Proceedings of the 2nd International Conference on Financial Technology and Business Analysis
DOI: 10.54254/2754-1169/46/20230315

The Influence of Fintech on Network Security and Regulatory Countermeasures

Zixuan Cui[1,a,*]

[1]*McMaster University, Hamilton, Ontario, Canada, L8S 4L8*
a. cuiz21@outlook.com
**corresponding author*

Abstract: In recent years, with the continuous development and innovation of fintech, it also has a series of impacts on network security. This paper uses the literature review method to study the influence of fintech on financial industry network security and regulatory countermeasures. In the aspect of impact analysis, this paper first discusses the data security and algorithm risks brought by the extensive application of artificial intelligence. Secondly, the use of big data technology may lead to the risk of data leakage and abuse. Finally, lagging regulatory policies may increase security risks in the financial sector. In response to these impacts, this paper proposes four regulatory policies, such as strengthening data security and privacy protection, strengthening management efforts, balancing the relationship between innovation and risk, and introducing relevant policies. The study believes that effective regulatory measures can deal with the security challenges in the development of fintech, and ensure the stability of the financial system and the rights and interests of users.

Keywords: fintech, network security, financial supervision, risk management, financial industry

1. Introduction

The rapid development and innovation of fintech, not only brings business upgrading to financial institutions and practical convenience to consumers, but also brings economic benefits and technological progress to technology enterprises. However, along with these advances, the emergence of fintech has raised concerns about the security and integrity of the financial system, and faced new risk challenges and regulatory challenges. This study explores the impact of fintech on network security and proposes regulatory measures to address related risks. In reviewing the existing literature, most research subjects focus on topics such as data security, fraud prevention, and regulatory challenges, while this study specifically examines the combined impact of fintech on cybersecurity and proposes targeted regulatory measures.

The research methodology used in this study included a literature review that examined some representative academic articles, research papers, and industry reports. This study explores several key research areas, including the risks introduced by AI in fintech, vulnerabilities associated with the use of big data, and the impact of regulatory policies on cybersecurity in the context of fintech. By analyzing and synthesizing the results of relevant research, this study contributes to a better understanding of the relationship between fintech and cybersecurity.

DOI: 10.54254/2754-1169/46/20230315

The significance of this study lies in its contribution to the field of fintech and cyber security. By integrating existing research and addressing identified risks and challenges, this study can provide valuable insights for policy makers, financial institutions and researchers. The findings can enhance understanding of the potential risks associated with the adoption of fintech and help stakeholders develop sound cybersecurity strategies and frameworks. In addition, the results of this study can contribute to the academic community by broadening the knowledge base and contributing to this evolving field and further research.

2. Analysis of the Impact of Fintech on Financial Industry Network Security

2.1. Risks Arising from Artificial Intelligence

First, the inaccuracy and bias of AI algorithms may negatively impact the security of financial institutions and users. Artificial intelligence model requires a large amount of data for training. If the training data is incomplete, inaccurate or biased, then the prediction results of the model will be wrong or biased. For example, since the consumption quota and total income of women are lower than that of men in historical data, the credit limit evaluation algorithm trained according to historical data shows gender discrimination in operation. Even though women have higher credit scores, they receive only one-tenth or one-twentieth of the credit lines of men in their families [1]. In the financial sector, it can lead to faulty risk assessments, poor investment decisions, and discriminatory loan approvals to the detriment of the financial system and its users.

Secondly, artificial intelligence algorithm has a strong black-box property. Complex architecture, and superior performance of machine learning especially deep learning algorithm is widely used in the financial field [1]. However, because the latter is a nonlinear algorithm, the unexplainable problem cannot be solved technically. Therefore, the working principle of some AI algorithms is difficult to explain, which makes it difficult to detect their potential security vulnerabilities. Malicious attackers can take advantage of this opacity to circumvent security measures through targeted attacks, for example, by manipulating data and making small changes to it to cause the AI model to make bad decisions. The increase in these instability factors will seriously affect financial security. The following chart depicts the risks posed by artificial intelligence to fintech.

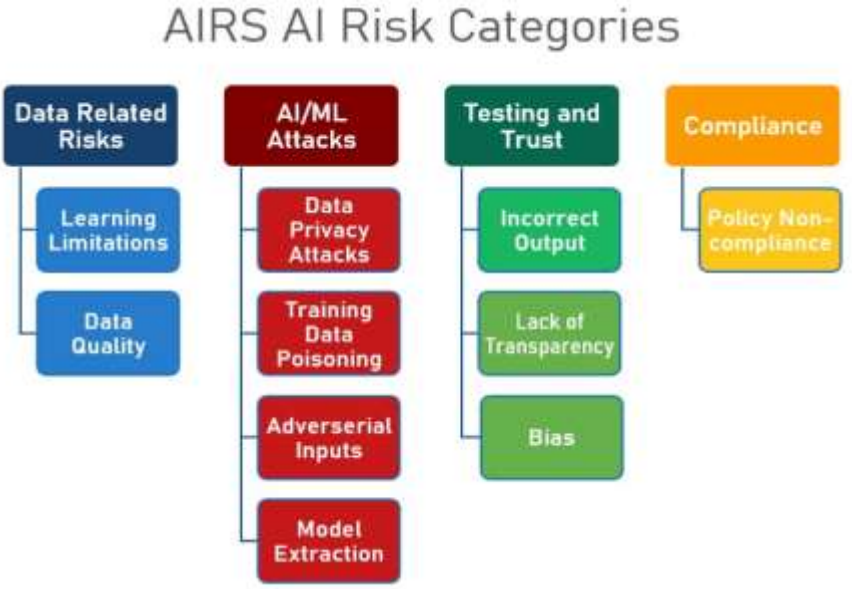

Figure 1: Artificial Intelligence Risk & Governance-AIRS AI Risk Categories [2].

DOI: 10.54254/2754-1169/46/20230315

2.2. Risks Associated with the Use of Big Data

The development of fintech enables financial institutions to collect and process large amounts of data, but the use of big data also brings some cybersecurity risks. As an important part of the Internet governance system, data security and privacy protection have become one of the main bottlenecks restricting the development of big data applications. One party's financial data also affects the privacy of the other party's financial data, which makes the protection of multi-source financial data privacy more challenging [3].

Figure 2: How You Can Apply Big Data to Risk Management [4].

First of all, the storage and processing of big data require a high level of data security protection, because big data collections include a large amount of sensitive personal and financial information. If these data storage and processing systems have loopholes or improper security control measures, it will lead to user privacy disclosure and financial fraud and other problems. Second, big data systems may face risks to data integrity. Financial institutions may need to share data to improve risk assessment and customer service. However, data can be tampered with and corrupted during collection, storage, processing, and sharing. Improper security control or inadequate protection may lead to the risk of data leakage. In addition, there is the risk of data abuse. Fintech companies analyze big data to obtain information such as customer behavior patterns and preferences in order to provide more personalized financial products and services. However, if big data is misused, it will violate the privacy of customers and cause legal disputes.

2.3. The Challenge of Regulatory Policies

The development of fintech also brings risks and challenges in terms of regulatory policy. First, regulators need to keep up with the rapid development of fintech and formulate corresponding regulatory policies and regulations in a timely manner. However, due to the rapid development of fintech, regulators may not be able to keep up with changes and innovations in technology in a timely manner, which may result in regulatory policies lagging behind the development of fintech and failing to effectively regulate emerging fintech businesses. Secondly, the inconsistency and difference in regulatory policies may also lead to risks. Regulation is further complicated by the cross-border business and data flows of fintech. However, different countries and regions have different regulatory standards and policies, such as requirements for data privacy protection and regulatory standards for fintech companies, which may cause financial institutions to face inconsistent regulatory

DOI: 10.54254/2754-1169/46/20230315

requirements and lead to regulatory loopholes. In addition, fintech innovation involves cutting-edge high-tech, supported by big data, cloud computing, artificial intelligence, blockchain and other technologies. The traditional financial supervision model may be difficult to cope with the new characteristics of new technologies and risks, so higher requirements are put forward for the technical resources, supervision methods and supervision ability of regulatory institutions [5].

Figure 3: Your trusted resource for compliance management [6].

3. Financial Industry Network Security Supervision Countermeasures under the Background of Fintech

3.1. Strengthen Data Security and Privacy Protection

Financial institutions and regulators should establish a perfect data security protection system, including ensuring the security of data storage and processing systems, using encryption technology, access control and identity authentication measures to protect the confidentiality and integrity of data. At the same time, they need to conduct regular security vulnerability scanning and risk assessment, timely repair vulnerabilities and strengthen security protection measures. Moreover, financial institutions and regulators should develop clear privacy policies and management methods for data sharing between companies, and clarify the scope and protection requirements of data sharing under different business models and application scenarios [7]. The important point is that users should have the right to choose whether or not to share personal information and be able to understand how other information is used and protected.

3.2. Strengthen Management

Regulators need to step up their management of fintech companies and financial institutions, including strengthening regulatory requirements, strengthening scrutiny and monitoring, and developing penalties. First, regulators can set stricter cybersecurity and data protection requirements, and require financial institutions to establish complete security management systems. Second, regulators should strengthen the examination and monitoring of financial institutions and ensure their compliance operations. Only by adhering to the principle of consistency can fair competition be maintained. Institutions and platforms can carry out financial business only after obtaining permission

DOI: 10.54254/2754-1169/46/20230315

from the regulatory authorities [8]. In addition, regulators should formulate clear punishment mechanisms for violations to play a supervisory role, including fines and license suspensions.

3.3. Balance the Relationship between Innovation and Risk

First, regulators should establish a regulatory framework for innovation and actively support the innovative development of fintech. For example, regulators can encourage financial institutions to adopt advanced technologies and models to improve the efficiency and user experience of financial services. However, along with innovation, regulators also need to require companies to be able to monitor cybersecurity risks in real-time and implement risk management measures for new technologies and business models [7]. In addition, regulators can establish cooperation mechanisms with financial institutions to provide guidance and cooperation to help financial institutions cope with cybersecurity risks brought by innovation.

3.4. Enact Relevant Policies

In order to effectively regulate cybersecurity in the fintech sector, regulators need to formulate relevant policies and regulations according to the development trend and characteristics of fintech. Regulators can issue special cyber security laws and regulations to regulate the operation and management of fintech business. Second, regulators should work closely with financial institutions, technology companies and research institutions to jointly develop cybersecurity policies and standards in the fintech sector, such as establishing management systems, adhering to credit review, and risk control [9]. In addition, regulators can cooperate with international organizations and regulators in other countries to enhance international cooperation and information sharing.

4. Conclusions

In conclusion, the rapid development and innovation of fintech also have an impact on cyber security. The research conclusion of this paper is that in the context of fintech, the financial industry network security regulation needs to strengthen data security and privacy protection, strengthen management efforts, balance the relationship between innovation and risk, and introduce relevant policies. However, there are some shortcomings in this study. First of all, this paper mainly analyzes and summarizes based on theories and existing literature, so there is a lack of empirical investigation to support the reliability and validity of the conclusion. Moreover, the focus of this study is the regulatory countermeasures of fintech network security, so it has not been discussed in the aspects of technology development trends and market competition. In future studies, more empirical investigations will be carried out, and relevant data will be collected and made into charts to support the research conclusions. Also, future studies will further expand their scope to include more fintech fields and related regulatory issues to further enhance the cybersecurity capabilities of the financial industry.

References

[1] *Risk Types and Regulatory Schemes for Financial Applications of Artificial Intelligence Algorithms – Security Insights | Decision makers' Network Security Knowledge Base (2023). https://www.secrss.com/articles/45889*

[2] *Artificial Intelligence Risk & Governance – AI Risks and Risk Categorization (2023).https://aiab.wharton.upenn.edu/research/artificial-intelligence-risk-governance/*

[3] *Typical Facts and Regular Pattern of Artificial Intelligence in Financial Technology - Artificial Intelligence Technology is Difficult to Implement | Privacy Protection Issue (2021). https://www.nsfc.gov.cn/csc/20345/20348/pdf/2021/202103-387-393.pdf*

[4] *How You Can Apply Big Data to Risk Management (2019). https://bigdataanalyticsnews.com/how-you-can-apply-big-data-to-risk-management/*

DOI: 10.54254/2754-1169/46/20230315

[5] Ma Hongxiang, Yang Yanhong, Wang Ruixiang. On Financial Regulatory Thinking - Science and Technology Innovation of Contemporary County Economy (2022). 87-89. The DOI: 10.16625 / j.carol carroll nki. 51-1752 / f 2022.12.027.

[6] Your Trusted Resource for Compliance Management - Compliance Audits: A Guide to Ensuring Regulatory Adherence (2023). https://www.v-comply.com/blog/compliance-audits-a-guide-to-ensuring-regulatory-adherence/

[7] Jin Zefen. Impact of Financial Technology on Financial Industry Network Security and Regulatory Countermeasures. Financial Technology Times,2019(08):66-70.

[8] Zhou Daoxu, Zhang Yifei, Li Enyin. Knowledge and Thinking About the Financial Security of Science and Technology [J]. Journal of Tsinghua University Financial Review, 2021 (9) : 107-112. The DOI: 10.19409 / j.carol carroll nki THF - review. 2021.09.027.

[9] The Central Bank Has Made A Strong Statement: Introducing Regulatory Policies for Financial Technology Companies (2023). https://bank.stockstar.com/IG2023052200005248.shtml