RESEARCH ARTICLE OPEN ACCESS

The Future of Fintech Fraud Prevention: Innovations and Strategies

Anirudh Mustyala
Software Engineering, Plano - Texas
Email: anirudhmusthyala@gmail.com

----------**********----------

Abstract :

The fintech industry is one of the most targeted sectors by fraudsters. The unabated spread of fraud in the sector not only harms fintech companies but also the customers they serve. Fintechs can manage the proliferation of scams in their sector by adopting modern cybersecurity technologies such as blockchain, AI and ML, geo-fencing, and multi-factor authentication models. They can further enhance the effectiveness of these technologies in mitigating fraud by supplementing them with best cybersecurity practices such as screening customers at the onboarding phase, monitoring their systems 24/7, screening all transactions for suspicious behavior, updating their systems regularly, and complying with KYC and AML regulations.

Keywords: Fintech, Fraud, AI&ML,Data,General

----------**********----------

I. INTRODUCTION

The fintech sector is revolutionizing financial markets across the globe. Today, people can conveniently access financial products such as insurance covers and money transfer services right from their palms. Besides easing access to financial products, fintech entities have revolutionized service delivery. Modern onsumers of financial services enjoy personalized services. Using data analytics, fintech entities customize their services based on individual clients' needs and preferences. Although fintechs are playing an integral role in revolutionizing the financial industry, the sector is being confronted by the emergence of cybercrimes targeting online-based financial services.

Javelin (2023) says that an average fintech company loses $51 million annually to fraud. The report notes that in 2022, the United States fintech companies lost about $20 billion to fraud, and more than 15.4 million adults were victims of fraud. Implications of fraud on fintechs span beyond financial losses. Fraud attracts lawsuits, which often result in penalties and compensations. Affected fintechs also suffer reputational losses that lead to customer mistrust. Customers who lose trust in their service providers often migrate to competitors (Paoli et al., 2018). Fraud harms customers as well. Victims of fraud suffer psychologically and emotionally, and some are left struggling financially. Sometimes, the impacts are so devastating on victims to the extent they lose their credit scores.

The consequences of fraud on fintechs are dire. For the sector to continue recording sustainable growth, the proliferation of scams in the sector must be tamed. This will create a secure environment where fraud losses are low, and customers trust and feel safe when using fintech services. Increased trust in fintech services will encourage more people to assimilate the technologies to a greater

extent. This writing explores some of the modern technologies and strategies the fintech industry can leverage to address the rising fraud cases in the sector.

II. BODY

Emerging technologies

Although the frequency of scams in the fintech sector is unremittingly worsening, that does not mean the industry is short of solutions to address the challenge. In fact, like never before, there are multiple technologies that can be exploited to reinforce the safety of fintech systems, effectively locking out fraudsters. Entities that employ these innovations seldom experience system breaches. These technologies include;

Blockchain technology

Blockchain is one of the most recent technologies transforming the cybersecurity sector. Blockchain is a distributed system that stores data on nodes organized in a peer-to-peer framework (Di Pierro, 2017). In blockchain, data is stored in blocks, and all nodes in the network must approve any modification of data through a consensus framework. Data stored on blockchain is immutable, and any authorized change to data is traceable and reversible. Unlike conventional systems, data stored on the blockchain is encrypted by sophisticated encryption algorithms. Blockchain is a modern ledger system specifically designed to thrive in the modern unsecure cyber environment.

Blockchain ensures the security of a system in various ways. Records stored on the blockchain cannot be altered. This is critical for preventing frauds such as account takeover, which involves fraudsters altering customer data such as login credentials. As aforementioned, in blockchain, data is stored on multiple computers within the network. In case of a breach, it is practically unviable for criminals to compromise all node ledgers. Distributed ledger helps limit the severity of

a successful attack. Since blockchain stores all transaction records, in case of a breach, changes can be traced and corrective actions implemented. Blockchain can also enhance the security of fintech systems by anonymizing customer data. Even when data is breached, fraudsters cannot link the data to their owners, making it difficult for them to use it. Blockchain's encryption feature also prevents unauthorized access to customer data, whether in transit or at rest.

Artificial intelligence and machine learning technologies

Virtually all sectors of the global economy are leveraging AI and ML technologies to automate processes, lower costs, and improve the productivity of their workforces. Artificial intelligence is the empowerment of machines with intelligence relatable to that of humans. AI enables machines to be smart, making them capable of performing roles that require thinking and were traditionally reserved for humans (Lee, 2020). Mahesh (2020) defines machine learning as the capability for machines to use learning algorithms to detect patterns in data and autonomously develop procedures for performing tasks. AI and ML have various applications in fintech security systems.

AI and ML technologies can learn about consumer behavior and monitor activities on customer accounts. Any activity that falls outside the known customer character triggers an alert. The system can respond to the alert by further verifying the user's identity or aborting the transaction. Besides monitoring customer accounts, AI and ML technologies can be deployed to monitor an entire FinTech system. All processes in the system are monitored, and suspicious activities are flagged in real-time. AI and ML can also be used in fintech security systems for threat hunting and threat intelligence. Threat intelligence involves AI and ML collecting information from digital sources, such as the dark web, social media, and

cybersecurity platforms, and processing it to identify emerging threats likely to affect the system. Threat hunting is the practice of scanning fintech systems to identify potential vulnerabilities and remediate them or alert teams responsible for addressing them. Conversational AI can also be used to prevent fraud in financial platforms. Talking to customers is an essential piece for mitigating fraud. Conventional AI can collect necessary information for verifying the authenticity of transactions. Conversational AI can be used alongside voice biometrics to prevent fraud.

Geo-fencing technologies

Though some fintechs have a global reach, most of them serve specific regions. In fact, most fintechs serve client bases within their countries. Fintechs that operate in specific regions have no business being accessible to people from other parts of the world. For instance, a fintech operating in the United States alone has no reason to allow Chinese traffic. Geo-fencing is a new technology that allows businesses to geographically restrict traffic to their cyber systems (Singh et al., 2018). Geo-fencing restricts traffic by looking at the geographical location it is coming from through assessing the IP address making requests. Geo-fencing reduces the accessibility of cyber systems, hence reducing the cybersecurity risk. The technology can also be configured to specifically lock out regions known for cyber threats. For example, a Fintech in the UK may consider using geo-fencing to lock out traffic from scammer-prone countries such as Nigeria, Romania, and Venezuela.

Multi-factor authentication

Multi-factor authentication is a relatively new authentication and verification method where users are authenticated several times before accessing their accounts. Two-factor authentication is the most common type of multifactor authentication. Fintechs firms can use two-factor authentication that combines inherence and knowledge factors to enhance

authentication security. For example, an ideal fintech authentication model should request biometric factors. Once biometrics are verified, the system should generate a one-time PIN (OTP) and send it to the user's email or SMS. The user can access the system after receiving the OTP.

Strategies

Technologies alone are not sufficient to combat fraud in the fintech sector. Although they provide the necessary background to mitigate fraud, cybersecurity technologies must be complemented by best security practices and strategies. Combining the best cybersecurity technologies with best practices is a sure way to achieve ultimate cyber security. Some of the best strategies for enhancing fintech cybersecurity include;

- **Customer onboarding**: Fintech security starts at the onboarding phase. A holistic onboarding process scans customer documents against trusted databases to ensure they are not fraudulent. Fraudsters usually use fake registration documents. An effective onboarding process should be able to get rid of fraudsters at the registration level.
- **Ongoing monitoring**: Cyber risks are constantly evolving. It is essential for fintechs to keep monitoring their systems for suspicious behavior and interactions between users.
- **Transaction screening**: Customer screening alone is not enough. All transactions must be subject to screening to ensure no illicit activities leak through the system. Transaction screening can be automated using AI and ML technologies.
- **Regular system updates**: Risks are constantly evolving, and fraudsters are always looking for vulnerabilities to exploit. To stay ahead of fraudsters, fintechs must frequently update their

systems to seal vulnerabilities before they are exploited.

- **Compliance with KYC and AML regulations**: KYC and AML regulations provide the framework for addressing frauds such as financial crimes. Fintechs that configure their operations and systems to comply with KYC and AML laws are in a better position to combat fraud.

III. CONCLUSION

The fintech industry is one of the most targeted sectors by fraudsters. The unabated spread of fraud in the sector not only harms fintech companies but also the customers they serve. Fintechs can manage the proliferation of scams in their sector by adopting modern cybersecurity technologies such as blockchain, AI and ML, geo-fencing, and multi-factor authentication models. Fintechs can enhance the effectiveness of these technologies in mitigating fraud by supplementing them with best cybersecurity practices such as screening customers at the onboarding phase, monitoring their systems 24/7, screening all transactions for suspicious behavior, updating their systems regularly, and complying with KYC and AML regulations. Fintech companies that leverage these technologies and pay attention to these strategies report advanced cybersecurity status.

References

Paoli, L., Visschers, J., & Verstraete, C. (2018). The impact of cybercrime on businesses: A novel conceptual framework and its application to Belgium. *Crime, Law and Social Change, 70*, 397-420.

Di Pierro, M. (2017). What is the blockchain?. *Computing in Science & Engineering*, *19*(5), 92-95.

Lee, J. (2020). Industrial ai. *Applications with sustainable performance*.

Mahesh, B. (2020). Machine learning algorithms-a review. *International Journal of Science and Research (IJSR).[Internet]*, *9*(1), 381-386.

Singh, A., Pal, A., Garg, D., & Yadav, D. (2018). Location-Based Services Using Geofencing. *International Journal of Advance Research and Development, 3*.

Javelin (2023), 2023 identity fraud study. The butterfly effect. Retrieved From: https://javelinstrategy.com/research/2023-identity-fraud-study-butterfly-effect