International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Advanced Threat Detection and Mitigation in FinTech Applications

Ajay Benadict Antony Raju

ajaybenadict@gmail.com

Abstract

Fintech has made finance a comedically convenient, fast and ever-revolving sector because it continues to expand every day as it is being developed. This has opened the flood gates of expected evolved cyber threats in the factors of malware, phishing, inside threats as well as APTs targeting FinTech application for the purpose of violating the security of financial data and transactions. The paper also includes threats that are of high importance to FinTech applications and their detection and countermeasure techniques which are AI, ML and blockchain. For which the formation of the multi-layered security frameworks, the utilization of the different algorithms for anomaly detection, as well as the development of the effective automated response systems becomes the fundamental requisite to enhance the overall resilience of the FinTech platforms. Identity theft flow FinTech Best practices What the paper will do Essentially, the main purpose of this paper is to describe an overall picture of what threats FinTech companies are up against and how one can safeguard digital assets. Such findings indicate that it is high time to shift from a more protective strategy that can readily align itself with the new threat and compliance environment in the FinTech sector.

Keywords: FinTech applications, Cyber threats, Threat detection, Mitigation strategies, Artificial intelligence (AI), Anomaly detection.

Introduction

The financial services sector expands with the highest evolutionary rates among all the industries, and it also transform the traditional financial services by using digital technologies. The following firms have provided the traditional banking services in a simple and convenient way touching the global market through mobile applications, block chain technology, artificial intelligence as well as big data; payments, lending, investments and banking. But this has brought several new risks to the financial services as most of them have gone digital. It also has to respond to rising risks sophistication level from those who seek its harm through malware, ransomware, phishing, insiders and advanced persistent threats. These threats result into signs of lower assurance to the preservation of this crucial financial information and may lead to financial loss, reputational loss and non- compliance with regulations in case of these breaches among these organizations.

For addressing such a phenomenon, the countermeasures that are fit for use need to be embraced by the FinTech firms at the right time together with the threat detection and mitigation solutions that fit their needs. Conventional security

Literature Review:

As a global liberalizing force Fintech has brought about innovations that has reposed the face of financial services in a bid to deliver better services, increase access to finance and customer experience, albeit this underlying innovation is not without its susceptibility to cyber threats which must be well addressed to mitigate the threat to cybersecurity.

According to the current technologies' analysis and the niche they have established within the FinTech industry, cybersecurity has benefited from AI and ML as the most popular and effective innovations within this sphere. Signs of potential cyber threat, which can be discernible when analyzing big data for pattern and anomaly include; advanced threat detection by using AI and ML. They can help FinTech platforms to track the threat in realtime and also allow such platforms to make early predictions so that they can deal with the threat as it unfolds. For example, Alheeti et al noted that IDS that is based ML is able to detect new forms of attacks which are hard to recognize under the traditional approach [1]. Sharma and Kumar detailed how predictive analytics from artificial intelligence were utilised in improving threats' detection and management in FinTechs [2].

It has also been used in improving security of cash related activities for example in banking sector. It is tamper-proof and is also decentralized in nature which make it useful in ensuring that data is not tampered with and is easily auditable thus the risk of fraud and unauthorized access is minimized. Chen and his colleagues' study focused on the idea of how blockchain can be adopted to increase the security of the financial transactions for the improvement of people's confidence in the financial sector [3]. Duan et al. [4] also described how the use of smart contracts in blockchain elevates the level of automation a step further with certain pre-defined actions being executed when some occurrences happen.

All these threats are witnessed in the current world and as such concept of war against them is almost as complicated; this is where the multiple layered security frameworks are useful. Incorporation of conventional security measures coupled with the advanced technologies is the best way to formulate a good security network. Thomas and Swain have also recommended the utilization of Intrusion Detection and Prevention Systems and encryption, and new preserving Artificial Intelligence and / or Machine Learning based threat models for enhancing the security of FinTech xiv [5]. It also supports their findings in the study: the layered model for protection from all kinds of cyber threats for the comprehensive and integrated solution.

This has placed anomaly detection through AI and ML as the central component of today's cybersecurity processes. Such systems learn operating system behaviours and then go searching for the deviation of such a behaviour which might be a sign of an intrusion. Ahmed et al. listed various techniques of anomaly detection in a review and the scalability and capability of the techniques to detect complicated attacks from big data streams in real time was noted as an advantage [6]. Still, this feature remains important for the early detection and stopping of the multi-stage attacks in the FinTech applications.

Of course, such data as, for instance, financial information should be protected with the help of such algorithms as encryption. It is therefore obvious that homomorphic encryption and quantum-resistant cryptography can act as an extra layer of security to secure the data at transit and at storage. On the same topic of the new techniques of encryption that are very important in the protection of the financial data from being accessed by the unauthorized persons Patel and Singh presented a paper [7]. They also pointed out that good encryption is required for improving the confidentiality and integrity of data especially for the FinTech sector.

The other big issue related to the use of this model is scalability. Liang and Cao introduced the aspects on

sharding as well as layer-2 protocols of blockchain that are the approaches to scaling of the financial services [8]. These help in high transaction volumes as well as the security required as one of the major hurdles to FinTech firms.

Perhaps the biggest issue that has been identified in regard to state-of-the-art cybersecurity solutions is the issue of interoperability and addressing of the current standard regulatory measures. Choudhary and Gupta added details to the impact of compliance over cybersecurity for FinTech companies and additionally pointed out that the SA for enhancing the good performance of security in the FinTech industry [9]. Therefore, their study suggests that there is imperative to familiarise the emergent cybersecurity frameworks to the regulatory demands in an effort to foster confidence and security in FI-nances applications.

Problem Statement

Technological integration in financial service industry has advanced over the recent future with the aid of FinTech. But this has also introduced various other technologies which pose threat to the traditional forms of safeguarding. Such as where FinTech applications that are processing the user's financial data are now exposed to more sophisticated threats such as malware, ransomware and advanced persistent threats (APTs) [2][6]. These threats are gradually bringing into question the conventional security measures like rather primitive encryption techniques and more critically firewalls [10].

Some such drawbacks of today's threat detection systems are high false positives and the issue of handling new threats, because of new technologies such as blockchain and AI [4][5]. Than, the growth of the legal regulators' complexity slows down the ability to implement proper security measures [9]. Since the criminals employ the more complex ways to breach into the FinTech platforms, it becomes imperative to design and apply the right, elastic and well-coordinated with one another security solutions that might include monitoring, data analysis, and strong encryption [7][8]. However, with these measures not implemented, the FinTech applications are still vulnerable to various attacks which could lead to great loss and loss of trust [3].

Solution

In order to counter the cybersecurity risks that define the applications of FinTech the following measures and technologies are necessitating: AI and ML enhance the prospects of threat identification as massive datasets containing the pattern and anomalous behavior of threats can be analyzed. Artificial intelligence improves threat identification; reduces the frequency of false alarms; and lets for the real-time observation and control of threatening events [2][6].

Increased security will be achieved due to the decentralized nature of the blockchain technology and that the records stored in the ledger cannot be altered. The use of Blockchain in financial management and transactions has been accredited for its security and transparency hence reducing the risks associated with it [3][4].

This is where adoption of elaborate encryption is significant in protecting the data of the financial sector. The technique of homomorphic encryption and quantum-resistant cryptography provides a certain measure of security to the data that are in transit as well as the data at rest that is not susceptible to moderations or attacks that are characteristic of traditional encryption methods [7][11].

It is thus possible to talk about compensation and integrated complex at the same time it is possible to consider IDPS, encryption, and real-time monitoring as a multilayer system of protection against different

types of cyber threats. In combination with other methods these elements help to create a powerful safety concept in an attempt to increase the general level of security [5].

Applying such solutions as shard and layer-2 protocols helps to manage a large number of traffic flows while maintaining the required level of protection. Such solutions are pivotal since blockchain networks applied in FinTech-related fields have to be efficient and, at the same time, scalable [8].

However, following the law is vital to the safeguard of the financial technology services, and therefore the faith placed on them. It is therefore necessary to develop security solutions in cyber security that prevent them from being contrary to the law of the country and international law to reduce the legal effect as well as enhance the general security [9].

As a result, with the aid of these aforementioned advanced technologies and methods, the FinTech firms can develop a deep approach to counter the complex cyber threats and in turn pass on the trustworthy platforms to the users.

Conclusion

Thus, to overcome the problem of cybersecurity in FinTech applications, it is necessary to apply several measures and tools. AI and ML incorporation is efficient in threat detection as it means that information is analysed in real time thus minimizing on false alarms and shortens the response time. Furthermore, there is also an improvement in the security since the technology used is block chain since it is a decentralized system and the record is unalterable hence reducing fraud cases.

Current and future threats to the financial data will be the solved by sophisticated encryption measures such as the homomorphic encryption and quantum-resistant cryptographies. Due to its integration with real-time monitoring, and intrusion detection systems, it is possible to develop a number of security levels which should be effective against most of the possible cyber threats.

Furthermore, the techniques like sharding as well as layer two protocols enable to control the throughput when multiple connections are made whilst maintain the security level intact. The follow and compliance with the current legal framework is equally important as managing the risks of clients and maintaining their trust in the FinTech platforms. Therefore, through these strategies and solutions fin tech firms shall be in a better stand to consider and reduce contemporary cyber threats that endanger the efficiency of financial systems.

References

1. Alheeti, K. M., Gruebler, A., & McDonald-Maier, K. D. (2022). "Machine Learning for Intrusion Detection Systems in Cybersecurity." *Journal of Network and Computer Applications*, 198, 103209.
2. Sharma, R., & Kumar, N. (2023). "AI-Powered Predictive Analytics for Cyber Threat Detection in FinTech Applications." *Cybersecurity Journal*, 15(3), 75-89.
3. Chen, D., Xu, Z., & Zhang, Y. (2022). "Blockchain Technology in Financial Transactions: Security and Trust Implications." *International Journal of Financial Studies*, 10(4), 189-202.
4. Duan, H., Liu, D., & Wu, Y. (2022). "Smart Contracts and Automated Cyber Threat Mitigation in FinTech." *Journal of Blockchain Research*, 5(2), 45-59.
5. Thomas, M., & Swain, J. (2023). "Enhancing Financial Security through Multi-Layered Security Frameworks." *Journal of Cyber Defense*, 19(1), 23-40.
6. Ahmed, M., Mahmood, A. N., & Hu, J. (2021). "A Survey of Anomaly Detection Techniques in Financial Applications." *Computers & Security*, 109, 102328.

7. Patel, S., & Singh, A. (2022). "Advanced Encryption Techniques for Secure Financial Data Transmission." *Journal of Cryptographic Engineering*, 12(2), 98-115.
8. Liang, X., & Cao, M. (2023). "Scalable Blockchain Solutions for Financial Services: Sharding and Layer-2 Protocols." *Financial Blockchain Review*, 7(1), 56-78.
9. Choudhary, A., & Gupta, P. (2022). "Regulatory Compliance and Cybersecurity in the FinTech Sector." *Journal of Financial Regulation and Compliance*, 30(4), 210-226.
10. Alheeti, K. M., Gruebler, A., & McDonald-Maier, K. D. (2022). "Machine Learning for Intrusion Detection Systems in Cybersecurity." *Journal of Network and Computer Applications*, 198, 103209.
11. Zhang, X., & Wang, L. (2023). "Homomorphic Encryption and Quantum-Resistant Cryptography for Financial Applications." *Journal of Secure Computing*, 15(3), 112-12