Application Analysis of Information Security Technology in Credit Card System

Yuanyuan Sun[1(✉)] and Trini Canals[2]

[1] Pacific Credit Card Center of Bank of Communications, Hefei, Anhui, China
15004869@qq.com
[2] University of Frankfurt, Frankfurt, Germany

Abstract. With the continuous advancement of computer science and technology and internationalization, global competition has become increasingly fierce, especially in the banking industry. To maintain and improve their competitiveness in the market, various banks have expanded the scope and content of the banking industry under the background of continuous improvement of their operating environment, and have continuously adopted new information technologies. Currently, the bank's credit card system has become a place that every bank attaches great importance to. The credit card system will have an increasingly important impact on consumption concepts and customer living in the future development. It can be said that understanding the development of the credit card system will affect the future development of the bank to a certain extent. This article analyzes the application of information security in the credit card system. First, it uses the literature research method to summarize the problems in the credit card system and the information security elements of the development of the credit card system, and uses the questionnaire survey method for the application status of information security in the credit card system. According to the investigation, about 45% of the bank's credit card systems have information leakage problems, and about 26% of them have hacked attacks. For information leakage, banks must not only strengthen external management, but also deal with internal problems. Management also needs to be strengthened. Among the suggestions given, 42% of staff member chose to strengthen computer intrusion detection technology, and 32% chose to improve hardware equipment.

Keywords: Information security · Credit card system · Banking industry · Future development

1 Introduction

With the widespread application of information technology and the rapid development of information technology in the financial field, commercial banks increasingly rely on information technology [1, 2]. Today's world is in a new era of mobile Internet, smart phones, mobile terminals, and the Internet have become the basic elements of modern life [3, 4]. At present, our country has fully entered the era of Internet funds. The Internet has brought new technologies and new opportunities for commercial banks, and it has

I. Ahmad et al. (Eds.): STSIoT 2021, LNDECT 122, pp. 11–19, 2023.
https://doi.org/10.1007/978-981-19-3632-6_2

also brought greater financial risks and challenges to commercial banks [5, 6]. With the rapid growth of Internet financing, threats to the security of personal information and financial assets are increasing, and bank information security has become a major issue. Many factors affect the information security of commercial banks. Security incidents such as information leakage will cause serious consequences to customers and the bank itself. The lighter ones will affect the bank's customer satisfaction, the more serious ones will affect the bank's daily activities. Therefore, in recent years, domestic commercial banks have taken information security management research as a research hotspot and focus [7, 8].

In the research on the application and analysis of information security in the credit card system, many scholars have studied it and achieved good results. For example, Omelyanenko introduced the information security management ideas, management methods, and management content of my country's banking industry. It is believed that the banking industry should pay attention to the importance of information security management, make full use of information security technology, and establish a bank's information security management system [9]. Based on information security, Kachyn elaborated on the concepts, principles and methods of information security risk assessment and domestic information security related policies, and emphasized the importance of information security risk assessment in information security management [10]. Domestic research on information security management theories tends to focus on the summary analysis of foreign information security management theories or simply discuss the construction of information security systems from a certain aspect. There are relatively few systematic and comprehensive theoretical analyses. It is still in its infancy.

This paper analyzes the application of information security in the credit card system. First, it uses the literature research method to summarize the problems in the credit card system and the information security elements of the development of the credit card system, and uses the questionnaire survey method for the application status of information security in the credit card system.

2 Research on Information Security and Credit Card System

2.1 Research Methods

2.1.1 Literature Research

Reading books and articles about the application of information security in the credit card system in literature, the advantage is that you can understand the development process of the research object from the source, and understand the development status of the research object, and provide a clear and structured theoretical basis for in-depth thesis development.

2.1.2 Investigation and Research Method

The questionnaire survey method is that this article conducts a survey through pre-prepared questions and analyzes the answers of the interviewees to draw the necessary conclusions. By designing a questionnaire, it's objective to understand the status quo of the application of information security in the credit card system.

2.1.3 Quantitative Analysis

Qualitative analysis is related to quantitative analysis. Quantitative analysis refers to the analysis of mathematical hypothesis determination, data collection, analysis, and testing [11].

Qualitative analysis refers to the process of conducting research through research and bibliographic analysis based on subjective understanding and qualitative analysis [12].

2.2 Information Security Issues Faced by Credit Card Systems

2.2.1 Threats from the Internet System

The complexity of the Internet system provides a starting point for malicious behavior. To control the information security risks of Internet financing, the challenges they face include malware and phishing sites.

2.2.2 Security Threats to User Privacy

In the era of big data, the widespread popularity of cloud computing, Map-Reduce, No-SQL, and other technologies enables Internet companies to quickly, effectively pass the geographic location, IP address, and access device types left by customers when visiting websites. Browsing behavior, consumption behavior and other information on customers' consumption habits, interest preferences and other information. This residual information is stolen by criminals and poses a major threat to the credit card system.

2.2.3 Threats to the Availability of Network Platforms

Availability is an important guarantee for the development of financial platforms. Once the availability is restricted, it will cause huge losses. For example, in 2013, bank cash registers, ATMs and online banking services in many areas of the country failed and lasted for nearly 1.5 h. According to the information on the bank's homepage, e-banking transactions reached 170 trillion US dollars in the first half of this year. Following this estimate, a one-hour failure could result in at least 30 billion transaction losses. It can be seen that the availability of the platform is the foundation and guarantee for the development of Internet financial services.

2.2.4 Threats from Inside the Company

There are two main threats to the information security of credit card systems, one is from the outside in, and the other is from the inside out. Currently, most multi-service network security methods are aimed at external threats, and greater trust in internal servers often ignores internal management of business information security. Since internal personnel can easily receive various information within the company, it will lead to the leakage of key information and the violation of electronic contracts.

2.3 Information Security Elements of Credit Card System Development

2.3.1 From a Strategic Point of View, Give Full Attention to Information Security

Internet finance companies need to recognize the importance of information security to Internet finance companies, pay attention to strategic information security issues, and plan information security and financial security risk management as a whole. Not only need to strengthen network security protection, take measures at the level of security and communication protocols, and solve the security problems of the Internet itself through a variety of technical means, but also need to strengthen innovation at the business level following business rules and innovation. Risk control and paying attention to the characteristics of innovative business are key factors to develop a smart security strategy.

2.3.2 Seek Multi-party Cooperation to Jointly Build an Internet Financial Ecological Environment

From the perspective of the industry, the information security of Internet financial companies is by no means a problem of a certain company, but requires close collaboration across the industry; from the perspective of the Internet industry, information security issues require the cooperation of relevant parties. Only the government, enterprises, and users can work together to build a safe Internet financial ecological environment.

2.3.3 Carefully Protect the Privacy and Data of Users by Observing the Law and Self-Discipline

A large number of users is the foundation of the long-term effect of Internet financial products. If the security of users' personal information cannot be effectively ensured on the Internet financial platform, the reputation of the platform will be damaged, which will result in the loss of platform users. Therefore, ISPs must strictly abide by the basic information security rules for data storage and analysis, effectively protect customer privacy, and ensure the security of users' private data.

2.3.4 Integrate Multiple Channels to Enhance User Information Security Training

Insufficient user security awareness is an important reason for information security risks. The dissemination and education of user information security awareness cannot be based solely on social resources. Internet finance companies need to be fully aware of the importance of publicizing and disseminating information security to users, integrate publicity and information security dissemination into product design, and accept general

evaluation. Provide users with financial risk tips and information security training, and emphasize the importance of information security issues to users in various ways, so that users can carefully develop the habit of paying attention to information security when using credit card system applications.

2.4 Information Security Data Evaluation Model

2.4.1 Establish a Judgment Matrix

Drawing out the target elements at each level and clarifying the relationship between them, we successfully established an interrelated hierarchical structure. Assume that the set consisting of n elements A1, A2, …, An corresponds to the corresponding criterion B. To obtain the model of the judgment matrix, it is necessary to pass the criterion of the upper layer as the calculation and derivation criterion. Under the guidance of the criterion, it is determined by comparing the n elements with each other.

2.4.2 Calculate the Product Mi of Each Row Element of the Matrix

Calculate M_i the power root of W_iˆ0

$$W_i^0 = \left(\prod_{j=1}^{n} a_{ij} \right)^{\frac{1}{n}} \ldots \mathrm{i} = 1, 2, \ldots\ldots \mathrm{n} \tag{1}$$

2.4.3 Normalize the Vector

$$W_i^0 = \frac{W_i^0}{\sum_{i=1}^{n} w_i^0} \ldots \mathrm{i} = 1, 2, \ldots\ldots \mathrm{n} \tag{2}$$

3 Investigation on the Status Quo of the Application of Information Security in the Credit Card System

3.1 Research Purpose

Investigate the application status of information security in the credit card system through the questionnaire survey method, and give corresponding suggestions based on the problems in the existing credit card system of the respondents, and analyze the measures that should be taken for information security based on the results.

3.2 Questionnaire Survey

3.2.1 Number of Questionnaires

According to the minimum sample size formula in statistics, the author sets the confidence level of the questionnaire to 8%, and the allowable error does not exceed 8%. Calculate the minimum sample size as

$$n_0 = \left(\frac{t_a}{2\Delta p}\right)^2 = \left(\frac{1.645}{2 \times 0.075}\right)^2 = 120 \tag{3}$$

That is, the minimum sample size of this questionnaire is 120 copies.

3.2.2 Data Source

This paper investigates the credit card system and the limited scope in the banking industry. Therefore, three banks in this city are randomly selected to be replaced by Bank A, Bank B, and Bank C. According to the minimum number of questionnaires, the number of questionnaires distributed by the three banks is respectively: 40, 50, 60, the number of questionnaires returned is 39, 49, 60.

4 Data Analysis

4.1 Investigation of Problems in the Credit Card System

This article uses a questionnaire survey method to investigate the problems of the bank's credit card system. The results of the survey are shown in Table 1.

Table 1. There is a problem with the credit card system

	A bank	B bank	C bank
Hacker attack	26%	25%	28%
Information leakage	45%	47%	46%
Data is changed	19%	18%	16%

As can be seen from Fig. 1, among the problems in the bank's credit card system, about 45% of the information leakage problems occurred, and about 26% of the problems occurred with hacker attacks. Regarding information leakage, banks must not only strengthen external management, but also strengthen internal management.

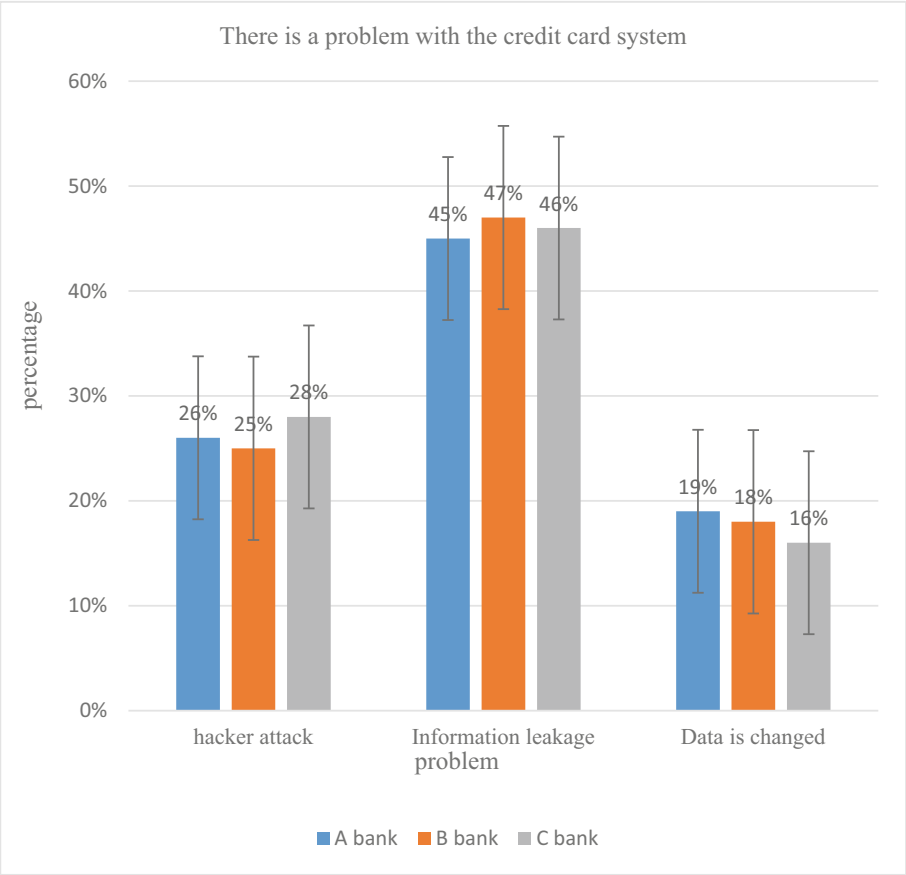

Fig. 1. There is a problem with the credit card system

4.2 Relevant Suggestions for Problems

This article uses a questionnaire survey method to investigate the problems that occur in the bank's credit card system. The results of the survey are shown in Table 2.

Table 2. Suggestions for problems

	A bank	B bank	C bank
Strengthen computer intrusion detection Application of measurement technology	40%	44%	42%
Improve hardware quality	30%	32%	34%
Database management security	30%	24%	24%

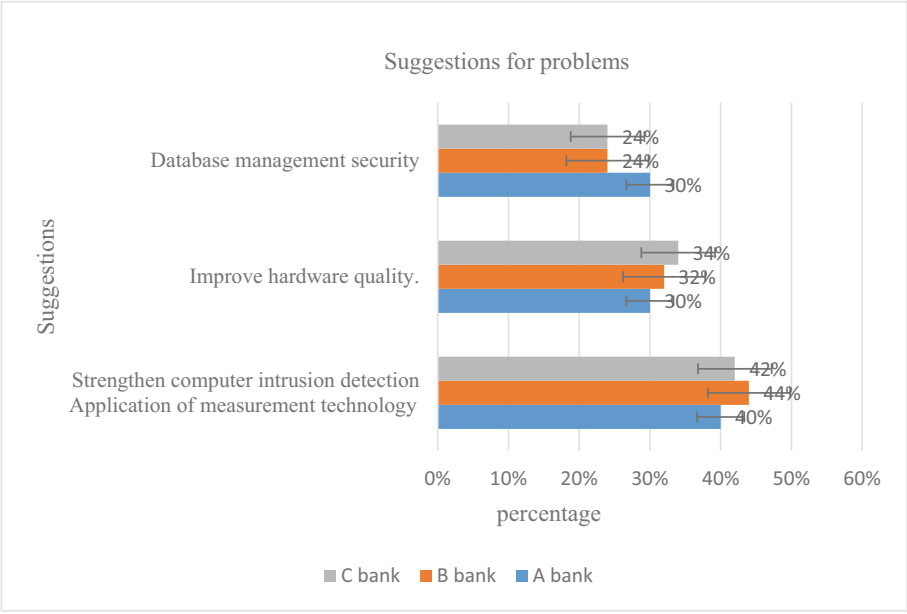

Fig. 2. Suggestions for problems

It can be seen from Fig. 2 that among the suggestions given, 42% of people choose to strengthen computer intrusion detection technology, and 32% of people choose to improve hardware equipment.

5 Conclusion

In recent years, with the rapid development of the mobile phone industry, many traditional industries have gradually changed. Funds were initially used as equivalent means of exchange. Due to economic globalization, the single economy has gradually integrated into the global environment. The bank credit card system is constantly evolving. With changes in consumer perceptions, credit cards have begun to grow in China. With the continuous development and growth of credit card sales, information security is an important guarantee for the credit card system. It can be seen from the survey results of this article that, first, among the problems in the bank credit card system, about 45% of the information leakage problems occurred, and about 26% of the problems occurred with hacker attacks. Second, among the suggestions given, 42% of people choose to strengthen computer intrusion detection technology, and 32% of people choose to improve hardware equipment. What's more, the internal management system of the bank should also be paid attention to. The user's information can be viewed and should be authorized.

References

1. Hao, S., Lü, Y., Jie, L., Yue, L., Xu, D.: Application of classified protection of information security in the information system of air pollution and health impact monitoring. Wei Sheng Yan Jiu J. Hygiene Res. **47**(1), 103–107 (2018)
2. Yong, Q.L.: Application analysis of artificial intelligence in library network security. J. Phys. Conf. Ser. **1744**(3), 032024 (7 pp) (2021)
3. Triana, Y.S., Pangabean, R. Risk analysis in the application of financore information systems using FMEA method. J. Phys. Conf. Ser. **1751**(1), 012032 (10pp) (2021)
4. Kim, S.B., Min, G.K., Park, J.H.: Simple credit card payment protocols based on SSL and passwords. J. Korea Inst. Inf. Sec. Cryptol. **26**(3), 563–572 (2016)
5. Khabarlak, K., Koriashkina, L.: Mobile access control system based on RFID tags and facial information. Bull. Nat. Tech. Univ. KhPI Ser. Syst. Anal. Control Inf. Technol. **2**(4), 69–74 (2021)
6. Demeshko, V.S.: Application of convolutional neural networks in the intelligence security system subsystem. Syst. Anal. Appl. Inf. Sci. **2**, 46–53 (2020)
7. Li, Y., Lu, Y.: Multimodality data analysis in information security ETCC: encrypted two-label classification using CNN. Sec. Commun. Netw. **4**, 1–11 (2021)
8. Borisova, D.E.: Improvement of wage system in health care as a factor in increasing the economic security of the region. Econ. Prof. Bus. **4**, 34–39 (2020)
9. Omelyanenko, V.: Analysis of information asymmetry in innovation system security ensuring. Mark. Manag. Innov. **4**, 199–208 (2017)
10. Kachynskyi, A.B., Styopochkina, I.S.: A systematic approach to the analysis of phenomena of the information and cyberspaces. Reports of the National Academy of Sciences of Ukraine (11), pp.16–23 (2020)
11. Cheng, L.I., Wang, J.J.: Quantitative and qualitative analysis of student tutors as near-peer teachers in the gross anatomy course. Ann. Anat. **210**(2), 147–154 (2017)
12. Maragkaki, A.E., Kotrotsios, T., Samaras, P., Manou, A., Lasaridi, K., Manios, T.: Quantitative and qualitative analysis of biomass from agro-industrial processes in the central macedonia region, Greece. Waste Biomass Valori. **7**(2), 383–395 (2016)