Three-dimensional Construction of Financial Technology Security: Risk Dimension Analysis, Protection Mechanism Design, and Governance System

Xitao Jiang*

School of Applied Economics, Guizhou University of Finance and Economics, Guizhou, China

*Corresponding author: busheng55@gmail.com

Abstract. With the rapid development of information technology and the widespread application of emerging technologies such as big data in the financial sector, FinTech has become a core force driving transformation in the financial industry. However, technological innovation is often a double-edged sword. Severe challenges to information security have also accompanied the widespread adoption of FinTech. Frequent security incidents, such as data leaks and cyberattacks, pose a serious threat to the operations of financial institutions and erode customer trust, making FinTech security increasingly crucial. This article constructs a three-dimensional framework for FinTech security, encompassing "risk-protection-governance," and systematically examines its core issues. First, it analyzes the cross-layer coupling risks of the technology, data, and application layers. Secondly, it constructs a protection mechanism encompassing zero-trust architecture, privacy-preserving computing, and a secure development lifecycle, focusing on technical defense, institutional norms, and end-to-end management. Finally, it proposes a governance system that incorporates penetrating supervision, sandbox optimization, the application of regulatory technology, and collaborative governance across the government, industry, and society. This research demonstrates the need for dynamic FinTech security prevention and control through a collaborative "technology-process-institutional" approach and multi-faceted governan ce, providing theoretical and practical support for the secure development of digital finance.

Keywords: Financial data security; financial technology security; protection mechanisms; governance systems.

1. Introduction

When the penetration rate of mobile payment exceeds 80%, the asset scale of smart investment advisors managed exceeds trillions of US dollars, and blockchain cross-border payments achieve instant settlement, financial technology has been upgraded from "technical supplement" to the "infrastructure" of the global financial system. However, behind the carnival given by technology, security risks are spreading in more complex forms. Various cases in reality reveal that financial technology security is no longer a single technical issue, but a systemic challenge related to financial consumer rights, market order, and even national financial security.

The academic community's attention to financial technology security stems from the disruptive impact of digital technology on traditional financial theories. Early research focused more on single risk prevention and control, such as cyber attack defense or data encryption technology, but ignored the coupling effect of technology-level vulnerabilities, data-level abuse, and application-level risks. The lack of an interdisciplinary perspective has also led to the separation of theories of law, computer science, and financial supervision. In recent years, although some scholars have explored the coordination between technology and supervision, there is still a lack of systematic explanation of the dynamic mechanism of "risk evolution-protection response-governance adaptation", and it is difficult to cope with the core contradiction of "technical iteration faster than rule updates" in financial technology.

This study is based on the three-dimensional framework of "risk-protection-governance", and systematically analyzes the risk dimensions of financial technology security technology technology layer, data layer, and application layer; builds a protection system that includes technical protection

such as zero-trust architecture, privacy computing, and other institutional norms, as well as security development life cycle, algorithm auditing and other institutional norms; explores innovative paths for penetrating supervision and collaborative governance of multiple subjects.

2. Core Risk Dimensions of Fintech Security

As FinTech reshapes financial services, its security risks are not limited to single-dimensional technical vulnerabilities or operational errors, but rather present a complex, multi-layered, cross-domain nature. From the technical foundation to data flow and end-user applications, risks are embedded in various forms throughout the FinTech chain. The technical layer, as the "skeleton" supporting financial innovation, faces inherent vulnerabilities and external attacks that directly threaten the underlying security of the system. The data layer, as the "blood" driving financial decision-making, faces potential privacy risks and decision-making biases due to its leaks, misuse, or quality defects. The application layer, as the "interface" connecting users and services, faces increased risk transmission due to the complexity of business scenarios and third-party connections. These three core risk dimensions are both relatively independent and interconnected, collectively constituting a systemic challenge to FinTech security that requires a holistic approach to analysis and response.

2.1. Core Risk Dimensions of the Technical Layer

As the foundation for the operation of financial technology, the technical layer has risks that cannot be ignored. On the one hand, emerging technologies have vulnerabilities themselves, and their consensus mechanisms may have defects. Some consensus algorithms are difficult to ensure the consistency and security of transactions when facing a large number of malicious attacks on nodes [1]. On the other hand, network infrastructure is threatened. Financial technology is highly dependent on the network to transmit data and process business. Distributed denial of service attacks can overload the servers of financial platforms and prevent them from providing services normally. Advanced persistent threat attacks are characterized by strong concealment and long duration. Hackers can use these attacks to steal core technical data and sensitive information, causing serious harm to financial institutions. Based on distributed denial of service attacks, by analyzing network traffic characteristics in real time, attack behaviors can be quickly identified, and traffic cleaning mechanisms can be triggered. At the same time, distributed defense architectures are explored to disperse attack pressure [2]. Based on the concealment of advanced persistent threat attacks, scholars have developed a traceability system based on big data. By correlating and analyzing long-term network logs and terminal behavior data, they can identify the latent stages in the attack chain and use threat intelligence libraries to provide early warnings of potential attack paths [3].

2.2. Core Risk Dimensions of the Data Layer

Existing research shows that data is a core resource for the development of financial technology, and its security is crucial. Data leakage is one of the main risks. Financial institutions and technology companies store a large amount of sensitive data, such as personal identity information, account information, and transaction records. Once leaked, it may be used by criminals for illegal activities such as fraud and money laundering, seriously infringing on user rights. Data compliance risks are also becoming increasingly prominent. Different countries and regions have different regulations on cross-border data flow and data storage. In addition, data quality risks can affect the accuracy of financial technology applications. Data contamination and sample bias may cause intelligent risk control models to misjudge, increasing the credit risk of financial institutions. Currently, academic research to address data risks is mainly divided into three parts: research on protection against data leakage risks, research on governance of data compliance risks, and research on optimization of data quality risks.

First, research on data leakage risk prevention involves establishing technical privacy protection solutions, including federated learning, homomorphic encryption, differential privacy, etc., to reduce

data exposure risks at the source [4]. Second, research on data compliance risks focuses on the balance between data sovereignty and cross-border efficiency, and proposes hierarchical and classified cross-border rules. For highly sensitive data, a "local storage + authorized outbound" model is implemented, while for low-sensitivity data, cross-border processes are simplified [5]. Finally, research on data quality risk optimization involves designing intelligent cleaning algorithms to identify outliers, duplicate data, and logical conflicts through machine learning, and automatically correct or mark problematic data.

2.3. Core Risk Dimensions of the Application Layer

The academic community has developed multi-dimensional research results on the solutions to these risks, such as the prevention and control of business scenario risks, risk management through mobile payments and smart investment advisors, and risk isolation of cross-border financial products. The former research proposes an identity verification solution based on multi-factor authentication, combining biometrics, device fingerprints, and dynamic verification codes to improve the security of account login and transactions; it develops a real-time transaction monitoring system, analyzes user behavior characteristics through machine learning, identifies abnormal transactions, and triggers interception mechanisms [6]. The latter uses AI-driven exchange rate risk models to adjust hedging tools in real time to reduce the impact of exchange rate fluctuations on product returns, and uses the cross-border business traceability system of blockchain to record the entire process of product design, sales, and redemption to ensure compliance with regulatory requirements in different regions.

In the research on the collaborative prevention and control of third-party dependency risks, it is shown that the construction of a third-party management system of "risk rating-access review-continuous monitoring" can clarify the security responsibility boundaries of the two parties through smart contracts, stipulate the scope of data sharing, risk event response time limit and compensation mechanism, and reduce the shirking of responsibility [7]. At the same time, a "circuit breaker mechanism" is designed to automatically cut off the interface connection with the financial platform when a major security incident occurs in the third party to prevent the spread of risks. In the forward-looking prevention and control research on the application risks of emerging technologies, scholars proposed a "digital asset ownership and custody" mechanism. Based on the unique characteristics of non-homogeneous tokens, the ownership of virtual assets is anchored, combined with the custody services of licensed institutions, and the compliance of asset registration, trading, and liquidation is achieved, and an anti-money laundering monitoring model for virtual assets is constructed. By analyzing the transfer path and counterparties of virtual assets, money laundering, illegal fundraising, and other behaviors can be identified.

3. Security Protection Mechanism of Financial Technology

Faced with the intertwined and overlapping security risks of FinTech at the technical, data, and application levels, relying solely on fragmented defenses is no longer an effective barrier. Building a systematic, comprehensive security protection mechanism has become an inevitable choice. This mechanism must be rooted in technological innovation, using cutting-edge technologies to address inherent vulnerabilities at the technical level; it must also rely on a framework of institutional norms, solidifying protection logic through standardized processes and rigid constraints; and it must permeate the entire product lifecycle, from design to operation and maintenance, to achieve proactive risk prevention and dynamic response. Only by organically integrating the "hard power" of technological defense, the "soft power" of institutional norms, and the "resilience" of full-process management can it build a multi-layered, complex defense dam for the safe development of FinTech, effectively resisting the penetration and impact of various risks.

3.1. From"Problem-Oriented" to"Mechanism Design"

The proposal of technical protection mechanisms stems from a systematic understanding of the particularity of financial technology risks. The academic community has designed targeted defense solutions by disassembling the manifestation and transmission logic of risks. In the exploration of "vulnerability response" for technical risks, facing technical risks such as defects in the blockchain consensus mechanism and distributed denial of service attacks, early research focused on patching single-point vulnerabilities. However, with the advancement of the times, the means of attack have also been upgraded. Scholars have found that a single technology is difficult to deal with, and thus proposed the idea of "active defense + dynamic adaptation". For example, for the traffic characteristics of distributed denial of service attacks, it can analyze the temporal and spatial characteristics of attack samples and then develop relevant intelligent detection models [8]. In response to the repeated occurrence of blockchain smart contract vulnerabilities, it should combine formal verification tools with the security development lifecycle to embed vulnerability defense into the entire development process [9].

Early data security research focused on storage encryption and access control, but this failed to meet the needs of cross-institutional collaboration. This led to the exploration of privacy-preserving computing technologies. Federated learning achieves "data remains static, model remains dynamic" through distributed modeling. The optimization of its parameter update mechanism aims to balance model accuracy with privacy leakage. Homomorphic encryption addresses the pain point of "encrypted data cannot be computed" by enabling direct computation on ciphertext through algebraic structure design, adapting to data collaboration scenarios in cross-border payments. The exploration of "scenario-adaptive" approaches to application-layer risks has prompted a shift in research from general-purpose defenses to specific scenarios.

3.2. From "Reactive Patching" to "Proactive Building"

The introduction of protection mechanisms relies heavily on the support of technological development, and also promotes the transformation of defense logic from "post-event remediation" to "full life cycle prevention and control". The introduction of AI intrusion detection systems stems from the ability of machine learning to analyze complex data. By learning financial transaction time series data using long-short-term memory recursive neural networks, it can accurately identify the latent characteristics of advanced persistent threat attacks [10]. The implementation of zero-trust architecture relies on the development of cloud computing and micro-isolation technology to achieve real-time verification and dynamic authorization of each access request, breaking through the traditional "internal and external network boundary" defense limitations. Early protection research focused on "post-launch defense", but the risks of financial technology products are constantly changing, so it is necessary to plan. The academic community has found through analysis of a large number of security incidents that more than 70% of risks are caused by defects in the design and development stages. Therefore, security should be embedded in the entire process of demand analysis, design, development, testing, operation, and maintenance to form a risk prevention and control logic.

3.3. From "Technology Islands" to "Collaborative Governance"

Improvements to protection mechanisms also stem from an understanding of the limitations of technical defenses. Technical measures alone cannot resolve compliance and accountability issues; they must be integrated with institutional norms to form a closed loop. The frequent occurrence of risks such as cross-border data flow conflicts and algorithmic discrimination has exposed the shortcomings of technical defenses in terms of compliance. By comparing the General Data Protection Regulation (GDPR) and China's Data Security Law, academics have proposed a standard combining "data classification and categorization with differentiated protection." To address the issue of algorithmic black boxes, based on the theory of algorithm transparency, a filing and auditing system has been designed, requiring robo-advisors to disclose model logic and decision-making basis, translating technical indicators into institutional requirements. A systematic emergency response

system is being designed, as the emergency response capabilities of a single institution are inherently insufficient.

Therefore, a comprehensive "detection-isolation-tracing-recovery" mechanism is needed. Research has found that the extent of damage from security incidents is negatively correlated with the level of system integrity. Therefore, technical solutions such as blockchain log tracing, risk mitigation through honeypot systems, and rapid recovery through multi-cloud architectures have been proposed. These solutions, combined with institutional designs such as vulnerability disclosure rewards and third-party emergency support, form a robust response system.

4. Fintech Governance System

4.1. Innovative Regulatory Models Overcome the Adaptability Bottlenecks of Traditional Regulation

Fintech regulatory needs can be addressed through three key approaches: penetrating supervision, sandbox optimization, and the application of regulatory technology. To address the issue of fintech products obscuring their underlying business essence through technological packaging, a research study proposes a "penetrating supervision" framework. By deconstructing the product's business logic and technical architecture, this framework identifies inherent risk attributes and aligns them with corresponding regulatory rules. Furthermore, academic research on sandbox regulation has refined this approach. First, during the entry phase, an "innovation-risk level" assessment matrix is constructed. This matrix uses quantitative indicators such as technological originality and user impact to screen suitable products for testing, preventing low-value innovation from hoarding resources. Secondly, a "dynamic risk threshold" mechanism is designed for the testing phase. This mechanism adjusts the testing scope based on real-time data such as user complaint rates and system failure rates, triggering a pause or exit when the risk threshold is exceeded. Finally, during the exit phase, test results are converted into algorithm model security parameters based on sandbox graduation criteria, ensuring a smooth transition to full-scale operations.

4.2. Improve the Collaborative Governance of Multiple Entities and Build a "Government-industry-society" Linkage Network

Given the cross-industry and cross-regional nature of FinTech, a governance system can be established from three perspectives: government regulation, industry self-regulation, and public oversight. First, at the government oversight level, the proposed "regulatory collaboration platform" should integrate regulatory data from the central bank, the Cyberspace Administration of China, and financial regulatory authorities, establishing a "data sharing-risk consultation-joint response" process to mitigate the limitations of single-department decision-making. Secondly, at the industry self-regulation level, academic insights could be used to help industry associations develop self-regulatory standards, such as security capability assessment standards for FinTech companies and entry barriers for third-party service providers. Simultaneously, a "threat intelligence alliance" based on federated learning could be established, allowing companies to share attack signatures without leaking sensitive data, thereby forming an industry-wide risk warning network. Finally, at the public oversight level, a "security vulnerability bounty" mechanism could be designed to encourage users to report product security issues through financial incentives, and a tiered vulnerability response process could be established, including a 24-hour response to high-risk vulnerabilities. Furthermore, third-party institutions could be brought in to rate the security governance capabilities of FinTech companies, linking the ratings to market access and consumer choices to create a "reputational constraint" mechanism.

5. Conclusion

This article systematically examines the core issues in the FinTech security field by constructing a three-dimensional framework of "risk-protection-governance," reaching the following conclusions. First, FinTech security risks evolve through a cross-layer coupling of "technology-data-application." Vulnerabilities at the technical layer can be transmitted to the application layer through data flows, and new application scenarios can, in turn, give rise to new technological risks. Single-dimensional risk control is inadequate to address systemic challenges and cannot be a one-size-fits-all approach. Second, protection mechanisms must achieve a coordinated "technology-process-system" approach. Effective protection relies on technological innovation to address technical vulnerabilities, proactively addressing risks throughout the security development lifecycle, and solidifying protection logic through institutional norms. The integration of these three elements can both address real-time risks and adapt to long-term technological iterations. Third, the multifaceted and coordinated governance system will become inevitable. The cross-domain nature of FinTech requires a shift away from traditional regulatory models. Penetrating supervision can address the problem of "regulatory arbitrage disguised as technology," sandbox regulation can balance innovation and risk, and RegTech improves regulatory efficiency. Furthermore, a collaborative network of "government-industry-society" further expands the scope of governance and fosters a synergistic governance force.

The core of FinTech security lies in building a dynamic system that ensures identifiable risks, adaptable protection, and coordinated governance. As the times evolve, the future will see more advanced technologies, more application scenarios, and more security challenges. Research on the deep integration of technology and finance must continue to break through disciplinary barriers, requiring constant updates and balancing technical feasibility with social value, providing theoretical and practical support for the secure and sustainable development of industries like digital finance and FinTech.

References

[1] Hu T Y. Research on smart contract security defect detection technology. Southeast University, 2024.

[2] Li C H. Research on distributed denial of service attack detection and optimization method based on MSCNN-BiGRU-SHA. Institute of Disaster Prevention Science and Technology, 2025.

[3] Liao W H. Real-time intrusion detection and investigation based on host traceability graph. University of Electronic Science and Technology of China, 2025.

[4] Chen Y S. Design and implementation of a data leakage protection system based on content audit. Shandong University, 2020.

[5] Wang X. Research on legal issues of cross-border electronic data forensics. Liaoning University, 2024.

[6] Zhu J M. Research on the optimization of international business risk management of commercial banks. Inner Mongolia University of Finance and Economics, 2025.

[7] Zhou Q. Financial technology innovation under third-party participation: research on the game between new and regulatory. Hunan University, 2022.

[8] Li C H. Research on distributed denial of service attack detection and optimization method based on MSCNN-BiGRU-SHA. College of Disaster Prevention Science and Technology, 2025.

[9] Dong C Y. Research on formal verification method of blockchain smart contract. Sichuan Normal University, 2021.

[10] Liao W H. Real-time intrusion detection and investigation based on host tracing graph. University of Electronic Science and Technology of China, 2025.