Research Article

Yanzhao Wang*

Intelligent cluster construction of internet financial security protection system in banking industry

https://doi.org/10.1515/comp-2022-0268
received November 28, 2022; accepted February 24, 2023

Abstract: As the rapid advancement of information security company is developing quickly and the technology including big information, big computer, large cloud, and artificial intelligence are being widely used, network security has entered a new era. While ushering in huge development opportunities, it also faces severe tests. Network security is a major issue related to the comprehensive realization of a well-off society and national security, and has risen to the national strategic level. The current financial industry network security construction mainly focuses on team, process construction, and the research and development of individual tools and equipment. It lacks system research and implementation guidelines for defense technology construction based on industry IT characteristics. At the same time, there is also a lack of objective and unified measurement and evaluation standards for enterprise security defense capabilities, which restricts the improvement of cybersecurity capabilities in the financial industry to a certain extent. In terms of actual combat exercises, in various actual combat exercises over the years, the technical architecture of the bank's network security defense has withstood the test of high-intensity confrontation. The defense process achieved zero deductions, and stood out among the participating defending teams through traceability and countermeasures, which effectively improved the network security large-scale group operations and security protection capabilities. The effectiveness of the technical architecture design is verified in actual combat, which shows that the control of the bank's internet financial security protection system is effective. With digital computing, all banking transactions are fully automatically implemented and the bank's clientele is systematically self-managed. It predicts that using this system, the speed can be increased by 98% and the accuracy can be increased by 12%.

Keywords: bank internet financial security, network financial ecology, financial technology, open internet bank, bank transactions

1 Introduction

Internet financial security is a whole, and we must not defend like blind people feeling like elephants. The ideal defense is to protect against all attacks, but considering the actual situation such as organizational resource constraints, we need to do "moderate" security, that is, the level of internet security measures should be consistent with business value. Internet financial security is not only a technical problem, but also a management problem. It includes not only general security issues, but also business security issues. Security construction is actually the process of fighting against invasion. Only by strengthening cooperation in all aspects and building an internet financial security system, can we win.

Internet finance is the most rapidly developing and emerging field at home and abroad. At the same time, it is facing many security threats. For example, through the online to offline closed-loop system of "QR code + account system + LBS + payment + relationship chain," a new "consumption scenario" has been formed. However, it is worrying that QR code payment has broken through the business model of traditional acceptance terminals, and its risk control level is directly related to the customer's information security and capital security. At present, the security standard of the terminal is not clear when the QR code is applied to the relevant technology in the field of payment, and the security of the relevant payment verification methods is still in doubt, and there are certain potential payment risks.

During recent few decades, open internet banking has become the forefront of financial technology under

* **Corresponding author: Yanzhao Wang,** Henan Institute of Economics and Trade, College of Finance, Zhengzhou 450018, Henan, China, e-mail: 20140100@huel.edu.cn

new financial landscape. It has become the internal driving force for digitalization, platformization, and ecological transformation which provides new opportunities for banking business reform, transformation and upgrading, and quality and efficiency improvement. Banks have changed from traditional branch model, APP model to API model. Through API technology, the whole line of scenarios is opened, and an online financial ecosystem of "sharing, openness, cooperation and innovation" is built. Open banking has evolved into an era of panoramic banking that intelligently senses user needs. Taking ecological scenarios as touchpoints, it connects all ecological parties through technologies such as APIs, SDKs, and small programs. Data openness expands data boundaries, technological interaction extends network boundaries, and business integration breaks industry boundaries. However, the application of financial technology and the reconstruction of business scenarios have led to new security challenges in areas such as compliance security, data security, privacy protection, and business security. The aim of this study is to build security protection clusters in banks through financial technology. Through the explanation of financial technology, online system and security, as well as bank internet intelligent clusters, it is found that the security of intelligent clusters through internet is higher.

Internet is one of the several services available for customers to access their information, correspond with each other, or perform financial procedures on the internet. Asuan believed that the service implementation method of bank transactions is to use the bank account, user name, and password that the customer already has, and then conduct bank transactions through online banking. The survival and development of banks are inseparable from the changes in the internet era. The banking industry has undergone tremendous changes in both service content and service methods. The banking business has developed from a single counter model to diversified scenarios such as PC, mobile terminal, and third-party payment [1]. Internet of things (IoT) refers to the ability to assign unique identifiers to efficiently connect related devices to enhance communication. The e-SIM application cannot generate reliable and realistic data. Mathew believed that the system should introduce strict conditions in order to evaluate and differentiate between IoT and non-IoT devices during their operation for obtaining the expected results from users [2]. The main model of location privacy protection proposed by Lai et al. is trusted third party (TTP), but once TTP is untrusted or attacked, the end user has the risk of location privacy leakage. In response to the above problems, he proposed a gridding symmetric encryption scheme that comprehensively used grid coordinate automatic processing and order-preserving encryption mechanism [3]. Prokopowicz et al. investigated the economic globalization in the development of international financial markets. In the context of national public administration security, the security of electronic data transmission on the internet is becoming more and more important [4]. Zhou et al. presented trustworthy agglomeration as a new agglomerative technique that used trustworthiness as a measure of metric during fuzzy agglomeration. They designed one series of general purpose trustworthiness clustering arithmetic in a solution architecture with alternating agglomerate clustering estimated for trustworthiness clumping models. Moreover, they also recommended one new trustworthy agglomeration for practical implementation with numerical instances for different dimensions of performance as well as outcome for the trustworthy agglomerations anchored on both randomly created and real sets of data [5]. Japan, Advanced, etc. proposed clustering algorithms, such as classical and fuzzy computational clustering algorithms and regular clustering algorithms [6]. Hasheminejad and Khorrami use research methods such as clustering algorithms to explore new features of customer accounts. With these new features, a profitable number of customers will be identified with more accurate information about the customer being clustered. There are two aggregation methodology (*K*-means and CPSOII) which have been used for checking the customer. Advantage of CPSOII over *K*-means is that CPSOII determines a number of aggregation automatically [7]. Vahdatzad and Zare investigated the modeling or clustering the trust behavior of the clients with the use of neural networking for optimal configuration by financial allocation for improving the banking performance. We determined each input dimension's respective coefficient through the use of the analytic hierarchy procedure, and these coefficients will then be considered the primary weapons of a fuzzy and neural wall network [8]. Negnevitsky conducted a congregation in the analysis of experimental consequences for determining the failure banking experience using self-organizing and neural networking. After describing primary factors and the likelihood that banks would fail, he then demonstrated a self-organizing neural network implementation with the results of his research. His findings demonstrated how the self-organized network represents the powerful vehicle used to identify the potentially collapsing individual banks. Finally, he addressed a number of limitations of the cluster analysis regarding understanding of the exact implications of every clustering

[9]. Chuy et al. have discussed about the conceptual questions about the role, the structure, and the financial institutions and made a relative analysis about the various typologies in the financial institution network. The importance as well as functioning of the financial institutions and their purpose is noted, before they outlined the different categories and types of the national financial institutes [10].

A research study sampling from this survey was composed out of 287 interviewees, which include 164 men (57.14%) and 123 women (42.86%). According to them, a transformation in banking would require, first and foremost, establishment on digital networking. Second, it will need transformation in the existing banking industry for activities that will reduce the costs in banking. Under digital banking, there will be fully automated services in banking and a self-administered system for the customers in the banks.

2 Financial technology

This article mainly describes the steps of establishing the Internet Golden Boy security protection system, and obtains the security of the protection system through experiments. A lot by way of economic powers will be at work, like other financial and related applications in the financial services and related sciences industries from the past. Such findings were intended both to guide research undertaken with senior administrators with regard to the economics in mobile payouts in general with the aim and to help determine several important streams in which to research. Fintech is the abbreviation of financial technology, which can be simply understood as finance + technology, but it is not a simple combination of the two. It refers to the use of various scientific and technological means to innovate the products and services provided by the traditional financial industry, improve efficiency, and effectively reduce operating costs. According to the definition of the Financial Stability Council, financial technology mainly refers to the emerging business models, new technology applications, new product services, etc., driven by emerging cutting-edge technologies such as big data, blockchain, cloud computing, and artificial intelligence, which have a significant impact on the financial market and the supply of financial services. Fintech start-ups and new entrants in the financial industry rely on various financial innovation technologies to transform the products and services of the traditional financial industry, broaden the access channels of traditional financial institutions, improve the operational efficiency of financial service providers, and improve their risk management capabilities. Both finance and technology have a rapid iterative speed, through the continuous development of a large number of small technologies, they will eventually complete leapfrog development. The iteration cycle of Fintech is faster. It is guided by financial demand and supported by technological innovation, and can complete huge and far-reaching changes in a short time. The model used for building the information about banks with internet is shown in Figure 1.

In Figure 1, there are products and risk management in finance. The bank and internet companies achieve win–win cooperation through the internet financial platform. Under internet companies, there are mainly platform systems, operating experience, financial customers,

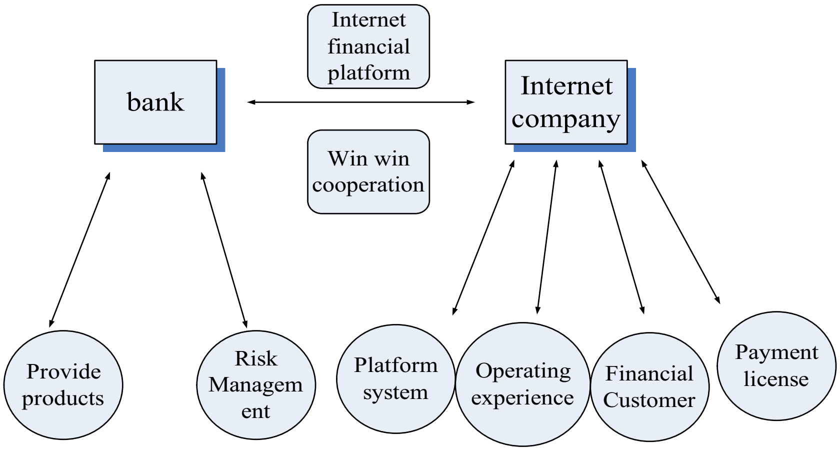

Figure 1: Bank and internet information construction mode.

and payment licenses. In this work, the problems that exist on the management as well as their governance and principal agency aspects in China's Fintech foundation were investigated. By using a game-based methodology, as well as emphasizing on potential advantages to community and optimism considerations by community hospitals, the stakeholders who influence the management in the technology foundation are analyzed. This includes the advancements made in technology, the changing nature, and expectations in consumer practices with respect to a digital provision for the delivery from financial institutions, as well as a regulatory response from the financial institution. These create opportunity for new and emerging, minimally regimented players [11]. Improvements to technology in the provision of banking through the internet are opening up a broad segment for the remote banking services, which in turn is resulting in an increase in the number of frauds in this segment. The protection against and the prevention of fraud during the provision of remote banking is imperative for solving this issue [12]. The most sophisticated prevention expertise has been unable to keep pace with the increasingly more complex and sophisticated versions of the malware, like the industry's significant use of anti-virus to combat attacks. And it works very well against any malware that has known signature. However, due to the large number of malware samples released every day and its inefficiency in dealing with vulnerabilities, if USIM information is used for passwordless protection of the private key (the actual detection rate ranges from 25 to 50%), which is used for online banking, online shopping, stock trading, etc., the security of user information can be improved [13,14]. In terms of two survey dimensions, financial integrity in the banking sector is defined as the basis for effectively utilizing and managing banks' financial resources and improving financial solvency to deal with financial risks brought about by uncertainty. Through the implementation of digital programs with algorithms, it is possible for the stable performance of the banks and the increase in the security of the virtual informational universe. Modules in the cryptographic regime can be partially reconfigured in operation (PR). The first module is for the dynamic cryptographic mechanisms of the key production while the second is used in the Data exception criteria for the inverted displacement and Advanced cryptography solutions for the shift of the blocks, both modules play important functions in the security of the data [15,16]. Tables 1–3 are data on audit quality, political affiliation, and investor protection for online banking and business magazines, respectively. There are four variables that have been chosen to be used to provide representation for the quality of the auditing. The return on assets (ROA) was used to benchmark the performance provided to the firm, while manager ownership is used as the measure instrument to benchmark the protection afforded to an investor [17].

Computer banking is perhaps one of the biggest time conserving innovation in banking technology since the automated teller machine, it also opens the new possibilities to the attackers, principally because the increasing number of computer bugs as well as the trojan problems are not yet being adequately resolved. Such viruses as well as the Trojan will attack the computers against the heart. Several approaches have been used to combat for them, while none were considered to be 100% more effective. More important is that most of the personal machines are virtually unprotected against viruses and hence are susceptible to attacks, which can be problematic. Since virtually no personal computing banking schemes are dependent on the authentication with the use of an identity key, and the systems can be vulnerable thereto, there is increasing concerns for consumer identification, the confidentiality on credentials, or the integrity of the transaction message. This study is to emphasize the protection of online banking. First, various vulnerabilities of e-banking are analyzed and all types of attacks are actually investigated. It then introduces a security cognizant infrastructure which prevents from the multiple attempts of attack. The proposed architecture with a security agreement and a credential verifying mechanism first checks for authenticity from the sender, which covers all the components from the detection for phishing to two factors certification. Using only a small and secure facility that created the trusted routes to the customers and not relying on a trusted customers' machine, it then describes a demonstrated deployment of this system [18,19], as shown in Figure 2.

Table 1: Performance objectives of listed companies for audit quality

Variances	Observations	Average	Schedule dev	Mines	Maximum
Political connection	249	1.260	1.440	1.000	2.000
ROA	249	1.121	1.229	−1.333	2.398
Audit quality	249	1.544	1.499	2.121	2.010

Table 2: Performance objectives of listed companies for political affiliation

Variances	Cooperative efficiency	Technical value	*P*-Values
Adj *r*	1.031		
R	0.046		
P-value	0.020		
F-ratio	2.980		
Firm age	−1.083	−2.76	0.077
Constants	0.253	3.29	0.001
Pol-conn	−1.073	−3.03	0.041
Inv protection	−1.039	−3.06	0.038

Table 3: Performance objectives of listed companies for investor protection

Variances	Royal	Auditing the quality	Plurinational state of Bolivia	Sponsors	Firm size	Visuals
Sponsors	−0.146	0.053	0.128	1.000		1.04
Firm Size	−0.086	0.029	−0.198	0.026	2.000	1.01
Pol con	−0.102	0.378	1.000			1.24
Audit qual	0.031	1.000				1.18
ROA	1.000					

This study proposes to introduce an improved alerting mechanism to monitor security protocols and generate messages as needed in a secure protocol approach with certificate and signature verification. Alert messages include: (1) If no appropriate certificate is received or available, then it will generate no certificate. (2) If the received certificate is damaged, a bad certificate will be generated. (3) If the received certificate is not supported, it will be unsupported certificate. (4) If the received certificate expires, an expired certificate will be generated. (5) If the received certificate part does not match, an unknown certificate will be generated.

Figure 3 shows the construction system of the internet and banks.

New developments in the IoT technologies may improve Business process administration effectiveness and consequently the performance is improved. In this study, an approach for re-engineering the protection regime of a banking location (BL) and making the BB "more intelligent" is described. On the basis of the multi-case method of research, in this study, we deploy the four step Business process re-engineering process development and design from the viewpoint of the information technology development. A multi-method methodology is used for the collection and verification of the results of the data to overcome limitations of the scarcity or information requirements of the modeling campaign. The approach reductions in preparation and system efforts, operational savings, as well as improvements in the quality of information, were achieved as a result of a thorough documentation audit and an intensive profiling exercise. It enhances protection against criminal aggression by improving the system's holistic validation [20].

3 Online system and security

Internet banking or electronic banking has caught on with banks, brokerage companies as well as insurance firms, which is evident since the end of 1990s not only across all developing nations but also across the electronics and business communities. Online internet banking and payments will increase rapidly, transactions over the internet are still ongoing. Information technology law provides a secure and legal framework for e-commerce transactions, educates and trains people on e-banking in various institutions so that people can become friendly to electronic banking. Electronic banking will pave the way for a cashless economy, which will bring transparency to the system. Sweden is the only cashless country in the world and almost all transactions made are online system transactions. Most people are using Paytm and other such applications for various transactions. Big data found that internet finance is on an upward trend year-on-year, as shown in Figure 4.

It can be seen from Figure 4 that the financial transaction volume is increasing year by year, which shows the gradual development of internet finance.

The gender data of online banking according to statistics are shown in Table 4.

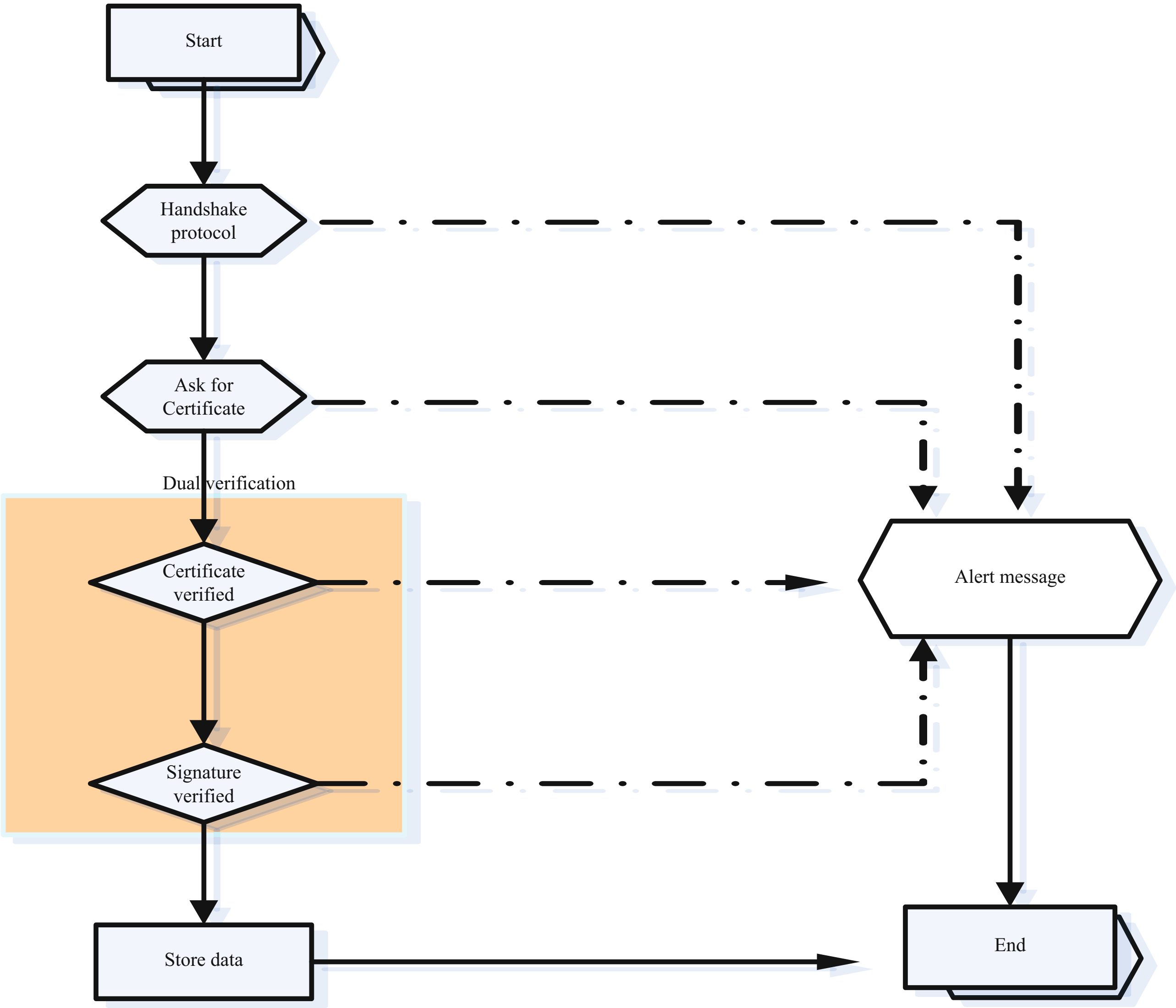

Figure 2: Description of system demonstration implementation.

Representing the data in tabular form, these data are based on online banking. It can be seen that a considerable proportion of online banking users use online banking 1–5 times/month. Another 31.5% use e-banking 6–10 times a month, and the use of online banking in terms of gender reflects the polarization towards men. This shows that in internet finance, the main crowd is still men, and women are relatively few.

4 Using bank internet intelligent clustering

The so-called banking internet clustering analysis is to discover the relationship between data objects and group the data. The greater the similarity within the group and the greater the difference between the groups, the better the clustering effect. In this study, the main method of cluster analysis is to explain the bank internet intelligent cluster.

By using algorithm evaluation criteria such as SSE, VRC, and DBI, it was concluded that CPSOII with DBI = 0.44 is the most suitable clustering algorithm. Because there are appropriate indicators to compare the algorithm results, the most appropriate DBI parameters can be selected.

By using the results of CPSOII, the lifespan of customers was calculated, and it was found that customers with the highest RFM indicator values lived the longest. Banks should plan their maintenance. Two clustering methods (*K*-means and CPSOII) have been used to check

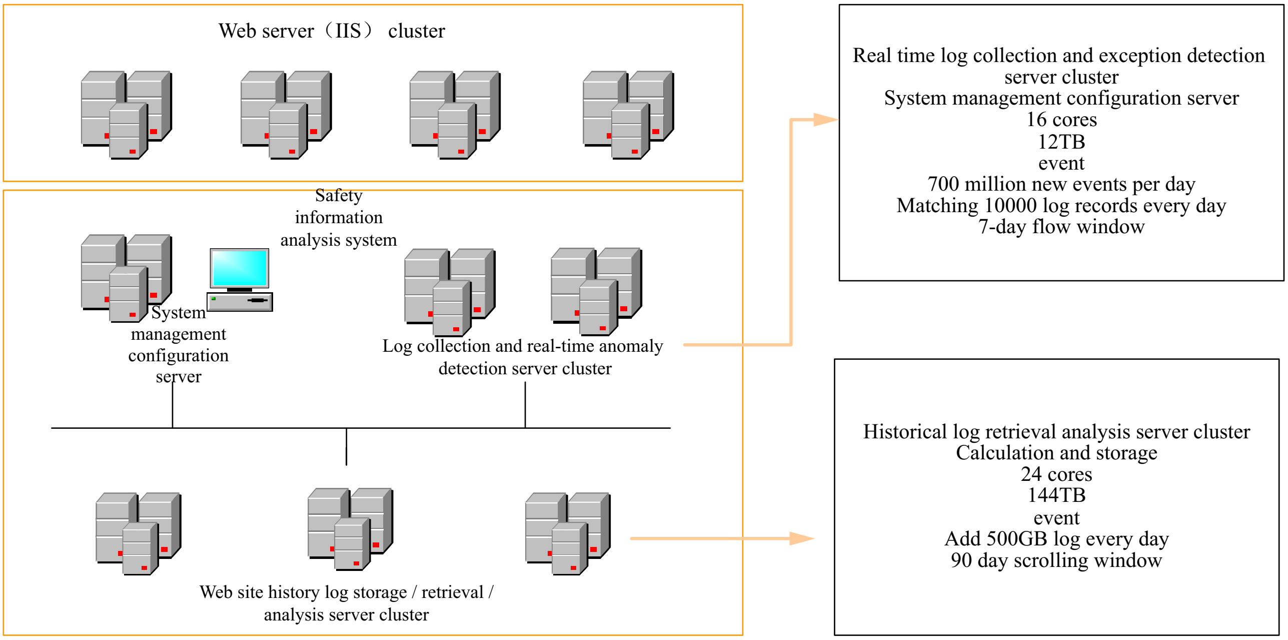
Web server（IIS） cluster
Safety information analysis system
System management configuration server
Log collection and real-time anomaly detection server cluster
Web site history log storage / retrieval / analysis server cluster
Real time log collection and exception detection server cluster
System management configuration server
16 cores
12TB
event
700 million new events per day
Matching 10000 log records every day
7-day flow window
Historical log retrieval analysis server cluster
Calculation and storage
24 cores
144TB
event
Add 500GB log every day
90 day scrolling window

Figure 3: Structure of internet banking.

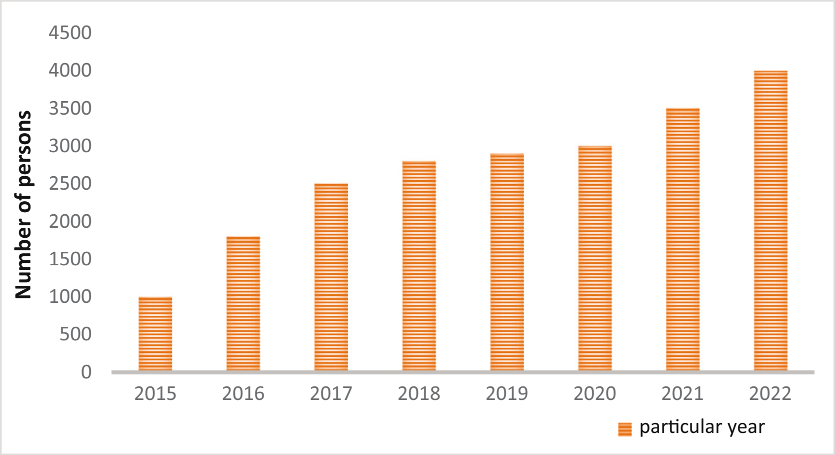

Figure 4: Banking internet finance trends.

customers. The advantage of CPSOII over *K*-means is that CPSOII can automatically determine the number of clusters.

The commonly used distance calculation formula is the Minkowski distance given as follows:

$$u_i = \{x_{i1,}x_{i2} \dots, x_{in}\}, u_i = \{x_{j1}, x_{j2} \dots, x_{jn}\}, \tag{1}$$

$$\text{dist}_{mk}(x_\text{i}, x_\text{j})^n = \left(\sum_{k=1}^{n} \text{I}x_{ik-x_{jk}}I\dot{p}\right), p \geq 1, \tag{2}$$

where u_i is the set of Minkowski distances of i users. Commonly used calculation formula based on square error.

Table 4: Gender data of online banking according to statistics

Frequency of use (number of times per month)	Percentage of total respondents		
	Female	Male	Sum
Not used	—	—	1.0
1–5	15.8	40.7	56.5
6–10	9.3	22.2	31.5
10–15	3.7	1.9	5.6
16–20	—	2.7	2.7
Above 20	—	2.7	2.7

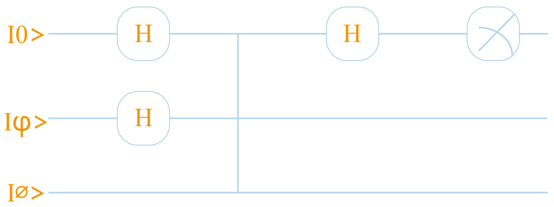

Figure 5: Circuit diagram of quantum nearest center algorithm corresponding to samples.

$$E = \sum_{I}^{K} \sum_{X \epsilon \mathrm{CI}} (X - U_I)^2. \tag{3}$$

E is the average error. Minkowski distance is also the abovementioned paradigm distance. When $p = 1$, it is the Manhattan distance, and the formula is as follows (taking two-dimensional space as an example).

$$D = Ix_{1}\_x_{2}I + Iy_{1}\_y_{2}I. \tag{4}$$

D is the Manhattan distance in two-dimensional space. The new clustering formula is as follows.

$$Z_J(I + 1) = \frac{1}{N} \sum_{k=1}^{n} X_i, \quad j = 1, 2 \ldots k. \tag{5}$$

Using the controlled-SWAP gate and Hadamard gate to transfer the distance of the two quantum states to the first control bit, it can be calculated as follows:

$$p(I0>) = \frac{1}{2} + \frac{1}{2} I < \Phi I\varphi > I^2. \tag{6}$$

Among them, $I < \Phi I\varphi > I^2$ is the distance between two quantum states, and its route is shown in Figure 5. The K-means algorithm can be calculated by the above quantum algorithm.

Input: sample set $D = \{x_1, x_2, \ldots, x_m\}$, number of clusters K, quantum K-means circuit, and update times m.

Process: 1. Randomly select K samples from D as initial centroids $\{u_1, u_2, \ldots, u_k\}$

2. Repeat m

3. Let $c_i = \Phi(i = 1, 2, \ldots, k)$

4. For $j = 1{,}2{,}\cdots m$ do

5. The features of x_j and cluster centers are compressed and embedded as parameters in the U-gate of the quantum K-means algorithm.

6. According to the quantum algorithm, the centroid closest to the sample j is obtained, assuming u_t

7. Assign x_j to the corresponding class c_t

8. End for

9. For $i = 1{,}2{,}\ldots \bullet k$ do

10. Calculating the new mean vector $u_i = \frac{1}{IciI} X$

11. End for

Output: clustering $C = \{c_1, c_2, \ldots, c_k\}$

Figure 6 shows the roadmap of the complete quantum K-means algorithm for a sample i.

By improving the algorithm, the intelligent clustering banking system and the survey views of traditional banks have been significantly improved, as shown in Figures 7 and 8.

Comparison of convergence speed between traditional algorithm and improved algorithm are shown in Figures 9 and 10.

Using smart clustering, customers are classified, as shown in Table 5.

The new characteristics of customers with their accounts, which can identify lucrative individuals for clustering out more accurate customer profiles, were explored. The two clustering techniques (K-means and CPSOII) were used to study the customers. An advantage of CPSOII compared to K-means was that CPSOII can automatically determine clusters quantitatively.

5 Network security of online banking

Assuming that the attacker knows the customer's username and its electronic banking system's password, the

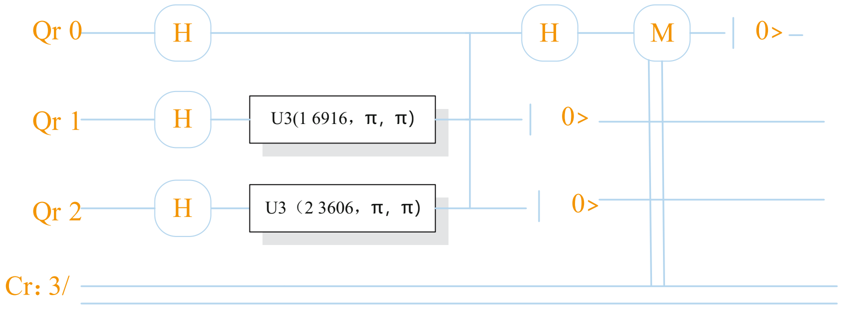

Figure 6: Quantum corresponding to the sample K-means algorithm circuit diagram.

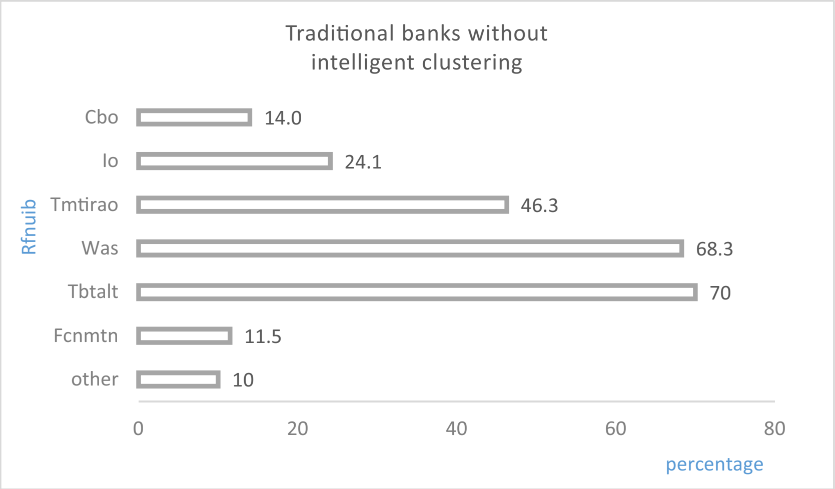

Figure 7: Reasons for not using internet banking. Note: Fcnmtn: function cannot meet the needs, Cbo: convenient banking outlets, Io: inconvenient operation, Tmtirao: too much trouble in registering and opening, Was: worry about safety, Tbtalt: traditional banks take a long time, and Rfnuib: reasons for not using internet banking.

attacker can take full control of the customer's account without the use of additional secrets to self-execute the transaction.

When customers need to gain access to the electronic banking system, they need to be authenticated first, by connecting to a bank through SSL or TLS to obtain a digital certificate. When the certificate is digitally signed by one of the trusted certificate authorities, the browser will not display a warning. Before the client enters the username and password, the client should check if the certificate belongs to the relevant bank.

Not everyone understands how certificates work. After sending a client an unprotected SSL/TLS link, some clients will not notice the problem. If they click on the link, the attacker is able to collect their account data on their own. Assuming the client always checks that SSL/TLS is used when communicating with the bank, the attacker may have received a signed digital certificate. The client can then see the SSL/TLS usage time, and the connected bank and browser do not display warnings. When a client authenticates, sometimes a masked or complex password is used therefore, the attacker needs more attempts to obtain the entire password.

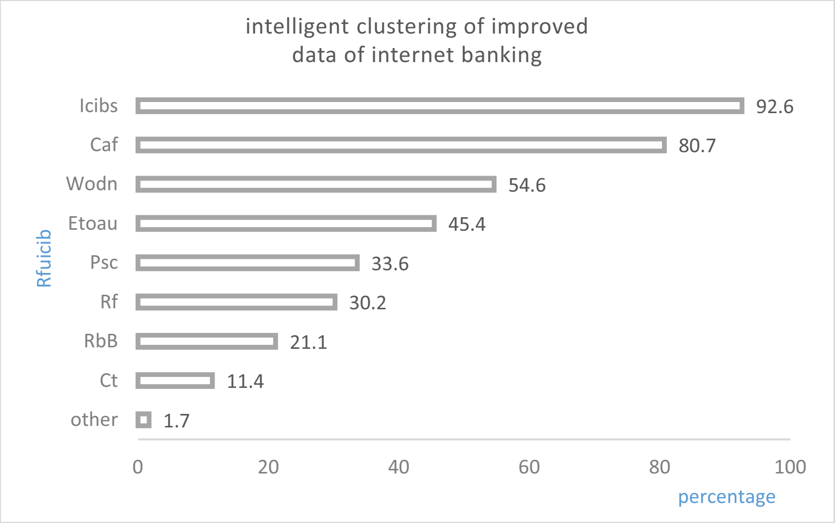

Figure 8: Reasons for using intelligent clustering internet banking. Note: Ct: curious try, RbB: recommended by merchants/banks internet banking, Rf: rich functions, Psc: preferential service charge, Etoau: easy to open and use, Wodn: work or daily needs, Caf: convenient and fast, Icibs: intelligent clustering internet banking security, and Rfuicib: reasons for using intelligent clustering internet banking.

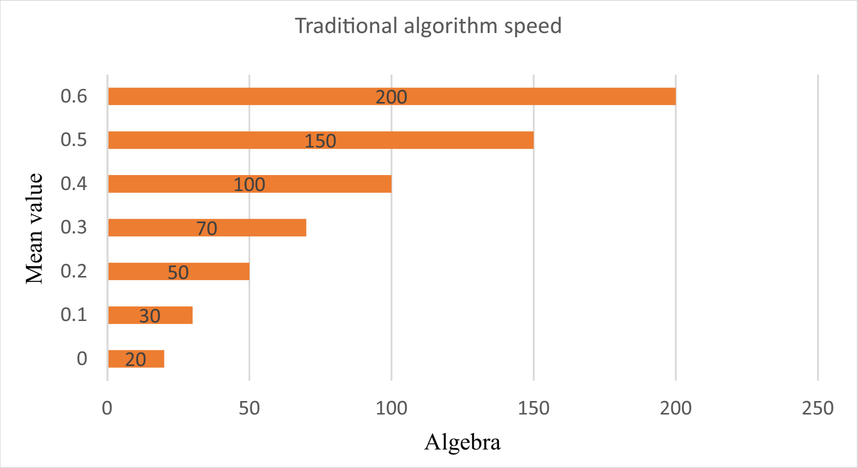

Figure 9: Convergence speed of traditional algorithm.

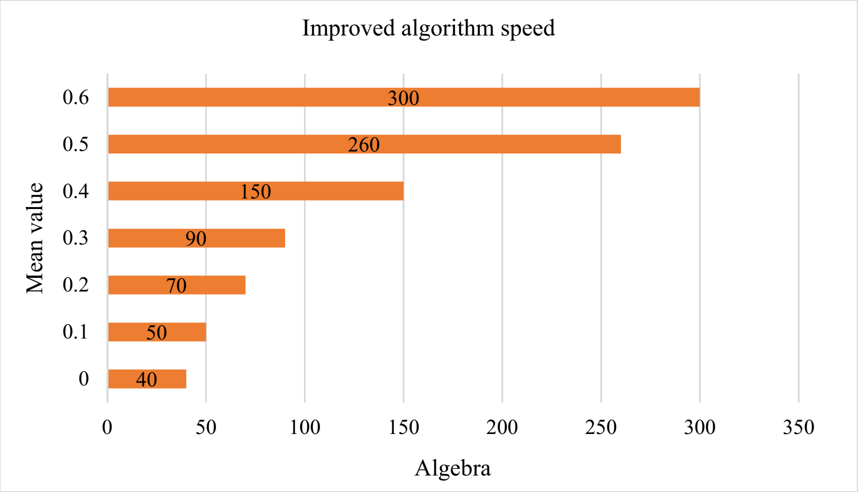

Figure 10: Convergence speed of the improved algorithm.

6 Discussion

The construction achievements of the internet financial information security system can be applied to the information security field related to the internet financial platform. The improvement in the information security level of the internet financial enterprises can reduce the problems caused by information security. The loss caused by it can avoid the loss to users and reflect good social benefits. With the strong dissemination of internet finance, it can enhance the attention of society and relevant enterprises and institutions to information security, increase

Table 5: Classification of customers using smart clustering

Customer type	Percentage	Traditional *K*-means algorithm	Improved algorithm
Premium customers	5.96	82.15	85.75
Key customers	14.56	85.49	87.14
Regular clients	59.24	79.97	94.14
For small accounts	10.45	84.86	89.06
Lead capture	6.76	89.13	94.13

the demand and investment in security, drive the development of independent and controllable information security industry, drive the increase in personnel positions, and generate good economic and social benefits. It also plays a positive role in promoting the establishment and improvement of the information security supervision system of internet finance. At the same time, the construction and promotion of the internet financial security system can promote and strengthen the safety education and guidance of the public, especially financial consumers, integrate the internet and financial knowledge, improve the information security awareness of financial consumers, and promote the internet financial enterprises to improve service standardization and increase customer satisfaction.

7 Conclusion

This research will reduce the risk of client funds being stolen, client authentication and transaction authorization are operations performed by specialized equipment on the network. Additionally, internet banking usage is rigorously tested and they will do everything they can to ensure the safety of the customers. Of course, with the rapid development of information technology, there are also many hidden dangers, and the confidentiality of financial information is particularly important. With the development of science and technology, the means of stealing passwords are varied and very much disguised. Once the password is stolen, it will cause great harm. Therefore, confidentiality work faces many difficulties. Carrying out new technology research and development has always been the core task of confidentiality work, and only continuous innovation can make the confidentiality work stronger. With the vigorous promotion of online banking, many new network security technologies are gradually popularized and applied, such as password technology, firewall technology, identity authentication technology, virus defense technology, etc. Some emerging technologies should be perfected as soon as possible, such as network isolation and electronic authentication technology. In terms of hardware, China is relatively backward in the field of CPU development and operating system kernel technology research, and it should increase development efforts to shorten the gap as soon as possible. The standardization system has become the key and urgent need for the development of related technologies in the network industry, and it is also an important measure for the rapid development of Chinese's financial information technology.

Funding information: This work is not currently supported and funded by any funds.

Conﬁct of interest: These are no potential competing interests.

Data availability statement: Data sharing is not applicable to this article as no datasets were generated or analyzed during the current study.

References

[1] A. Asuan, “Transaksi perbankan melalui internet banking,” *Solusi*, vol. 17, no. 3, pp. 317–335, 2019.

[2] A. Mathew, “Threats and protection on e-sim,” *Int. J. Recent. Technol. Eng.*, vol. 9, no. 3, pp. 184–186, 2020.

[3] R. Lai, T. Wang, and Y. Z. Chen, “Using gridding symmetric encryption for location privacy protection,” *J. Commun.*, vol. 13, no. 11, pp. 673–678, 2018.

[4] D. Prokopowicz, S. Gwoździewicz, J. Grzegorek, and M. Matosek, “Determinants of the safety of the electronic daily transfer in the context of global trends on the internet development of the mobile banking,” *Int. J. N. Econ. Soc. Sci.*, vol. 7, no. 1, pp. 188–201, 2018.

[5] J. Zhou, Q. Wang, C. C. Hung, and F. Yang, “Credibilistic clustering algorithms via alternating cluster estimation,” *J. Intell. Manuf.*, vol. 28, no. 3, pp. 727–738, 2017.

[6] Japan, Advanced, Institute, et al., “Understanding Data through Clustering,” *J. Jpn. Soc. Fuzzy Theory Intell. Inform.*, vol. 17, no. 1, pp. 34–36, 2017.

[7] S. Hasheminejad and M. Khorrami, “Clustering of bank customers based on lifetime value using data mining methods,” *Intell. Decis. Technol.*, vol. 14, no. 4, pp. 507–515, 2020.

[8] M. A. Vahdatzad and H. K. Zare, “An evaluation method and clustering of credibly behavior of customers using AHP and fuzzy neural networks,” *J. Intell. Fuzzy Syst.*, vol. 35, no. 6, pp. 1–13, 2018.

[9] M. Negnevitsky, “Identification of failing banks using clustering with self-organising neural networks,” *Procedia Comput. Sci.*, vol. 108, pp. 1327–1333, 2017.

[10] I. R. Chuy, V. I. Kutsyk, and T. Y. Andreikiv, “The financial system modelling by various signs of clustering,” *Financ. Credit. Act. Probl. Theory Pract.*, vol. 2, no. 29, pp. 315–324, 2019.

[11] J. D. Wilson, Creating strategic value through financial technology, Wiley Finance Series, 2017, pp. 156–184.

[12] V. Shelmenkov, “Information security in remote banking,” *Proc. Inst. State Law RAS*, vol. 15, no. 3, pp. 188–204, 2020.

[13] X. Yuan, PhD forum: Deep learning-based real-time malware detection with multi-stage analysis, *IEEE International Conference on Smart Computing*, IEEE, 2017, pp. 1–2.

[14] K. Seon-Joo, "Passwordless protection for private key using USIM information," *J. Korea Contents Assoc.*, vol. 17, no. 6, pp. 32–38, 2017.

[15] L. O. Hariaha and R. R. Kulish, "Financial security of banking in a digitalized economy," *Probl. Econ.*, vol. 4, no. 42, pp. 163–171, 2019.

[16] B. M. Krishna, "Dynamically evolvable hardware-software co-design based crypto system through partial reconfiguration," *J. Theor. Appl. Inf. Technol.*, vol. 95, no. 10, pp. 2159–2169, 2017.

[17] S. U. Polycarp and U. M. Tanko, "Audit quality, political connection and investors protection and how they affect Nigeria firms performance," *J. Internet Bank. Commer.*, vol. 24, no. 3, pp. 1–20, 2019.

[18] A. A. Aryamov and Y. V. Gracheva, "Digitalization: Criminal law risks in the economy," *Actual. Probl. Russian Law*, vol. 6, pp. 108–116, 2019.

[19] K. Nur, A. Kumar, and M. Akhtaruzzaman, "A new approach to enhance internet banking security," *Int. J. Comput. Appl.*, vol. 160, no. 8, pp. 35–39, 2017.

[20] S. Ammirato, F. Sofo, A. M. Felicetti, and C. Raso, "The potential of IoT in redesigning the bank branch protection system: An Italian case study," *Bus. Process. Manag. J.*, vol. 25, no. 7, pp. 1441–1473, 2019.