ISSN: 2583-9888
DOI: doi.org/10.51219/JAIMLD/joseph-aaron-tsapa/82

URF PUBLISHERS
connect with research world

Journal of Artificial Intelligence, Machine Learning and Data Science

https://urfpublishers.com/journal/artificial-intelligence

Vol: 1 & Iss: 1

Research Article

Strengthening FinTech Defenses: A Novel Approach with Federated Learning and Anomaly Identification

Joseph Aaron Tsapa*

Joseph Aaron Tsapa, USA

Citation: Joseph Aaron Tsapa. Strengthening FinTech Defenses: A Novel Approach with Federated Learning and Anomaly Identification. *J Artif Intell Mach Learn & Data Sci 2023*, 1(1), 265-268. DOI: doi.org/10.51219/JAIMLD/joseph-aaron-tsapa/82

Received: 02 February, 2023; **Accepted:** 18 February, 2023; **Published:** 20 February, 2023

***Corresponding author:** Joseph Aaron Tsapa, USA

ABSTRACT

The paper examines integrating federated learning and anomaly detection techniques to strengthen cybersecurity in the financial technology sector. Such financial data is highly significant, and the intrusion-related concern has brought them together. The paper focuses on developing a solution using data processing in distributed mode and timely identifications of anomalies to the current cyber threats, data breaches, and fraud schemes. This paper further discusses the most crucial cybersecurity problem in FinTech, which is keeping financial information non-public to be protected in a digital environment. The paper offers federated learning, a distributed machine learning paradigm that combines anomaly detection to detect any unusual event as a potential security breach. This approach can overcome delicate and private data protection issues by using distributed data processing and anomaly detection algorithms while guaranteeing data security and safety. At the same time, the writing points out other roles, consequences, and capabilities as a possible holistic solution, which could, at some point, achieve cybersecurity, regulatory compliance, and resilience in the FinTech ecosystem.

Keywords: FinTech, Cybersecurity, Federated learning, Anomaly detection, Data privacy, Distributed data processing

1. Introduction

The combination of these two sectors, FinTech, is supported by a fusion of technology and finance, improving financial services through innovation and digitalization. Our task may be characterized as a democratic process wherein the financial service is available for all; there would be an efficient payment system and economic inclusion. However, the cyber world is evolving, so hacking and data security risks are getting more serious. Such financial information is confidential, and the investment in securing the data is crucial due to the risk of people's profiles being linked to personal and financial details. Cybersecurity has old-fashioned security worldwide, with two problems: increasing cyber risks and laws. The developments in distributed learning, such as consensus-based detection of anomalies, seem to be the 'promising ways' one should prioritize. Its models are trained in a distributed network whereby we never have to share our private data[1]. Moreover, intrusion detection algorithms can discover behavior patterns or activities that are suspect and threats. This type of tech can be regarded as a versatile weapon in the issue of cybersecurity, regulatory compliance, and data privacy protection in the FinTech industry.

2. Problem Statement

The charts below indicate that FinTech faces a confusing and dynamic cyber threat terrain of emerging dangers, data breaches, and financial fencing plots.

These obstacles mainly affect data safety and security in financial services, which are also under threat by the business and private sector companies. Nevertheless, stringent regulatory rules induce a duty to secure the sensitive personal data of the client while engendering certain apprehensions about the privacy of data and conformity to the regulations[3]. The centralized architecture of many FinTech platforms, which rely heavily on central servers, can create a single point of failure

or vulnerability. This large attack surface area makes FinTech companies potential targets for malicious actors seeking weak links to exploit. The inherent risks associated with this centralized approach must be carefully addressed to enhance the overall security and resilience of the FinTech ecosystem.

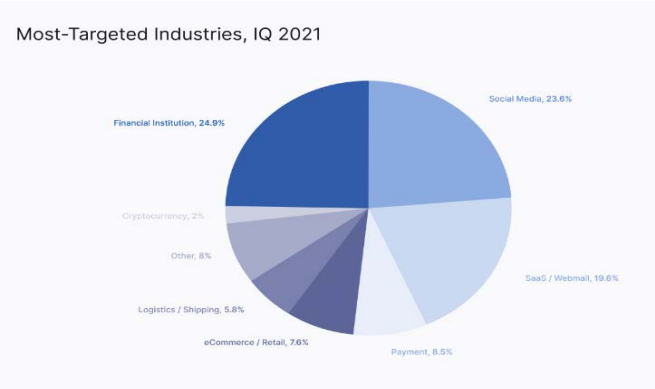

Figure 1: Cyberthreats for financial systems[2].

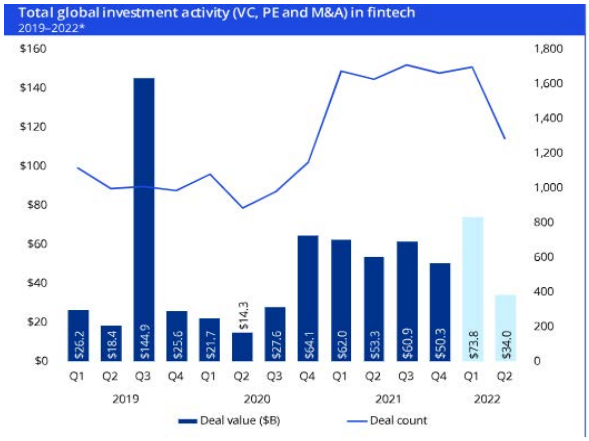

Figure 2: Impact of Cyber Risks on Global Investments[3].

Nevertheless, this problem calls for the utmost efficiency of various regulations on FinTech services and the discovery of novel cybersecurity options that can neutralize the threat, fulfill regulatory standards, and protect customers' privacy.

3. Solution

The federated learning and anomaly detection algorithms, which were outpenciled as a remedy for cybersecurity challenges of the FinTech industry, have been proposed. The federated learning approach takes place in which models are trained from the distributed devices, such as complete data privacy, which has been ensured with no need for data to be transferred.

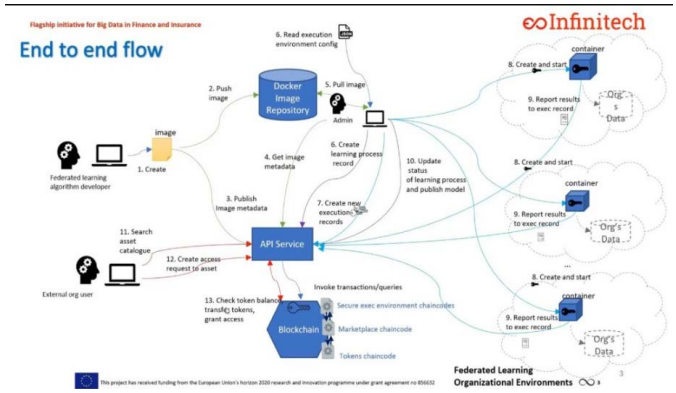

Figure 3: Federated Machine Learning (FML) for Digital Financial and FinTech Applications.

The data-oriented protection models are finished by applying anomaly detection tools to detect abnormal data patterns or activities, which are the distinctive traits of security threats from distributed data[4]. With this technique, federated learning can be utilized with anomaly detection to meet the needed degree of scalability when dealing with vital and distributed data. Real-time algorithms can then be applied to detect anomalies and avert security incidents.

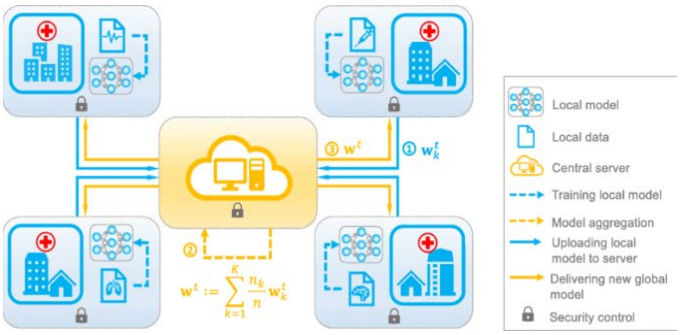

Figure 4: Schematic diagram of the federated learning framework.

The schematic diagram of the federated learning framework with the anomaly detection modules incorporated is shown on the diagrams. This architecture facilitates end-to-end cooperation and helps aggregate the models from the distributed sources[5]. As a result, it ensures the safety of cybersecurity, data privacy, and compliance in the FinTech landscape.

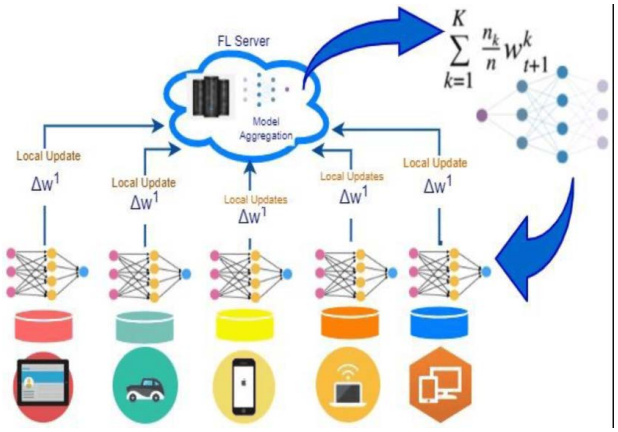

Figure 5: Applications of federated learning, taxonomy, and challenges.

4. Uses

The action plan includes FinTech's successfully diversified employment areas. In real-time, the technology can detect and prohibit fraud by suspecting and preventing all fraud activities at the moment of the transfer, keeping the merchant and consumer safe from chances of loss.

Along with integrating federated learning, anomaly detection, and threat intelligence sharing between FinTech sectors, cybersecurity collaboration will be created, enabling the detection of threats; therefore, data will not be disclosed. Furthermore, this solution can adjust the individual user's security measures, increasing efficiency and enhancing security in the FinTech platform[6]. A chart demonstrates the increase in the development of federated learning in detecting anomalies over the traditional way. The following figure shows that federated learning affects security vulnerabilities the most, indicating that the union of recent technologies for achieving cybersecurity efficiency is a progressive trend for FinTech.

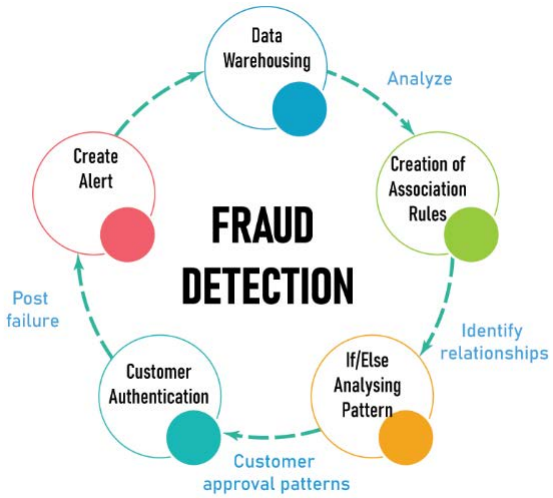

Figure 6: Fraud Detection[6].

5. Impact

Communicating federated learning and irregular event detection in the FinTech area entails deep cyber security and operational resilience effects. It is advisable to note that it significantly strengthens FinTech's cybersecurity posture through its ability to actively identify and mitigate threats.

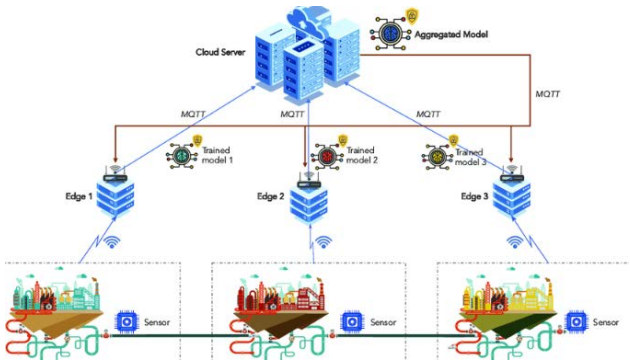

Figure 7: Application and structure of Federated-Learning-based Anomaly Detection[7].

They avert the actuality above through swift acting and defending confidential financial information. That said, the service through which this solution will be achieved will also ensure that it complies with data privacy regulations and that highly efficient security measures are implemented. This will thus link two aspects of regulatory compliance. The rules in place allow FinTech companies to function within legal frameworks while managing appropriate security parameters[8]. Another of these is that the use of federated learning and anomaly detection reduces financial losses because cyber attacks and fraudulent activities are almost nonexistent due to these attacks. Effective identification and management of risks will help banks successfully take liability damage to their health and stability. Reference is made to examples or case studies that depict the influential role of technological developments in cyber defense and assurance of FinTech operations' resilience.

6. Scope

Fusing federated learning and anomaly detection cybersecurity for FinTech applications sparks advantages at varying levels. At the same time, scalability should be the point to take into account because it provides the solution with the ability to adjust seamlessly the level of fintech from startups to large corporations[9]. Last but not least, system compatibility is important regarding proper technology and FinTech sector integration to eliminate disruptions or interferences by the old systems. Besides that, the practical application of federated learning and anomaly detection from the viewpoint of FinTech is an opportunity for innovations that could be used to improve cybersecurity controls. New algorithms, enhanced data management, and privacy protection tools should improve significantly.

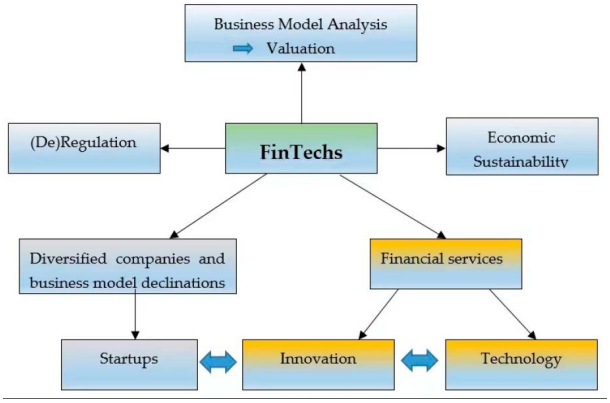

Figure 8: Scalability and compatibility[10].

A diagram exhibiting the scalability and compatibility alongside the proposed ones will be the visual representation of the adaptability and flexibility across different FinTech environments simultaneously and the ease to which it will face cyber security breakdowns while having the functionality to tackle them by accommodating industry ongoing requirements.

7. Conclusion

Lastly, system integration of federated learning and anomaly detection approach provides a critical response for more security awareness in the FinTech domain. It deals with the security problem of the evolving nature of security risks, preservation of data privacy for consumers and financial data, and imposition of regulatory requirements that improve the reliability of FinTech programs under the given cyber attacks and fraud. The effects go beyond just providing for physical safety; they also offer the main benefits of improved compliance and fewer ineffectual losses. The point that cybersecurity keeps on being developed together with FinTech technology and research means that the future of FinTech cybersecurity is ready to go on to the next level of innovation and strength, which will guarantee the robust security of this modern innovation. It is vital to infuse cutting-edge technology into information security systems because the very nature of digital financial space spreads trust and privacy across the globe.

8. References

1. L Cao, Q Yang, PS Yu. Data science and AI in FinTech: An overview. Int J Data Sci Anal, 2021.
2. RO Ogundokun, S Misra, R Maskeliunas, et al. A review on federated learning and machine learning approaches: Categorization, application areas, and blockchain technology. Information, 2022; 13: 263.
3. S Mehrban, Muhammad Waqas Nadeem, Muzammil Hussain, et al. Towards secure FinTech: A survey, taxonomy, and open research challenges. IEEE Access, 2020; 8: 23391-23406.
4. B Stojanović, J Božić. Robust financial fraud alerting system based in the cloud environment. Sensors (Basel), 2022; 22: 9461.

5. S. Das. The future of fintech. Financial Management, 2019; 48: 981-1007.

6. G Chakraborty. Evolving profiles of financial risk management in the era of digitization: The tomorrow that began in the past. Journal of Public Affairs, 2019; 20: e2034.

7. A Adeyoju. Cybercrime and cybersecurity: FinTech's greatest challenges. SSRN Electronic Journal, 2021.

8. AW Ng, BKB Kwok. Emergence of fintech and cybersecurity in a global financial center. Journal of Financial Regulation and Compliance, 2017; 25: 422-434.

9. R Moro-Visconti, S Cruz Rambaud, J. López Pascual. Sustainability in FinTechs: An explanation through business model scalability and market valuation. Sustainability, 2020; 12: 10316.

10. P Gomber, RJ Kauffman,. Parker, et al. On the fintech revolution: Interpreting the Forces of innovation, disruption, and transformation in financial services. Journal of Management Information Systems, 2018; 35: 220-265.