assessment of the target layer

First, calculate the risk category frequency level $f(\beta_j)$ and risk category loss level $l(\beta_j)$ by the D-S theory, and then the risk category weight $W(\beta_j)$ calculated by the FAHP method, the risk level Lv for financial services can be obtained by the following formula.

$$Lv = \left\{\sum {}_{j=1}^{5} f(\beta_j) * W(\beta_j)\right\} * \left\{\sum {}_{j=1}^{5} l(\beta_j) * W(\beta_j)\right\} \quad (11)$$

Result representation using triangular fuzzy value

To characterize the level of privacy risks in financial services more objectively, this paper combines the fuzzy theory and proposes to use a triangular fuzzy value[35] to represent the level of a credible risk indicator to redescribe the level of privacy risk, as illustrated in (Fig. 4).

in the above figure, the horizontal axis represents the level of risk Lv and the vertical axis represents the level of confidence level t(S) of the risk. The triangle consists of three points, which are:

(1) Lv^{min} means the minimum level of the risk, which is necessary for t(S) > 0 .
(2) Lv^{max} means the maximum level of the risk, which is necessary for t(S) > 0 .
(3) Lv^{mid} represents the highest confidence level of the risk, that is, the risk has the highest probability of belonging to the Lv^{mid} level.

As mentioned in the previous section, according to the fuzzy theory change formulas (9)–(11), we can obtain the following formulas (12)–(14).

$$\begin{aligned} Lv^{min} &= f^{min}(I_i) * l^{min}(I_i) \\ Lv^{max} &= f^{max}(I_i) * l^{max}(I_i) \\ Lv^{mid} &= f^{mid}(I_i) * l^{mid}(I_i) \end{aligned} \quad (12)$$

In the above formula, $f^{min}(I_i)$ represents the lower limit level of the risk frequency of the indicator I_i, $l^{min}(I_i)$ represents the lower limit level of the risk loss. $f^{max}(I_i)$ means the upper limit level of the risk frequency of the indicator I_i, $l^{max}(I_i)$ means the upper limit level of the risk loss. $f^{mid}(I_i)$ Indicates the indicator I_i's risk frequency level maximum confidence level. $l^{mid}(I_i)$ Indicates the indicator I_i's risk loss level maximum confidence level.

$$Lv^{min}(\beta_j) = f^{min}(\beta_j) * l^{min}(\beta_j)$$

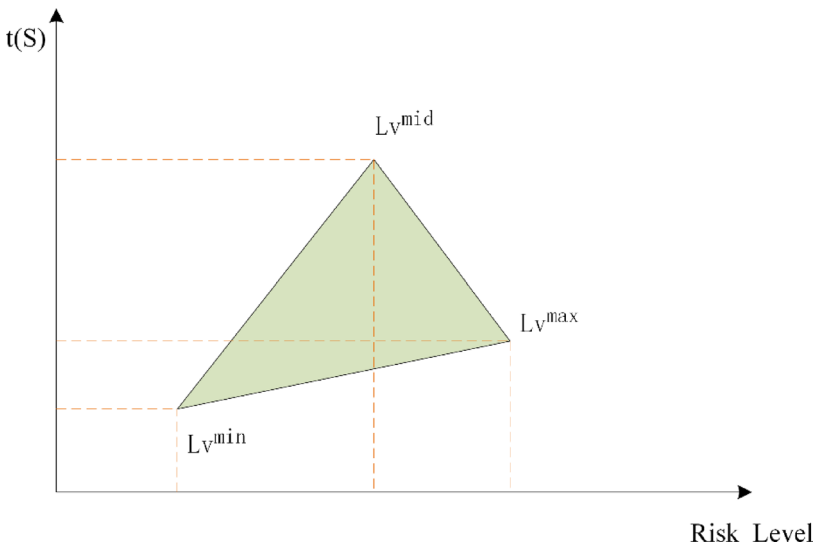


Fig. 4. Description of risk level using triangular fuzzy value.

$$= \left\{ \sum {}_{i=1}^{12} f^{min}\left(I_i\right) * W\left(I_i, \beta_j\right) \right\} * \left\{ \sum {}_{i=1}^{12} l^{min}\left(I_i\right) * W\left(I_i, \beta_j\right) \right\}$$

$$Lv^{max}\left(\beta_j\right) = f^{max}\left(\beta_j\right) * l^{max}\left(\beta_j\right)$$

$$= \left\{ \sum_{i=1}^{12} f^{max}\left(I_i\right) * W\left(I_i, \beta_j\right) \right\} * \left\{ \sum_{i=1}^{12} l^{max}\left(I_i\right) * W\left(I_i, \beta_j\right) \right\} \tag{13}$$

$$Lv^{mid}\left(\beta_j\right) = f^{mid}\left(\beta_j\right) * l^{mid}\left(\beta_j\right)$$

$$= \left\{ \sum {}_{i=1}^{12} f^{mid}\left(I_i\right) * W\left(I_i, \beta_j\right) \right\} * \left\{ \sum {}_{i=1}^{12} l^{mid}\left(I_i\right) * W\left(I_i, \beta_j\right) \right\}$$

Same as the above, the $f^{min}\left(\beta_j\right)$ and $l^{min}\left(\beta_j\right)$ represent the lower limit level of risk frequency and loss of the risk category β_j. $f^{max}\left(\beta_j\right)$ and $l^{max}\left(\beta_j\right)$ represent the upper limit level of risk frequency and loss of the risk category β_j, $f^{mid}\left(\beta_j\right)$ and $l^{mid}\left(\beta_j\right)$ represent the risk category β_j's maximum confidence level of risk frequency and loss.

$$Lv^{min} = \left\{ \sum {}_{j=1}^{5} f^{min}\left(\beta_j\right) {*} W\left(\beta_j\right) \right\} * \left\{ \sum {}_{j=1}^{5} l^{min}\left(\beta_j\right) {*} W\left(\beta_j\right) \right\}$$

$$Lv^{max} = \left\{ \sum {}_{j=1}^{5} f^{max}\left(\beta_j\right) {*} W\left(\beta_j\right) \right\} * \left\{ \sum {}_{j=1}^{5} l^{max}\left(\beta_j\right) {*} W\left(\beta_j\right) \right\} \tag{14}$$

$$Lv^{mid} = \left\{ \sum {}_{j=1}^{5} f^{mid}\left(\beta_j\right) {*} W\left(\beta_j\right) \right\} * \left\{ \sum {}_{j=1}^{5} l^{mid}\left(\beta_j\right) {*} W\left(\beta_j\right) \right\}$$

The use of triangular fuzzy value in assessing risk level allows for a more realistic capture of risk uncertainties, providing a more comprehensive and accurate risk assessment.

Case study

To validate the effectiveness of the above assessment method, two financial services providers are evaluated in this paper. The first is a financial services provider specializing in financial investment and securities trading, whose services cover convenient digital payment and comprehensive mobile banking functions. The second provider, specializing in credit services, is committed to providing users with high-quality financial investment and wealth management services. Through a preliminary survey, this paper concludes the features of these two financial institutions, details of which can be found in (Table 8). This assessment aims to validate the applicability and effectiveness of the proposed method in real-world financial services scenarios.

Risk indicators	Company 1	Company 2
I_1: Malicious Internal Employee Behavior	Lower level of disciplinary infractions exist	Internal employees have a high disciplinary record
I_2: Software or application vulnerability	Has no obvious technical vulnerabilities and can pass security tests	Has no obvious technical vulnerabilities and can pass security tests
I_3: Abusive collection of permissions by third-party applications	There are few financial product ads is abusive collection of information	There are more investment trading ads that collect more users' information
I_4: Data leakage due to internal system or platform error	Internal systems and platforms are stable and pose little threat to users' privacy in the event of a service failure.	Systems and platforms have been in operation for many years and service failures can pose a significant threat to users' privacy
I_5: Data Store or Server Authentication Vulnerability	Strict access control such as real-name authentication	Can be logged in through third-party applications, some vulnerabilities exist
I_6: Connection to unsecured network during data transfer	Secure network connections are used, Sensitive information such as users contact details will not be exposed	Sometimes a secure network connection is not used, which may expose information such as users contact details
I_7: Services provider data loss	Take multiple security measures to prevent data loss	The security measures implemented are not sufficient to avoid users' data loss
I_8: Operating system or terminal device vulnerabilities	No obvious vulnerabilities in terminals	No obvious vulnerabilities in terminals
I_9: User rights not properly configured or managed by internal personnel	The rights are properly configured. Internal employees can access only basic users' information	The permission configuration is improper, and some employees can access a large number of users information
I_{10}: Third party applications hacked	Not being associated with or authorized to cooperate with third-party applications, it is relatively secure	Have risks associated with information and authorized cooperation with third-party applications
I_{11}: Vulnerability of encryption mechanism	A strong encryption mechanism is used to protect users' information from vulnerability threats	The encryption mechanism used is not strong, and users' information may be threatened
I_{12}: Improper key management during use	Regular rotation and stringent control measures are implemented for the key	There is no regular rotation and strict control for the key

Table 8. Risk features of the two financial institutions.

Risk weight assessment

The weights of the indicators and risk categories were calculated according to the method in Sect. 3 and are shown in Table 9 below.

Risk level assessment

After assessing the weights, the next step is to assess the risk levels of financial services, based on the method covered in Sect. 4.2 of this paper. We invited 15 experts from diverse backgrounds to assess risk indicators, including academic experts in the fields of financial risk, management and cloud service security, as well as practitioners from actual financial institutions. Tables 10 and 11 show their assessment results of Company 2 and Company 1.

After obtaining the above assessment data, the risk level assessment method in Sect. 4 is used to simplify the data in Tables 10 and 11 using Bayesian approximation, and then the approximated data are fused using D-S theory, and the outcomes of this fusion are presented in Tables 12 and 13 below.

Comparison of assessment results by layer

After obtaining the results from Tables 12 and 13, the results of privacy risk assessment of the financial services of Company 2 can be calculated by substituting them into formulas (12)-(14), and the same can be done to assess the financial services of Company 1. Finally, the risk of the financial services of the two companies is compared bottom-up.

(1) Comparison of risk levels of the indicator layer. The indicators' fuzzy risk levels in the indicator layer can be expressed as $Lv\left(I_i\right) = \{Lv^{min}\left(I_i\right), Lv^{mid}\left(I_i\right), Lv^{max}\left(I_i\right)\}$, and the results of the calculations based on the data in Tables 12 and 13 are shown in (Table 14,15 and Figs. 5, 6) below.

According to the hierarchical definitions in Table 7, some of the indicators for company 2 in Fig. 5, $Lv^{mid}\left(I_1\right)$ =9. $Lv^{mid}\left(I_{12}\right)$ = 9, which belong to the III risk level. It indicates that Company 2's indicator I_1 and indicator I_{12} have a large privacy security problem, may leak important information such as user's identification details, contact logs, and health status and other important information when using the company's services. It also poses a serious threat to the privacy security of the financial services of Company 2, and both the company and the users need to focus on this issue. Especially the indicator I_1 "Malicious behavior of internal employees", its risk level $Lv^{max}\left(I_i\right)$ =16, which belongs to the IV risk level, the highest of all indicators, may disclose critical user information and requires special attention. In addition to this, the other risk indicators for Company 2 $Lv^{mid}\left(I_i\right) \leq 6$, belongs to the I or II risk level, indicating that these indicators are relatively safe and have a low probability of privacy security issues, with $Lv^{mid}\left(I_8\right) = 2$, indicates that the company has a high level of security in its operating system or end devices.

In Fig. 6, Company 1's risk indicator level $Lv^{mid}\left(I_i\right) \leq 6$, belongs to risk level I or II, representing that the company's risk indicators are all relatively safe and do not pose much of a threat to the user's privacy risk. There are only two indicators $Lv^{max}\left(I_3\right) = 12$ and $Lv^{max}\left(I_{12}\right) = 12$,this means that the company's risk indicators for "third-party apps collecting information" and "secret key management" are still likely to result in a serious threat to users' privacy, users need to pay attention to this point. The company's risk indicators $Lv^{mid}\left(I_4, I_7, I_8\right) = 3$, which fall into risk level I, represents that the company's platforms and operating systems, as well as services providers, are highly secure.

(2) Comparison of risk levels in scheme layer. Also, according to Tables 9, 12 and 13 and formula (13), The risk categories' fuzzy risk levels in the scheme layer can be calculated as the following Figs. 7, 8 below.

From the above two graphs, it can be seen that the two companies are in risk categories $4< Lv^{mid}\left(\beta_j\right) < 6$, which belongs to the II risk level, indicating that the two companies' risk categories are probable to be in a relatively safe situation. However, Company 1 has a risk category $6< Lv^{max}\left(\beta_j\right) < 8$, which belongs to the III

	β_1	β_2	β_3	β_4	β_5
$W(\beta_j)$	0.228	0.204	0.185	0.206	0.177
	$W(I_i,\beta_1)$	$W(I_i,\beta_2)$	$W(I_i,\beta_3)$	$W(I_i,\beta_4)$	$W(I_i,\beta_5)$
I_1	0.098	0.081	0.075	0.089	0.086
I_2	0.087	0.095	0.088	0.082	0.080
I_3	0.083	0.081	0.092	0.082	0.078
I_4	0.093	0.087	0.082	0.087	0.085
I_5	0.082	0.094	0.087	0.083	0.081
I_6	0.073	0.071	0.097	0.069	0.080
I_7	0.089	0.086	0.080	0.098	0.081
I_8	0.083	0.093	0.087	0.084	0.081
I_9	0.093	0.075	0.075	0.083	0.076
I_{10}	0.072	0.078	0.082	0.092	0.086
I_{11}	0.075	0.088	0.088	0.082	0.096
I_{12}	0.071	0.072	0.068	0.069	0.091

Table 9. Weights of risk indicators and risk categories.

	I_1			I_2			I_3		
S	$t_1(S_1)$	$t_2(S_2)$	$t_3(S_3)$	$t_1(S_1)$	$t_2(S_2)$	$t_3(S_3)$	$t_1(S_1)$	$t_2(S_2)$	$t_3(S_3)$
1	0	0	0	0.2	0.1	0.2	0	0	0
1–2	0.2	0.2	0.1	0.6	0.5	0.7	0	0	0
2	0.2	0.2	0.3	0.1	0.3	0.1	0.1	0	0.1
2–3	0.2	0.1	0.2	0.1	0.1	0	0.1	0.1	0.1
3	0.3	0.3	0.2	0	0	0	0.1	0.2	0.3
3–4	0.1	0.2	0.2	0	0	0	0.4	0.5	0.3
4	0	0	0	0	0	0	0.3	0.2	0.2
	I_4			I_5			I_6		
S	$t_1(S_1)$	$t_2(S_2)$	$t_3(S_3)$	$t_1(S_1)$	$t_2(S_2)$	$t_3(S_3)$	$t_1(S_1)$	$t_2(S_2)$	$t_3(S_3)$
1	0.7	0.8	0.6	0.2	0.1	0	0.1	0	0
1–2	0.2	0.1	0.2	0.2	0.1	0.1	0.2	0.1	0.1
2	0.1	0.1	0.2	0.3	0.2	0.1	0.5	0.6	0.6
2–3	0	0	0	0.3	0	0.5	0.2	0.3	0.3
3	0	0	0	0	0.4	0.2	0	0	0
3–4	0	0	0	0	0.2	0.1	0	0	0
4	0	0	0	0	0	0	0	0	0
	I_7			I_8			I_9		
S	$t_1(S_1)$	$t_2(S_2)$	$t_3(S_3)$	$t_1(S_1)$	$t_2(S_2)$	$t_3(S_3)$	$t_1(S_1)$	$t_2(S_2)$	$t_3(S_3)$
1	0.2	0.3	0.3	0.6	0.5	0.5	0	0	0
1–2	0.5	0.6	0.5	0.2	0.2	0.2	0.1	0	0.1
2	0.2	0.1	0.1	0.2	0.1	0.2	0.4	0.2	0.4
2–3	0.1	0	0.1	0	0.1	0.1	0.1	0.3	0.1
3	0	0	0	0	0.1	0	0.3	0.4	0.3
3–4	0	0	0	0	0	0	0.1	0.1	0.1
4	0	0	0	0	0	0	0	0	0
	I_{10}			I_{11}			I_{12}		
S	$t_1(S_1)$	$t_2(S_2)$	$t_3(S_3)$	$t_1(S_1)$	$t_2(S_2)$	$t_3(S_3)$	$t_1(S_1)$	$t_2(S_2)$	$t_3(S_3)$
1	0.3	0.3	0.1	0	0	0	0	0	0
1–2	0.3	0.1	0.3	0.2	0.1	0.2	0	0.1	0
2	0.3	0.5	0.6	0.3	0.3	0.2	0.2	0.2	0.1
2–3	0.1	0.1	0	0.1	0.2	0.2	0.2	0.2	0.3
3	0	0	0	0.3	0.3	0.2	0.4	0.5	0.4
3–4	0	0	0	0.1	0.1	0.2	0.2	0	0.2
4	0	0	0	0	0	0	0	0	0

Table 10. Risk indicators frequency level assessment results of company 2.

risk level, while all of Company 2's risk categories $Lv^{max}\left(\beta_j\right) > 9$, which belongs to the IV risk level, suggests that Company 1's highest risk class belongs to the III risk level, while Company 2's highest risk class belongs to the IV risk level, which makes Company 1 more privacy safe than Company 2 in comparison.

(3) Comparison of risk level in the target layer. As before, the financial services' fuzzy risk level of two companies can be calculated according to formula (14) as the following Table 16 below.

The above table shows that the risk level range of company 2 is [1.752, 9.159], and the risk level range of company 1 is [1.699, 7.861]. In this case, both the lowest and highest values of the risk range for Company 2 are larger than those for Company 1, which indicates that company 1 is relatively safer than company 2 in terms of financial services as a whole. However, in general, both companies have a risk value of $4 < Lv^{mid} < 6$, which is in the level II, demonstrating that both companies are more secure in their services.

The case study demonstrates that the method accurately identifies high-risk indicators (e.g., Indicators I1 and I12 of Company 2), which are highly consistent with the privacy leakage scenarios described in the introduction—fully validating the feasibility of the method. Additionally, the case study provides users with comprehensive risk assessment information, enabling them to conduct detailed analyses based on their unique needs and thereby make more informed choices of financial services that best align with their privacy protection requirements.

Comparison of methods

The method used in this paper is suitable for assessing privacy security issues in financial services. It provides users with information about the risk weights and levels of the indicators related to financial services, and helps users choose and use financial services rationally, and it is also a kind of security and risk assessment method.

	I_1			I_2			I_3		
S	$t_1(S_1)$	$t_2(S_2)$	$t_3(S_3)$	$t_1(S_1)$	$t_2(S_2)$	$t_3(S_3)$	$t_1(S_1)$	$t_2(S_2)$	$t_3(S_3)$
1	0	0	0	0	0	0	0.1	0.2	0.1
1–2	0	0	0	0	0	0.2	0.3	0.2	0.3
2	0.2	0.1	0	0.2	0.6	0.2	0.3	0.2	0.3
2–3	0	0.1	0.8	0.5	0.3	0.4	0.1	0.2	0.2
3	0.6	0.7	0	0.3	0.1	0.1	0.2	0.2	0.1
3–4	0.2	0.1	0.2	0	0	0.1	0	0	0
4	0	0	0	0	0	0	0	0	0
	I_4			I_5			I_6		
S	$t_1(S_1)$	$t_2(S_2)$	$t_3(S_3)$	$t_1(S_1)$	$t_2(S_2)$	$t_3(S_3)$	$t_1(S_1)$	$t_2(S_2)$	$t_3(S_3)$
1	0	0	0	0	0	0	0.2	0.1	0.1
1–2	0	0	0	0.4	0.2	0.2	0.2	0.1	0.2
2	0	0	0	0.2	0.4	0.3	0.2	0.3	0.3
2–3	0.2	0.2	0.1	0.1	0.1	0.2	0	0	0
3	0.2	0.3	0.4	0.2	0.1	0.2	0.4	0.5	0.4
3–4	0.5	0.3	0.3	0.1	0.2	0.1	0	0	0
4	0.1	0.2	0.2	0	0	0	0	0	0
	I_7			I_8			I_9		
S	$t_1(S_1)$	$t_2(S_2)$	$t_3(S_3)$	$t_1(S_1)$	$t_2(S_2)$	$t_3(S_3)$	$t_1(S_1)$	$t_2(S_2)$	$t_3(S_3)$
1	0	0	0	0.1	0.1	0.2	0.2	0.1	0.1
1–2	0.2	0.2	0.1	0.4	0.4	0.1	0.1	0.2	0.2
2	0.4	0.5	0.6	0.2	0.2	0.5	0.3	0.4	0.2
2–3	0.2	0.1	0.2	0.3	0.2	0.2	0.3	0.1	0.3
3	0.2	0.1	0.1	0	0.1	0	0.1	0.2	0.2
3–4	0	0.1	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0
	I_{10}			I_{11}			I_{12}		
S	$t_1(S_1)$	$t_2(S_2)$	$t_3(S_3)$	$t_1(S_1)$	$t_2(S_2)$	$t_3(S_3)$	$t_1(S_1)$	$t_2(S_2)$	$t_3(S_3)$
1	0	0	0	0.2	0.2	0.1	0	0	0
1–2	0.1	0	0	0.2	0.2	0.3	0	0	0
2	0.4	0.2	0.2	0.3	0.5	0.4	0.3	0.2	0.2
2–3	0.1	0.4	0.3	0.2	0.1	0.2	0.2	0.2	0.3
3	0.4	0.4	0.4	0.1	0	0	0.3	0.3	0.1
3–4	0	0	0.1	0	0	0	0.2	0.3	0.3
4	0	0	0	0	0	0	0	0	0.1

Table 11. Risk indicators loss level assessment results of company 2.

S			t(*S*)			
	I_1	I_2	I_3	I_4	I_5	I_6
1	0.0099	0.4286	0.0000	0.9643	0.0250	0.0033
2	0.4455	0.5714	0.0068	0.0357	0.5250	0.9772
3	0.5347	0.0000	0.5744	0.0000	0.4500	0.0195
4	0.0099	0.0000	0.4188	0.0000	0.0000	0.0000
	I_7	I_8	I_9	I_{10}	I_{11}	I_{12}
1	0.5625	0.8305	0.0000	0.1788	0.0100	0.0000
2	0.4375	0.1695	0.4724	0.8212	0.5373	0.1370
3	0.0000	0.0000	0.5249	0.0000	0.4478	0.8630
4	0.0000	0.0000	0.0026	0.0000	0.0050	0.0000

Table 12. Fused results for company 2's risk indicator frequency level.

S			t(S)			
	I_1	I_2	I_3	I_4	I_5	I_6
1	0.0000	0.0000	0.1468	0.0000	0.0363	0.1304
2	0.0423	0.7241	0.7706	0.0055	0.7778	0.4348
3	0.9524	0.2759	0.0826	0.7890	0.1814	0.4348
4	0.0053	0.0000	0.0000	0.2055	0.0045	0.0000
	I_7	I_8	I_9	I_{10}	I_{11}	I_{12}
1	0.0065	0.1121	0.0628	0.0000	0.1115	0.0000
2	0.9351	0.8610	0.7977	0.3600	0.8780	0.1938
3	0.0584	0.0269	0.1395	0.6400	0.0105	0.7597
4	0.0000	0.0000	0.0000	0.0000	0.0000	0.0465

Table 13. Fused results for company 1's risk indicator frequency level.

	I_1	I_2	I_3	I_4	I_5	I_6	I_7	I_8	I_9	I_{10}	I_{11}	I_{12}
Lv^{min}	1	1	2	1	1	1	1	1	2	1	1	2
Lv^{mid}	3	2	3	1	2	2	1	1	3	2	2	3
Lv^{max}	4	2	4	2	3	3	2	2	4	2	3	3

Table 14. Risk frequency fuzzy level for each indicator of company 2.

	I_1	I_2	I_3	I_4	I_5	I_6	I_7	I_8	I_9	I_{10}	I_{11}	I_{12}
Lv^{min}	2	2	1	2	1	1	1	1	1	2	1	2
Lv^{mid}	3	2	2	3	2	2	2	2	2	3	2	3
Lv^{max}	4	3	3	4	4	3	2	3	3	3	3	4

Table 15. Risk loss fuzzy level for each indicator of company 2.

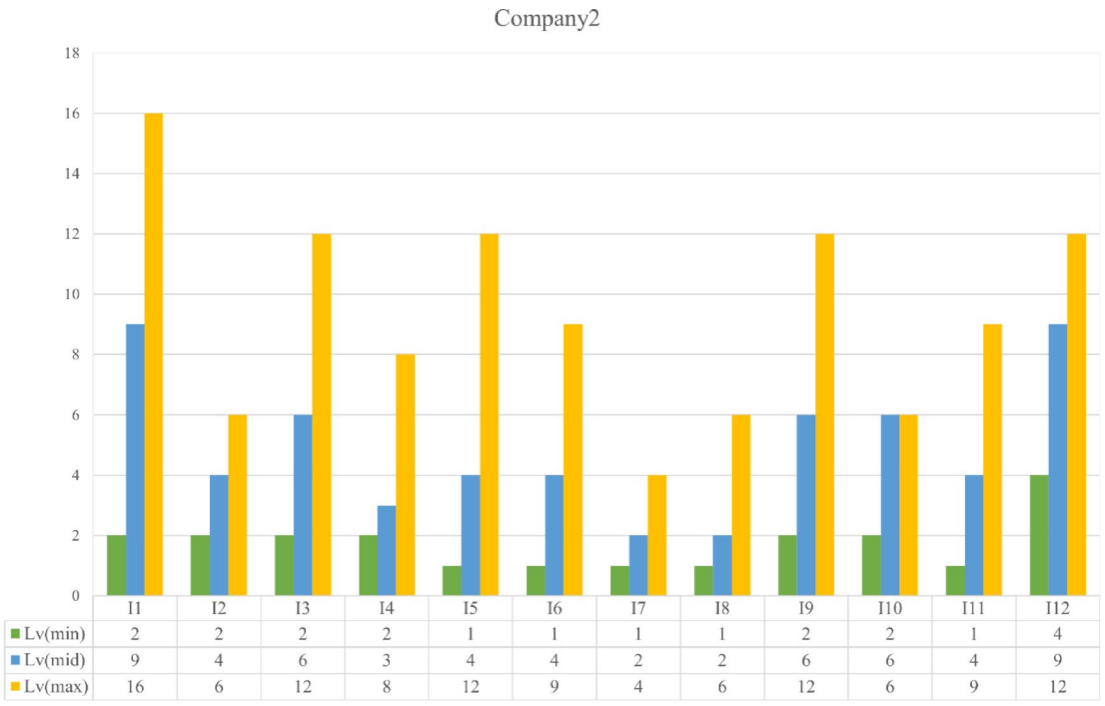
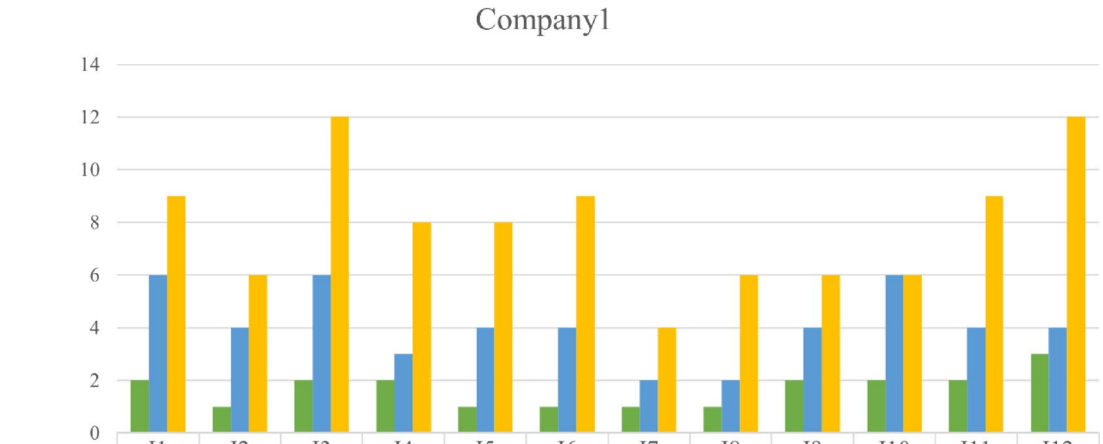
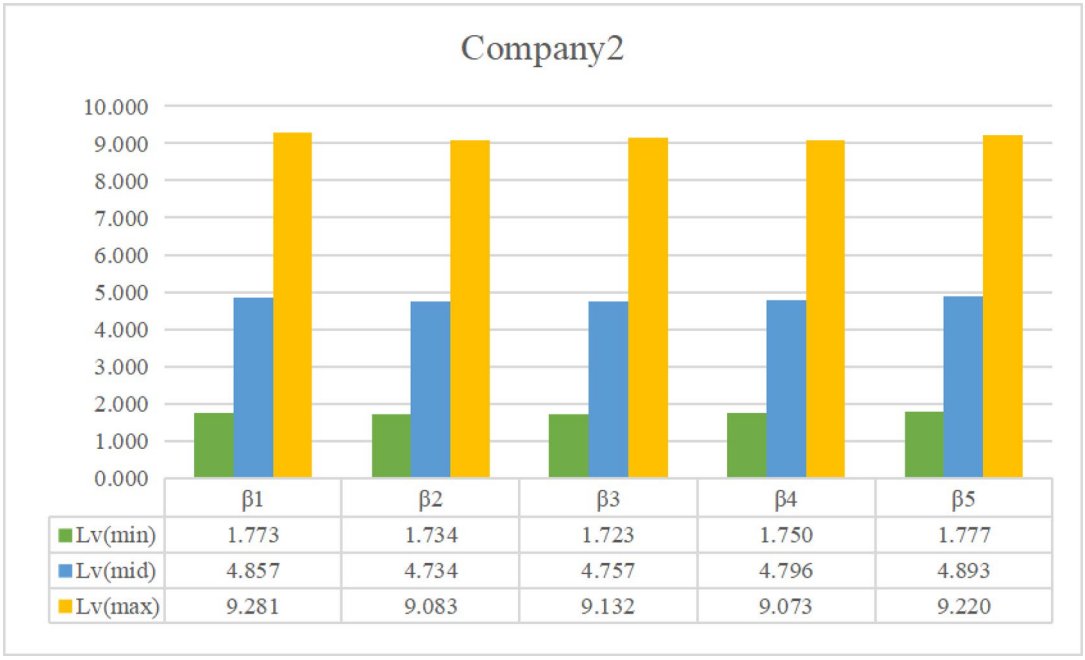


Fig. 5. Financial services indicators fuzzy risk levels of Company 2.



	I1	I2	I3	I4	I5	I6	I7	I8	I9	I10	I11	I12
Lv(min)	2	1	2	2	1	1	1	1	2	2	2	3
Lv(mid)	6	4	6	3	4	4	2	2	4	6	4	4
Lv(max)	9	6	12	8	8	9	4	6	6	6	9	12

Fig. 6. Financial services indicators fuzzy risk levels of Company 1.



	β1	β2	β3	β4	β5
Lv(min)	1.773	1.734	1.723	1.750	1.777
Lv(mid)	4.857	4.734	4.757	4.796	4.893
Lv(max)	9.281	9.083	9.132	9.073	9.220

Fig. 7. Risk categories' fuzzy risk levels of Company 2.

To have a better understanding of its characteristics, there should be a comparison with other common methods of risk assessment. These common methods include AHP-based risk weight assessment method[36–38], risk level assessment method based on risk matrix[39–41], risk uncertainty assessment method based on information entropy[23,42–44], which are more practical risk assessment methods that offer users with valid evaluation results. These methods are compared in the following ways.

(1) Cost: This item considers the investment of resources necessary to conduct the assessment and includes factors such as the ease of expert assessment, the total number of tasks to be performed, and the complexity of the calculations. Higher costs mean that more resources are required to conduct the assessment.
(2) Objectivity: This indicator measures how objectively and accurately the assessment results describe the privacy risks in financial services. Assessments with a higher degree of objectivity provide a more accurate picture of the privacy risks in the services.

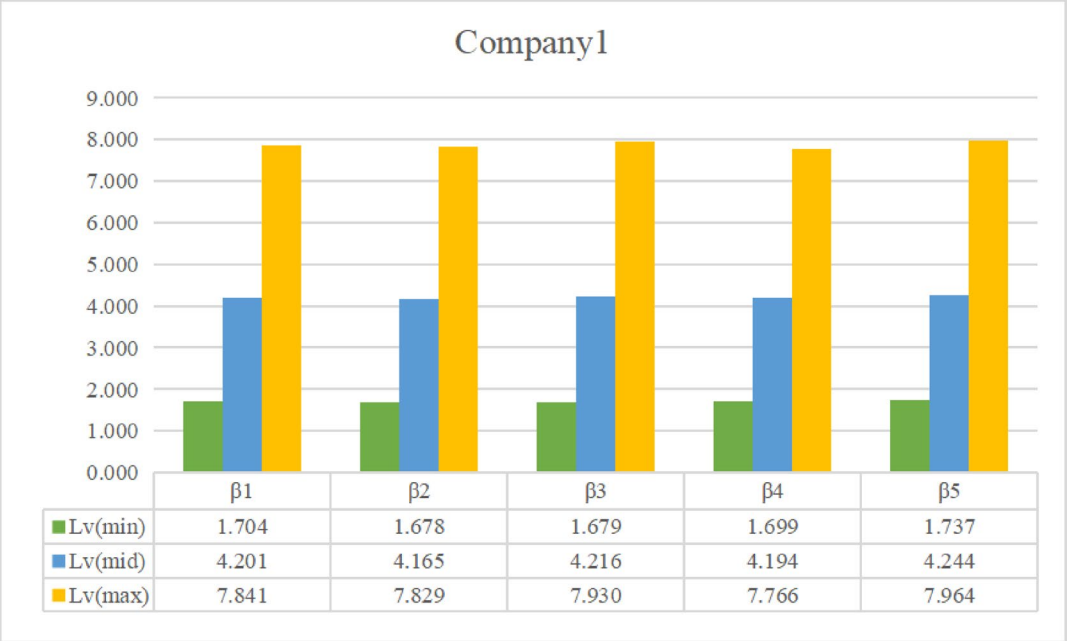


Fig. 8. Risk categories' fuzzy risk levels of Company 1.

Company2						Company1					
Lv^{min}		Lv^{mid}		Lv^{max}		Lv^{min}		Lv^{mid}		Lv^{max}	
1.752		4.807		9.159		1.699		4.203		7.861	
	β_1	β_2	β_3	β_4	β_5		β_1	β_2	β_3	β_4	β_5
f^{min}	1.247	1.228	1.235	1.233	1.245	f^{min}	1.083	1.081	1.092	1.082	1.078
f^{mid}	2.080	2.042	2.062	2.052	2.084	f^{mid}	1.746	1.743	1.775	1.743	1.740
f^{max}	2.851	2.797	2.824	2.809	2.827	f^{max}	2.483	2.472	2.511	2.472	2.508
	β_1	β_2	β_3	β_4	β_5		β_1	β_2	β_3	β_4	β_5
l^{min}	1.421	1.413	1.395	1.419	1.428	l^{min}	1.574	1.552	1.538	1.571	1.611
l^{mid}	2.334	2.318	2.307	2.337	2.348	l^{mid}	2.406	2.390	2.375	2.406	2.439
l^{max}	3.256	3.247	3.233	3.230	3.261	l^{max}	3.157	3.167	3.158	3.141	3.175

Table 16. Comparison of the risk level of financial services between the two Companies.

(3) Comprehensiveness: This indicator reflects the comprehensiveness and completeness of the privacy risk assessment results. The ability of a method to provide more dimensions of privacy risk assessment information indicates that the method performs better in terms of comprehensiveness.
(4) Decision support: This indicator measures the extent to which the results of the assessment actually help users to manage their private information wisely. The higher the value of the reference information provided by the assessment, the stronger the support it provides to users in making informed decisions.
(5) Scalability: This indicator measures the ability of the method to adapt as it encounters new problems or expands its application scenarios.

In this paper, we use {1,2,3} to indicate the level of the above aspects, 3 means good performance in this aspect, 2 means average, 1 means poor. For the cost aspect, 3 means the required cost is larger, 2 means average, 1 means lower cost, and the comparisons of these methods in the above aspects are shown in Tables 17, 18, 19, 20 and 21 below.

With the above situation analysis and rating, we use radar map to compare them together, Fig. 9 shows the results of the comparison.

The above comparison indicates that the method has good performance in scalability, objectivity, comprehensiveness and decision support. However, due to the combination of multiple methods, in order to improve the comprehensiveness and decision support of this paper's method, it must be lacking in other aspects, so it may not perform very well in terms of cost.

methods	Comparison of the costs of methods	Level
AHP	The number of times the judgment matrix is built is greater than 6, because the method may not be completely consistent when establishing the judgment matrix, and the matrix needs to be adjusted several times to meet the consistency requirements.	2
Risk matrix	Only 12 risk indicators need to be evaluated in terms of risk frequency and risk loss.	1
Information entropy	It is necessary to calculate the probability distribution of 12 risk indicators, calculate the entropy weight and carry out uncertainty analysis for the risk level.	2
This paper	Similar to AHP, 6 judgment matrices need to be established, but no consistency test is required. A risk rating assessment is also required for 12 risk indicators.	2

Table 17. Comparison of this paper's method with others in terms of cost.

Methods	Comparison of the objectivity of methods	Level
AHP	The AHP employs a pairwise comparison strategy during evaluation, mitigating the impact of subjective human biases on the assessment outcomes.	2
Risk matrix	In risk assessment, this method tends to assign a risk level directly, thus making the evaluation process susceptible to the interference of subjective judgement and leading to a lack of objectivity in the assessment results.	1
Information entropy	The method is highly dependent on data in the assessment process and has a high degree of objectivity in quantifying uncertainty by analyzing the distribution of data.	3
This paper	This method retains the merits of the AHP pairwise comparison during weight assessment, incorporates the D-S theory to consolidate evaluations from experts in risk level assessment, and utilizes fuzzy theory to characterize risk levels, thereby significantly diminishing the impact of human subjectivity on the evaluation.	3

Table 18. Comparison of this paper's method with others in terms of objectivity.

Methods	Comparison of the comprehensiveness of methods	Level
AHP	The method provides users with impact weights for each risk indicator and risk class in the privacy risk model for financial services, enabling multidimensional and multilevel assessments.	2
Risk matrix	The results of this approach are not sufficiently comprehensive, as only each risk element can be assessed with independence.	1
Information entropy	The method can also provide users with entropy weight assessment and risk indicator level uncertainty analysis during the assessment process.	2
This paper	In the assessment process, it not only provides users with the results of AHP's multi-dimensional and multi-level weight assessment, but also provides the results of risk level assessment.	3

Table 19. Comparison of this paper's method with others in terms of comprehensiveness.

Methods	Comparison of decision support for methods	Level
AHP	The method can only provide users with impact weights for risk elements in the in the privacy risk model for financial services, and does not provide an assessment of the risk level.	1
Risk matrix	The method gives the users the results of risk level, and can help the user to know each indicator from both aspects.	2
Information entropy	The method allows for the description of the risk level by the degree of uncertainty, but does not provide a detailed description of the risk level.	2
This paper	The method not only assessed the weights of the indicators, but also the risk levels of the indicators, defined three risk levels in combination with the triangular fuzzy value, and finally also assessed their comprehensive level.	3

Table 20. Comparison of this paper's method with others in terms of decision support.

Methods	Comparison of scalability of methods	Level
AHP	When the assessment needs change, the method simply adds risk categories and risk indicators to the risk privacy model, but requires a new weighting assessment and consistency test.	2
Risk matrix	When the assessment needs change, the method simply adds the appropriate risk indicators and adds new rows or columns to the matrix. It has little impact on the model structure and is simple to operate.	3
Information entropy	The method relies on the overall distribution of the data to assess uncertainty, and when new risk indicators are introduced, they may significantly change the distributional properties of the data, thus affecting the calculation and interpretation of entropy. This may require larger adjustments or reassessment of the assessment model.	2
This paper	When the assessment needs change, the method is similar to AHP, also need to re-evaluate the weights but do not need to conduct consistency test; in the risk level assessment is similar to Risk matrix only need to expand the corresponding risk indicators.	3

Table 21. Comparison of this paper's method with others in terms of scalability.

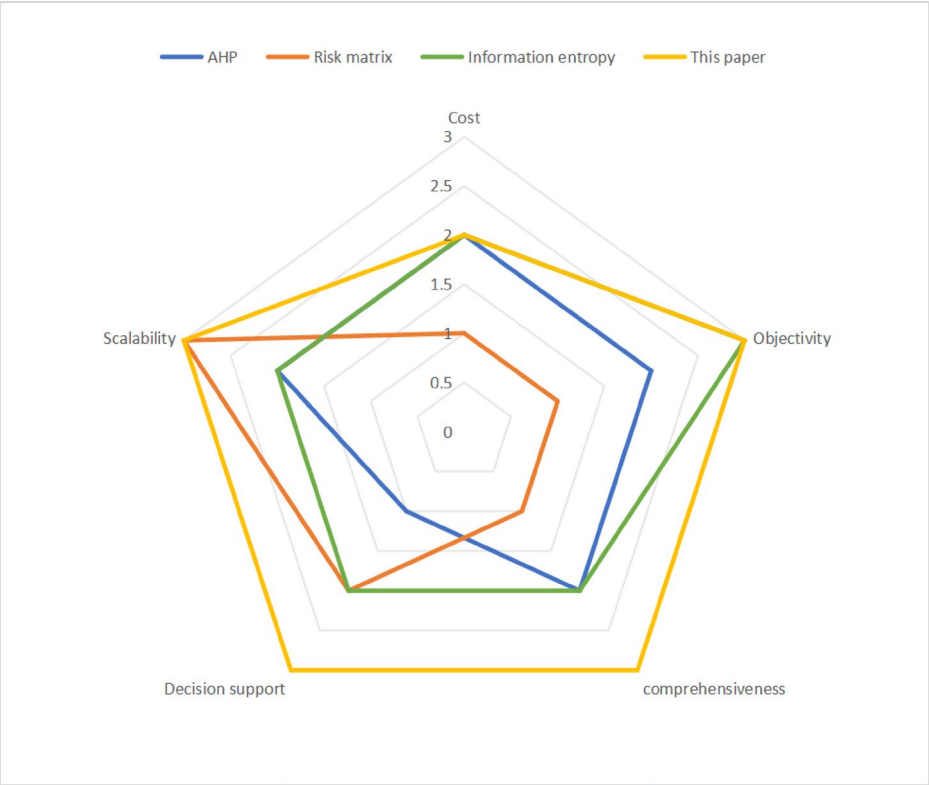


Fig. 9. Comparison of the characteristics of this paper's method with others.

Summary

In this paper, Firstly, the privacy risk categories and risk indicators of financial services are sorted out, and a privacy risk attribute model for financial services is constructed to assess the weights of each layer of the model. Secondly, this paper realizes the effective assessment of privacy risk class by combining D-S theory and fuzzy theory. Finally, a comprehensive assessment method that combines FAHP and D-S theory is proposed. The method breaks through the limitation that traditional assessment models are not comprehensive enough to assess financial services, and it can offer users the comprehensive and objective assessment results of financial services and assist them in effectively managing their privacy information. The method also significantly improves the ability to handle complex data and uncertain information, thus enhancing the efficiency and objectivity of the assessment, especially in financial environment with high multivariate and uncertainty. However, the method used in this paper has some limitations, it can only give a "static" assessment result, but the privacy security of financial services may also change over time. Therefore, in future research, we will further determine the confidence level of risk level and explore efficient dynamic risk assessment methods.

Data availability

The data used to support the findings of this study are available from the corresponding author upon request.

Code availability

The code used to support the findings of this study has been uploaded as a supplementary file and is available for reference. Additionally, the code can also be obtained from the corresponding author upon request.

Received: 8 May 2024; Accepted: 14 August 2025
Published online: 01 October 2025

References

1. The World Bank, The Global Findex Database 2021. China. (2022).
2. Zhicheng, L. Theory and practice of user privacy data security assuranc-ein internet financial business. *Cyberspace Secur.* **11** (01), 11–15. (2020).
3. Ziyuan, C. The impact of digital finance on the digital transformation be-havior of commercial banks. *Mall Modernization*. https://doi.org/10.14013/j.cnki.scxdh.2024.07.044 (2024).
4. Verizon 2023 Data Breach Investigations Report, (2023).
5. Hazzazi, M. M. et al. A fin-ite state machine-based improved cryptographic technique. *Mathematics* **11** (10). (2023).
6. Abdullah Alenizi, S. M. Abdullah, B. Enhancing secure fi-nancial transactions through the synergy of blockchain and artificial intelli-gence. *Ain Shams Eng. J.* https://doi.org/10.1016/j.asej.2024.102733 (2024).

7. Su, Z., Wang, H., Wang, H. & Shi, X. A financial data security sharing solution based on blockchain technology and proxy re-encryption technolo-gy. *2020 IEEE 3rd International Conference of Safe Production and Info-rmatization (IICSPI), Chongqing City, China* 462–465 https://doi.org/10.1109/icspi51290.2020.9332363 (2020).
8. Zhiqiang, W. A., Ni, Z., Tian, Z. & Wang, Y. G. Rese-arch on blockchain abnormal transaction detection technology combining CNN and transformer structure,computers and electrical engineering. **116**, 109194 https://doi.org/10.1016/j.compeleceng.2024.109194 (2024).
9. Xiaofen, M. Optimization Research of Financial Sharing Center of Colle-ges and Universities Empowered by Blockchain Technology. *CooperativeEcon. Technol.* https://doi.org/10.13665/j.cnki.hzjjykj.2024.12.055 (2024).
10. Zhao, Y. & Yifei, S. Research on financial public cloud security risk andsecurity system. *Financial Electron.*, (4) 53–54. (2015).
11. Delei, P., Zilin, Z. Research on the risks and regulation of Cross-bo-rder financial data flow in the digital era. *Int. Bus. Res-earch*. **13** (01), 14–25. https://doi.org/10.13680/j.cnki.ibr.2022.01.004 (2022).
12. Lingyan, S. Transformative impact of digital finance on traditional Fina-ncial industry and transformation path. *Dongyue Luncheon Ser.* **44** (03), 141–148. https://doi.org/10.15981/j.cnki.dongyueluncong.2023.02.017 (2023).
13. Hui, L. Legal regulation of big Data financial algorithms. *Financial Theory Pract.* **42** (02), 148–154 https://doi.org/10.16339/j.cnkihdxbcjb.2021.02.020 (2021).
14. Huairong, H., et al. An accelerated method for pro-tecting data privacy in financial scenarios based on lnear operation. *Appl. Sci.* **13** (3). (2023).
15. Dhiman, S., Nayak, S., Mahato, G. K., Ram, A. & Chakraborty, S. K. H-omomorphic Encryption based Federated Learning for Financial Data Secu-rity. *2023 4th International Conference on Computing and CommunicationSystems (I3CS)* pp. 1–6. https://doi.org/10.1109/I3CS58314.2023.10127502 (2023).
16. Xu, Z. et al. IB2P: An ima-ge-based privacy-preserving blockchain model for financial services. *2021 IEEE International Conference on Blockchain (Blockchain), Melbourne, Au-stralia* https://doi.org/10.1109/Blockchain53845.2021.00083 (2021).
17. Meikang Qiu, K., Gai, H. & Zhao, M. Liu.et al. Privacy-preserving smart data storage for financial industry in cloud computing.
18. Zhong Yihui Design of cloud data storage security and financial risk cont-rol management early warning system based on sensor networks, Measure-ment. *Sensors* **32**, 101064. https://doi.org/10.1016/j.measen.2024.101064 (2024).
19. Luo, D. Research on Financial Systemic Risk Assessment Algorithm Bas-ed on Risk Data Fuzzy Cluster. Analysis. *2022 2nd International Confere-nce on Networking, Communications and Information Technology (NetCIT),Manchester, United Kingdom* 216–219 https://doi.org/10.1109/NetCIT574192022.00060 (2022).
20. Mohammed, A. Aad van M. Risk assessment methodology ForEMV financial transaction systems. *Electron. Notes Theoret. Comput. Sci.* **340**, 137–150 https://doi.org/10.1016/j.entcs.2018.09.010 (2018).
21. Huaiwen, Z., Adnan K., Xinyu, W. & Alina, M. B, Corporate financial risk assessment and role of big data; new perspective using fuzzy analytic hierarchy process. *J. Econ. Forecast.* **0** (2), 181–199 (2021).
22. Ali-Eldin, A., Zuiderwijk, A. & Janssen, M. *A Privacy Risk Assessment Model for Open Data* (Business Modeling and Software Design, 2018).
23. Yang, M. Research on privacy security steady stateevaluation model of mobile application based on information entropy and Markov theory. *Inte-rnational J. Netw. Secur.* **23** (5), 807–816 (2021).
24. Zhang, T., Zhao, K., Yang, M., Gao, T. & Xie, W. Research on privacy security risk assessment method of mobile commerce based on informationentropy and Markov. *Wireless Commun. Mobile Comput.* **11** (2020).
25. Shi, M., Jiang, R., Zhou, W., Liu, S. & Sciancalepore, S. A privacy riskassessment model for medical big data based on adaptive neuro-fuzzy the-ory. *Secur. Commun. Netw.* **9**, 1–18, (2020).
26. Khankeh, H. R. et al. How do cancerpatients refuse treatment? A grounded theory study. *BMC Palliat. Care* **22** (1) (2023).
27. Balusa, B. C. Amit Kumar gorai,sensitivity analysis of fuzzy-an-alytic hierarchical process (FAHP) decision-making model in selection of underground metal mining method. *J. Sustainable Min.* **18** (1), 8–17. https://doi.org/10.1016/j.jsm.2018.10.003 (2019).
28. Meng, F. & Chen, X. A new method for triangular fuzzy compare wise judgment matrix process based on consistency analysis. *Int. Jo-urnal Fuzzy Syst.* **19** (1), 27–46 (2017).
29. Ming, Y. *Comprehensive Assessment of Mobi-le Service Privacy Security Based on FAHP and D–S Theory*. (eds Jiang) (Wireless Communications and Mobile Computing, 2022).
30. Zhou, X. et al. *A DEMATEL-Based Completion Meth-od for Incomplete Pairwise Comparison Matrix in AHP* (Cornell Univer-sity - arXiv, 2016).
31. Chao, W., Chen, L. & Liangguo, K.Method for quantitative expression of psychological safety and security distance(PSSD) using fuzzy theory. M-ethod for quantitative expression of psychological safety and security dist-ance (PSSD) using fuzzy theory.
32. Yantao Geng. Research on multimodal data fusion method based on deep learning and D-S evidence theory[D]. https://doi.org/10.27398/d.cnki.gxalu.2023.000345 (Xi'an University of Technology, 2024).
33. Robbins, H. E. An empirical bayes approach to statistics. Spring-er Series in Statistics, Breakthroughs in Statistics. https://doi.org/10.1007/978-1-4612-0919-5_26 (1992).
34. Zhu, Q., Kuang, X. & Shen, Y. Risk matrix method and its application in the field of technical project risk management. *Eng. Sci.* **5**, 78–88 (2003).
35. Yang, M., Gao, T., Xie, W., Jia, L. & Zhang, T. The assessment of Clo-ud service trustworthiness state based on D-S theory and Markov chain. *IEEE Access.* **10**, 68618–68632. https://doi.org/10.1109/ACCESS.2022.3185684 (2022).
36. Singh, M., Khajuria, V. & Singh, S. Kamal singh,landslide susceptibility evaluation in the Beas river basin of North-Western himalaya: a Geospatial analysis employing the analytical hierarchy Process(AHP) method. *Quaternary Sci. Adv.* **14**, 100180. https://doi.org/10.1016/j.qsa.2024.100180 (2024).
37. Estrada-Esponda, R. D., López-Benítez, M. & Matturro, G. Juan Carlos Osorio-Gómez,Selection of software agile practices using Ana-lytic hierarchy process. *Heliyon* **10**, 1, e22948. https://doi.org/10.1016/j.heliyon.2023.e22948 (2024).
38. Singh, M. et al. Landslide susceptibility evaluation in the Beas river basin of North-Western himalaya: a Geospatial analysisemploying the analytical hierarchy process (AHP) method. *Quaternary Sci. Adv.*, 14100180 (2024).
39. Ju, M. Establishment and application of city safety assessment model B-ased on risk matrix. **6** (3). (2023).
40. Su, X. et al. *An Airport Ser-vice Risk Management System Based on Risk Matrix and Borda Count Method, 2022 2nd International Conference on Big Data. Artif. Intell. (ICBAR)*, 161–165, (2022).
41. Xiyuan Miao, H. & Jing, L. W. The identification of high-risk factors of banks based on risk matrix. *Procedia Comput. Sci.* **214**, 272–279. https://doi.org/10.1016/j.procs.2022.11.175 (2022).
42. Mohammed, H. & Saad, D. X. Initial selection of configurations based on information entropy for multi-level design optimization. *Proc. CIRP* **119**, 533–538, https://doi.org/10.1016/j.procir.2023.02.148 (2023).
43. Yuan, K. et al. AK-SYS-IE: A novel adaptive Kriging- based method for system reliability assessment combining information entropy. *Reliabil. Eng. Syst. Safety* 246110070 (2024).
44. Ni, B. S. C., Wang, J. & Wang, Y. Research on venture capitalbased on information entropy, BP neural network and CVaR model of di-gital currency in Yangtze river delta. *Procedia Comput. Sci.* **187**, 278–283. https://doi.org/10.1016/j.procs.2021.04.063 (2021).

Acknowledgements

The authors would like to thank the anonymous reviewers and the editors for their suggestions.

Author contributions

Material preparation, data collection, and analysis were performed by Rong Jiang, Jia Wang and Tiebing Li. First draft of the manuscript was written by Dongri He and Ming Yang, and all authors commented on previous versions of the manuscript. All authors read and approved the final manuscript.

Funding

This research was supported by the National Natural Science Foundation of China (no. 72261033), Yunnan Fundamental Research Projects (nos. 202501AT070461).

Declarations

Competing interests

The authors declare no competing interests.

Ethical statement

I certify that this manuscript is the original and has not been published. During the submission period, it will not be submitted to other places for publication. The authors declare that they have no conflict of interest. This article does not contain any studies with human participants or animals performed by any of the authors.

Additional information

Supplementary Information The online version contains supplementary material available at https://doi.org/10.1038/s41598-025-16457-9.

Correspondence and requests for materials should be addressed to M.Y.

Reprints and permissions information is available at www.nature.com/reprints.

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.