Internet Technology Letters

WILEY

SPECIAL ISSUE ARTICLE

Integrating Big Data and AI for Network Security in 6G to Enhance University Financial Management

Jun Liang | Ling Pu | WeiweiSun

Economics Department, School of Qinhuangdao Vocational and Technical College, Qinhuangdao, Hebei, China

Correspondence: Ling Pu (plpuling@163.com)

Received: 12 March 2025 | **Revised:** 15 July 2025 | **Accepted:** 26 July 2025

Funding: The authors received no specific funding for this work.

Keywords: 6G networks | anomaly detection (AD) | artificial intelligence (AI) | Big Data (BD) | federated learning (FL) | university financial security (UFS)

ABSTRACT

In the 6G network structures, the integration of Big Data (BD) and artificial intelligence (AI) is beneficial for the purpose of improving cybersecurity in university financial management systems. So, the integration of the BD and AI in the 6G structures are suggested in this study. Then, the conventional centralized security systems are ineffective in the rapid digitalization of financial transactions. Because these conventional systems are susceptible to single points of failure (SPF), delayed threat detection, and data privacy breaches. In the real-time (RT) financial backgrounds, these conventional systems face difficulties in protecting the network against advanced cyber threats. These situations will call for a decentralized, adaptive, and privacy-preserving (PP) security framework in the rapidly evolving 6G structures. This demanded framework may help in anomaly detection (AD) in financial transactions without affecting vital data. Thus, a novel federated learning (FL)-based AD in financial security (FL-AD-FS) framework is suggested in this study. To train the AI models collaboratively over several edge devices, this suggested model utilizes FL. This application will also ensure the privacy of the data. Then, in financial operations, the RT AD and threat mitigation was facilitated by the system, as it integrates with 6G-enabled (EC) edge computing. The simulations were conducted; from the outcomes, it is clear that the suggested FL-AD-FS model executes better by reducing false positive rates (FPRs), increasing detection (ACC) accuracy, and minimizing latency. In university backgrounds, secure, fast, and reliable monitoring of financial transactions was facilitated by this suggested method. For revolutionizing cybersecurity in digital financial systems, the potential of the integration of the FL, AI, and 6G technologies is demonstrated by the FL-AD-FS framework. For modern university financial management, this suggested method creates a customized scalable, secure, and privacy-aware solution.

1 | Introduction

In the university campus, the rapid development of digital banking raises additional cybersecurity issues [1]. When financial transactions move toward digitalization, a robust security measures are vital for institutions. Because these security measures may secure private financial data from cyberattacks [2]. By using ultra-low latency, great connection, and unrivaled speed, businesses are improving financial management systems, facilitated by the 6G networks [3]. The ineffectiveness of the current centralized security policies and more complicated attacks may demand more adaptable and intelligent solutions [4]. These conventional methods usually depend upon centralized methods, so they are susceptible to data breaches, SPF. These conventional systems are ineffective in detecting complex cyber threats [5]. To perform financial theft, attackers may alter systems, steal

information, and take advantage of centralized system flaws [6]. Since current security technologies, including firewalls and intrusion detection systems (IDSs), are unable to keep up with the constantly evolving nature of cyber threats, a new approach is necessary [7]. Big Data and artificial intelligence (AI) provide prospective answers in predictive analytics, real-time threat monitoring, and automated anomaly identification in university financial operations [8].

To handle these security issues, Big Data, AI, and federated learning (FL) are recommended to be used in 6G-enabled network security systems [9]. By letting several distributed nodes train ML models without sharing RT financial data, FL preserves privacy and improves cybersecurity [9]. Using FL-AD-FS, universities could improve their RT financial risk-minimizing, cyber AD, and fraudulent transaction identification capabilities [10]. This paper investigates utilizing 6G-enabled EC and how FL-AD-FS enhances the security of university money [11]. Lower latency, higher detection ACC, and continuous protection of financial transactions from developing cyber threats follow from moving security analytics closer to the data source [12]. The research assures safe financial operations, reduces false positives, and sets a benchmark for AI-driven network safety in 6G settings through empirical analysis [13]. FL-AD-FS also shows an improvement in cybersecurity [14].

2 | Related Work

This initiative aims to improve 6G network security utilizing AI-driven solutions. AI continuously detects vulnerabilities in real time, and security mechanisms are regularly modified [15]. Intent-based networking allows user-centric configurations to be automated. Large-scale network systems may be optimized using AI to improve security and minimize costs. The research then underlines the need for AI in healthcare applications to enhance efficiency and data management from the Internet of Things (IoTs) using fuzzy classifiers. This paper proposes an Intelligent autonomous transport system (IATS) constructed on the Ethereum blockchain to enhance logistics security [16]. The immutability of data housed on the blockchain makes it the perfect fit for sensitive data such as orders, shipping details, and personnel information. Employing the many management modules of the system, the light gradient boosting machine (LightGBM) approach is used for vehicle and cargo matching. Simulations of the proposed model allow one to evaluate security forecast accuracy and system performance. This review covers updates to 6G technology, including wireless networks based on Terahertz, software-defined networking (SDN), network functions virtualization (NFV), cloud/fog computing, and AI integration [17]. It looks at privacy and security issues and offers ideas to help better satisfy expectations for future quality of service. The study's future applications include smart healthcare, Industry 5.0, and virtual reality. It fills in research gaps, clarifying the potential security solutions for 6G networks and their future use.

This study investigates how AI and mobile cloud computing might improve service personalizing and reliability using 6G networks. Among AI applications are cybersecurity, fraud detection, and network monitoring. The scalable computing powers offered by the cloud enable real-time data processing [18]. The study advises handling huge volumes of data securely and efficiently utilizing HPC to ensure consistent service delivery. It also explores AI-driven forensic techniques meant to enhance network security. In this paper, the possibilities of 6G, IoT, and AI are highly reliant on one another ecosystems [19]. AI helps to maximize network operations, increase data processing efficiency, and enable proactive management utilizing predictive analytics. The paper shows how adaptive IoTs systems enabled by AI respond in real-time to changed surroundings [20]. The paper promotes proactive security measures because maximizing AI benefits while minimizing hazards depends on this.

Existing studies on financial security in digital environments predominantly focus on centralized machine learning models for anomaly detection. These models are limited by privacy concerns, susceptibility to single points of failure, and high latency in detecting real-time threats. Moreover, prior literature inadequately addresses integrating emerging 6G network capabilities with AI-driven cybersecurity, especially in the context of university financial systems. There is also a lack of frameworks that leverage decentralized learning to preserve data privacy while maintaining high detection accuracy and system efficiency. The suggested FL-AD-FS framework introduces a novel integration of FL, BD analytics (BDA), and 6G EC. Unlike traditional centralized models, FL-AD-FS enables decentralized AD by training AI models locally across distributed edge devices, thereby preserving data privacy and reducing risk exposure. Leveraging 6G's ultralow latency and high bandwidth, the model supports RT monitoring of university financial transactions. The novelty lies in its adaptive architecture, which improves threat detection accuracy, minimizes FPR, and ensures secure and efficient financial operations, marking a significant advancement in the cybersecurity of academic financial systems.

3 | Proposed Method

Combining BD, AI, and 6G transforms cybersecurity and financial management in banks and educational institutions. The University Financial System comes first; it uses 6G network infrastructure to provide secure, fast data transport. Data related to security and money is handled by a BDA layer, which then feeds an AI-driven security layer. Using machine learning, this layer detects anomalies and suppresses dishonest behavior. The approach enables both effective risk control and safe and sensible budgeting. Using AI and advanced network security helps one to protect university finances, lower fraud rates better, and increase general financial efficiency in RT.

$$p_s e = ue\left[a - ewn''\right] * V\left[a - sn''\right] + ye'' \tag{1}$$

This Equation (1) represents an event $p_s e$ in the FL-AD-FS architecture, which stands for within Financial Security. Anomaly detection user engagement ($ue\left[a - ewn''\right]$), security metric variation ($V\left[a - sn''\right]$), and rate of adaptive learning (ye'') affected by anomalies. To provide optimum detection of hazards may dynamically alter security thresholds, as quantified by this equation.

$$T_f r = Tc\left[a - rn''\right] + yd\left[x - ae''\right] \times nc\left[fpc'\right] \tag{2}$$

Equation (2) illustrates the relationship $T_f r$ between FL predictions $Tc\left[a - rn''\right]$, network confidence $yd\left[x - ae''\right]$, adaptive risk variables $nc\left[fpc'\right]$, and transaction complexity.

In 6G-enabled university finance management, this equation guarantees real-time risk assessment, enabling financial cyber threats.

$$p_{cg}e = mx\left[e - sn''\right] + ur\left[a - sd''\right] - vxs'' \tag{3}$$

A $p_{cg}e$ event occurs in the FL-AD-FS framework. Based on developing anomalies ($ur\left[a - sd''\right]$), user reaction ($mx\left[e - sn''\right]$) to identify threats and weakness exposure, it simulates how data mining (vxs'') discovers security flaws. Equation (3) is useful for improving proactive cybersecurity measures by evaluating possible vulnerabilities.

$$x_{vc}p = ne\left[a - wn''\right] + yf\left[v - ne''\right] \times hdc'' \tag{4}$$

Within the FL-AD-FS framework $ne\left[a - wn''\right]+$, the cybersecurity performance variance ($x_{vc}p$). To identify monetary outliers $yf\left[v - ne''\right]$, it simulates the connection between hdc'', the three variables of adaptive security factors. With this Equation (4), the FL-AD-FS model may dynamically adjust security protocols, guaranteeing university financial transactions.

The cyber network, which comprises hardware, software, cloud architecture, information technology providers, and communication systems, helps to facilitate the modernization of financial procedures. Making financial choices, distributing data, and completing transactions is simple with these digital elements. Depending on a strong cyber infrastructure, essential nodes in the financial network are banks, investment funds, insurance companies, and central counterparties; they make secure, transparent, and efficient financial transactions possible. Cyber resilience is very important as, as the image illustrates, flaws in the cyber layer might directly affect the financial industry. Combining cybersecurity frameworks with financial risk management will help financial institutions protect the future of global finance in this digital era by lowering cyber risks, preventing fraud, and increasing the trustworthiness of digital transactions.

$$Z_v b = bne\left[r - na''\right] + ye\left[w - an''\right] \times nsx'' \tag{5}$$

The variation in blockchain-based verification of safety ($Z_v b$) inside the FL-AD-FS architecture is represented by the Equation (5). It simulates the relationship between learning weights ($bne\left[r - na''\right]$) and blockchain network effectiveness (nsx'') as it pertains to financial transaction security and anomaly detection ($ye\left[w - an''\right]$). Equation (5) guarantees that the FL-AD-FS model utilizes the blockchain's decentralized security.

$$p_f v = ts\left[a - fm''\right] + ye\left[s - nq''\right] \times ns\left[d - s'\right] \tag{6}$$

This Equation (6) shows $ns\left[d - s'\right]$ the financial vulnerability probability ($p_f v$) inside the FL-AD-FS model. To anticipate possible $ye\left[s - nq''\right]$ financial dangers, it correlates $ts\left[a - fm''\right]$, which stands for adaptive learning. Strong cybersecurity in 6G connectivity is ensured by this equation, which aids the FL-AD-FS model in proactively identifying weaknesses.

$$\left[p_s e\right] = ms\left[w - aq''\right] + n\left[d - ne''\right] \times bxs'' \tag{7}$$

The likelihood of a safe financial transaction $\left[p_s e\right]$ according to the FL-AD-FS model is given by the Equation (7). The model accounts for security ($ms\left[w - aq''\right]$), network scalability ($n\left[d - ne''\right]$), and security measures (bxs'') on transaction protection. 6G-enabled university administration may be certain that the FL-AD-FS model will dynamically strengthen financial stability.

$$p_w s = ys' \times bm' + \left[a - fn''\right] - V\left[s - ae''\right] \tag{8}$$

A secure wireless transaction's likelihood ($p_w s$) inside the FL-AD-FS paradigm. To make sure that financial data is sent securely, it uses adaptive secure weighting ($ys' \times bm'$), blockchain-based tracking ($\left[a - fn''\right]$), and variance within AD ($V\left[s - ae''\right]$). In Equation (8), the FL-AD-FS model can improve cybersecurity in university finance management using this equation. Adversarial training was implemented by injecting carefully crafted adversarial examples into the training data at the node level, enabling the model to learn and recognize manipulative patterns designed to deceive anomaly detectors. This hardened the model against common evasion techniques used in financial fraud. Additionally, differential privacy was applied to obfuscate individual data contributions during federated model updates, thereby preventing attackers from reconstructing sensitive transaction details through reverse engineering.

The FL-AD-FS architecture includes AI, 6G-enabled EC, BD, and Figure 1 to enhance cybersecurity in university financial management. Distributed AD using FL-AD-FS allows numerous 6G-connected edge devices to be used; therefore, removing the requirement for centralized security models subject to SPF. Built on each edge node's analysis of local financial data, a privacy-preserving FL model can detect anomalies in real time. Analyzing patterns, stopping fraud, and spotting cyber hazards help the anomaly detection engine driven by AI significantly lower false positives and guarantee secure financial transactions. Cybersecurity efficiency was a composite metric capturing the framework's overall threat detection and operational responsiveness. Latency reduction was crucial in validating the real-time performance benefits of 6G and edge computing, while the scalability index assessed how well the system maintained performance across multiple distributed nodes. Additionally, model convergence time was used to monitor the speed of learning and adaptation during federated training, and the financial transaction security score measured the framework's ability to protect data integrity during live simulations.

Figure 2 presents a safe FL architecture intending to guarantee financial security and combat fraud. Federated learning orchestration (FLO) mostly lets cooperative model training with homomorphic encryption ensure data privacy. To exchange encrypted data, bank servers, automated teller machine networks, and stock market systems rely on the same safe SSL/TLS communication path. This financial security data is used in distributed model training to enhance fraud detection without disclosing private user information. Using trained models to find anomalies, a threat-mitigating system looks at potential security hazards. Finally, a dispersed alarm system is installed to prevent fraud. It alerts interested parties when something suspicious occurs, enabling a real-time response to threats. This approach reduces fraud threats, leverages FL to safeguard financial transactions, and enhances cybersecurity across financial networks.

4 | Result and Discussion

Integrated with 6G networks, Big Data, and AI, are revolutionizing university financial management cybersecurity. Cyberattacks quickly compromise conventional centralized security systems, so a distributed, AI-powered solution is required. Using FL and 6G-enabled edge computing, this study presents the FL-AD-FS system, which boosts security, safeguards financial transactions, and improves real-time anomaly detection.

4.1 | Dataset Description

Forecasting a CAGR of 7.4%, the USD 11.93 billion data center chip market is expected to become USD 19.66 billion by 2032. Among significant advancements are Samsung's AGI-oriented processors, NVIDIA's cuLitho integration, and Intel's Xeon 6 AI CPUs [21]. Although trends reveal scalable chip solutions and AI-driven innovations, IoT adoption and energy efficiency demands drive market progress. Table 1 shows the simulation environment. By leveraging FL, FL-AD-FS enables distributed model training directly at the data source, eliminating the need to transfer sensitive financial data to a central server. This enhances cybersecurity efficiency, as real-time anomaly detection can be executed locally with higher precision and reduced false positives. In terms of latency, the framework benefits from edge computing and 6G connectivity, achieving rapid threat detection with minimal delays markedly lower than the latency seen in centralized systems that rely on long transmission routes and centralized processing. Furthermore, scalability is greatly

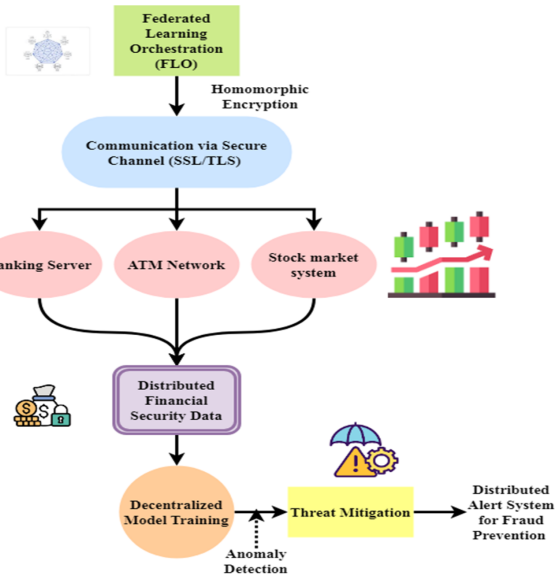

FIGURE 2 | Federated learning for financial fraud prevention.

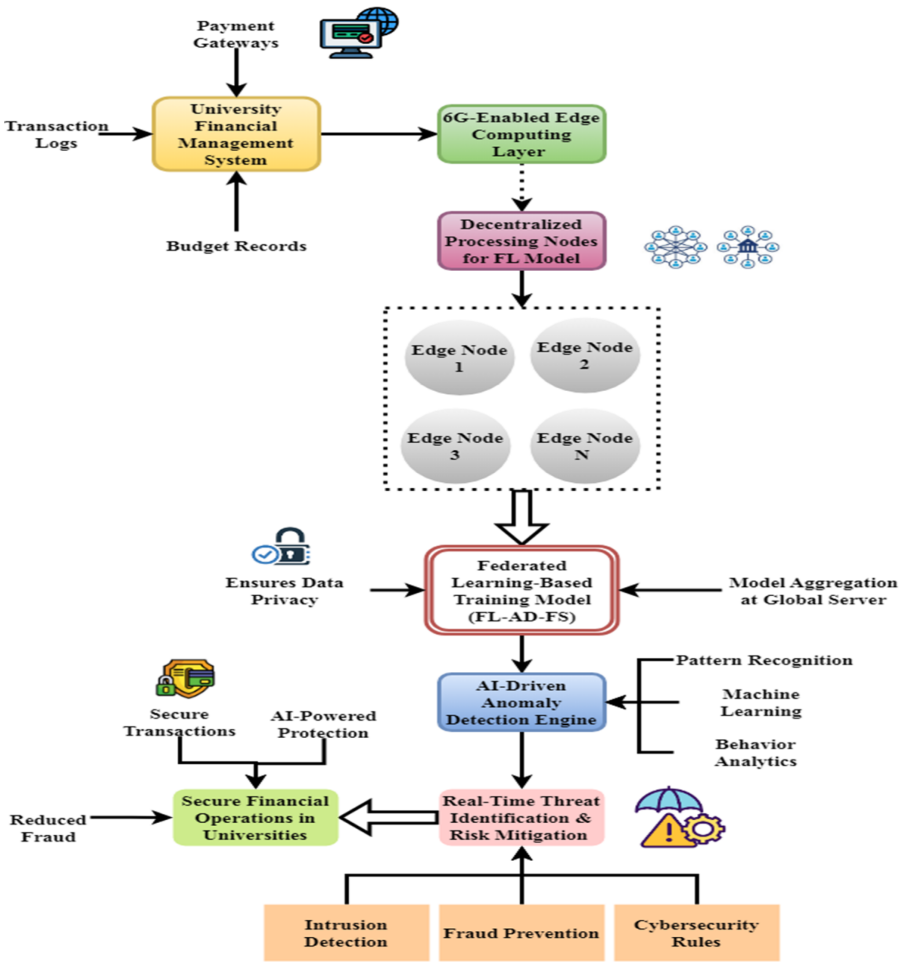

FIGURE 1 | FL-AD-FS: AI-powered FL for secure 6G financial transactions.

improved, as FL-AD-FS can seamlessly integrate with multiple financial nodes across university systems without overloading a central server.

4.2 | Analysis of Cybersecurity Efficiency

The Figure 3 presents a comparative analysis of the cybersecurity efficiency rate (94.52%) against the number of samples for four different models: BDN-S, AIN-S, RNN-F, and LSTM-F. Each subplot represents the performance trend of a specific model as the number of samples increases. The graphs indicate that all models show a steady improvement in efficiency rate with an increasing number of samples, demonstrating their learning capabilities and scalability. Among the models, LSTM-F shows the highest efficiency rate overall, suggesting superior performance in handling sequential data in cybersecurity applications. This figure supports the claim that advanced AI models can significantly enhance threat detection efficiency in a 6G-enabled university financial network environment. FedAvg allows multiple decentralized nodes to train local models on their private financial data and share only the encrypted model updates with a central server for aggregation. This preserves data privacy while enabling the global model to learn from diverse and institution-specific transaction patterns, resulting in more accurate detection of subtle anomalies. Additionally, SMPC ensures that the shared model parameters remain secure and tamper-proof during aggregation, preventing potential data leakage.

TABLE 1 | Simulation environment.

Metrics	Description
Processor	Specifies the CPU/GPU used for simulations, including clock speed and core count.
Memory (RAM)	Defines the available system memory for processing simulations efficiently.
Storage	Indicates the type (SSD/HDD) and data storage and retrieval capacity.
Operating System	Details the OS environment (e.g., Linux, Windows) supporting the simulation framework.
Simulation Software	Lists the tools and frameworks (e.g., MATLAB, TensorFlow, NS3) used for experiments
Network Configuration	Specifies network parameters, including bandwidth, latency, and protocol settings
Dataset	Describes the data sources used for training and evaluating the model
Energy Consumption	Measures power usage efficiency during simulation runs
Evaluation Metrics	Defines performance criteria like accuracy, latency, and false positive rates.

4.3 | Analysis of False Positives

The FL-AD-FS design has many main benefits, one of which is that, as Figure 4 indicates, its false positive rate is low. Excessive false alarms are a regular problem with traditional cybersecurity systems that cause inefficiency and unnecessary system actions. Table 2 shows the comparison of the existing method and the proposed method. Due to FL feature extraction capabilities, CNNs were used to detect local patterns and anomalies in structured financial inputs, such as transaction sequences or categorical attributes. LSTM networks were incorporated to

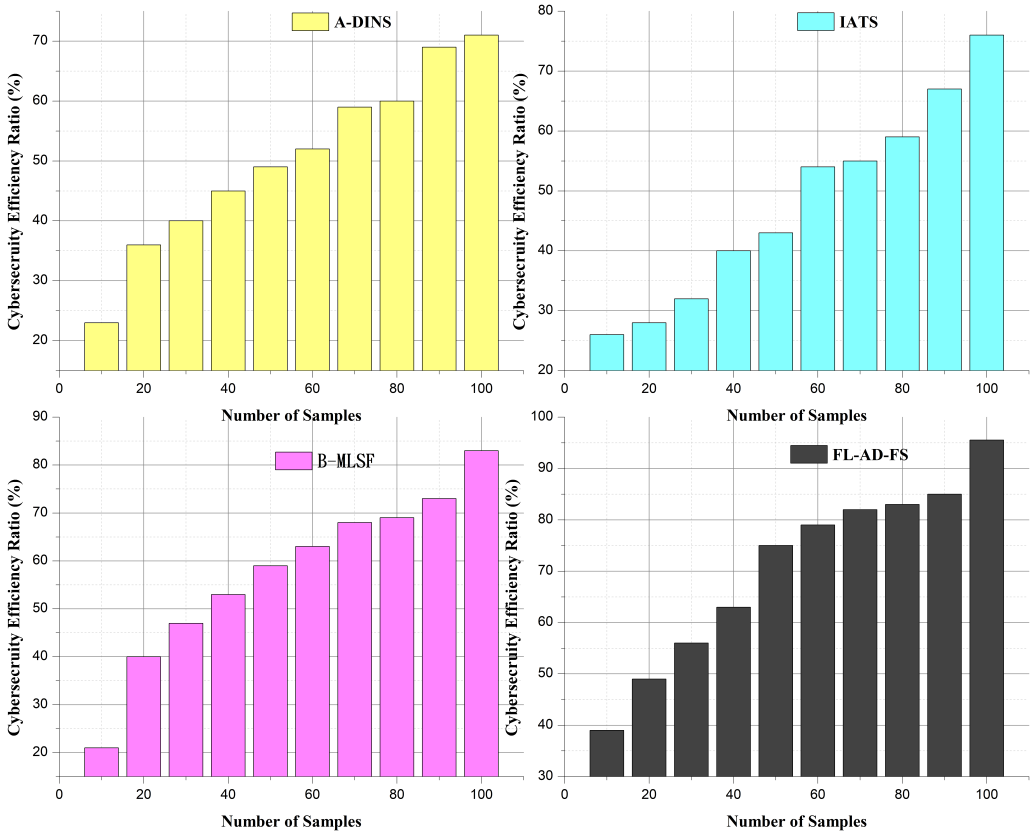

FIGURE 3 | Analysis of cybersecurity efficiency.

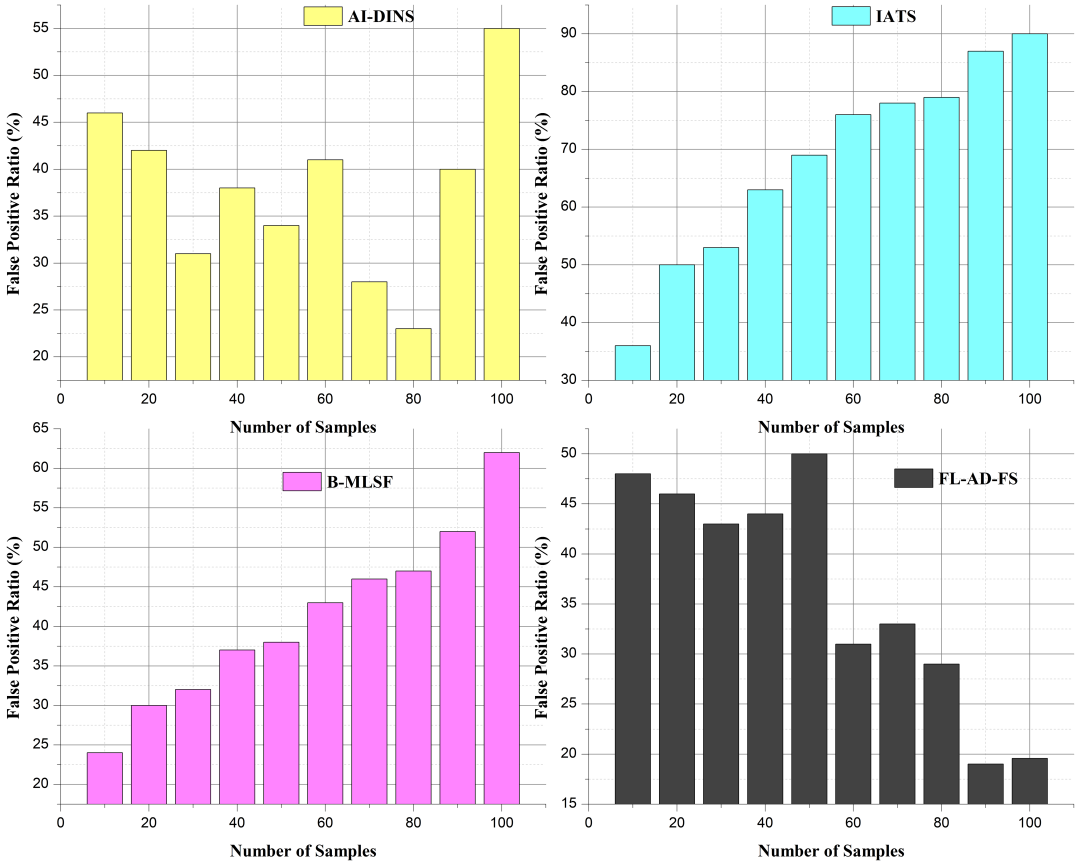

FIGURE 4 | Analysis of false positives.

TABLE 2 | Comparison of existing method and proposed method.

Aspects	A-DINS	IATS	B-MLSF	FL-AD-FS	Key features
Cybersecurity efficiency	81.85%	88.24%	90.67%	94.52%	Enhanced real-time anomaly detection with AI and federated learning
False positives	70.11%	38.90%	25.63%	18.57%	Reduced false alarms through AI-driven accurate threat identification
Detection accuracy	85.33%	89.45%	91.78%	93.38%	AI-powered precision anomaly detection for secure financial transactions
Latency reduction	79.75%	84.12%	91.33%	96.25%	6G-enabled edge computing ensures real-time threat detection
Financial transaction security	78.82%	82.67%	89.21%	95.33%	Decentralized and adaptive framework enhancing financial data protection

model time-dependent behaviors and sequential anomalies, making them ideal for analyzing temporal patterns in transaction flows where fraudulent activities often involve time-based irregularities. Autoencoders were chosen for their strength in unsupervised anomaly detection, as they learn to reconstruct normal transaction data and flag deviations as potential threats.

To further reduce computational overhead, the framework employs lightweight deep learning models with optimized architectures, such as pruned CNN-LSTM networks and quantized autoencoders, which maintain detection accuracy while reducing the size and complexity of the models. Additionally, asynchronous FL allows individual nodes to update the global model at staggered intervals rather than synchronously, avoiding system bottlenecks and ensuring smoother integration of updates even under high-volume data streams.

5 | Conclusion

Cybersecurity in university financial management will likely modify its paradigm with the entrance of 6G networks containing AI and Big Data. This paper introduces the FL-AD-FS system to improve real-time anomaly detection, data privacy, and financial transaction security using FL and 6G-enabled edge computing. The usefulness of the FL-AD-FS model, with a cybersecurity

efficiency of 94.52%, detection accuracy of 93.38%, and a latency reduction of 96.25%, is shown by actual data. False positives decline to 18.57%. Future developments might improve detection accuracy and add further security measures for complete protection. Integrating adaptive AI models into the FL-AD-FS architecture will be the main focus of future work to enhance real-time threat classifying and response systems.

Conflicts of Interest

The authors declare no conflicts of interest.

Data Availability Statement

Data sharing is not applicable to this article as no new data were created or analyzed in this study.

References

1. H. F. Ahmad, W. Rafique, R. U. Rasool, A. Alhumam, Z. Anwar, and J. Qadir, "Leveraging 6G, Extended Reality, and IoT Big Data Analytics for Healthcare: A Review," *Computer Science Review* 48 (2023): 100558.

2. A. Jahid, M. H. Alsharif, and T. J. Hall, "The Convergence of Blockchain, IoT and 6G: Potential, Opportunities, Challenges and Research Roadmap," *Journal of Network and Computer Applications* 217 (2023): 103677.

3. M. Yadav, U. Agarwal, V. Rishiwal, et al., "Exploring Synergy of Blockchain and 6G Network for Industrial Automation," *IEEE Access* 11 (2023): 137163–137187.

4. N. Kaur, N. Kshetri, and P. S. Pandey, "6AInets: Harnessing Artificial Intelligence for the 6G Network Security: Impacts and Challenges," 2024 preprint, arXiv, 7, February, https://doi.org/10.48550/arXiv.2404.08643.

5. A. V. Jha, B. Appasani, M. S. Khan, S. Zeadally, and I. Katib, "6G for Intelligent Transportation Systems: Standards, Technologies, and Challenges," *Telecommunication Systems* 86, no. 2 (2024): 241–268.

6. M. Arun, T. T. Le, D. Barik, et al., "Deep Learning-Enabled Integration of Renewable Energy Sources Through Photovoltaics in Buildings," *Case Studies in Thermal Engineering* 61 (2024): 105115.

7. H. Jahankhani, S. Kendzierskyj, and O. Hussien, "Approaches and Methods for Regulation of Security Risks in 5G and 6G," in *Wireless Networks: Cyber Security Threats and Countermeasures*, eds. H. Jahankhani and A. El Hajjar (Springer International Publishing, 2023), 43–70.

8. N. A. Alshaer and T. I. Ismail, "AI-Driven Quantum Technology for Enhanced 6G Networks: Opportunities, Challenges, and Future Directions," *Journal of Laser Science and Applications* 1, no. 1 (2024): 21–30.

9. S. S. Sefati, A. U. Haq, R. Craciunescu, S. Halunga, A. Mihovska, and O. Fratu, "A Comprehensive Survey on Resource Management in 6G Network Based on Internet of Things," *IEEE Access* 12 (2024): 113741–113784.

10. V. Ziegler, P. Schneider, H. Viswanathan, M. Montag, S. Kanugovi, and A. Rezaki, "Security and Trust in the 6G Era," *IEEE Access* 9 (2021): 142314–142327.

11. P. Porambage, G. Gür, D. P. M. Osorio, M. Liyanage, A. Gurtov, and M. Ylianttila, "The Roadmap to 6G Security and Privacy," *IEEE Open Journal of the Communications Society* 2 (2021): 1094–1122.

12. M. Zawish, F. A. Dharejo, S. A. Khowaja, et al., "AI and 6G Into the Metaverse: Fundamentals, Challenges and Future Research Trends," *IEEE Open Journal of the Communications Society* 5 (2024): 730–778.

13. T. Oleksandr, D. Oleksandra, and M. Anatolii, "Basic Technologies and Techniques ML/AI for Improving Physical Layer Security for 5g/6g Communications Systems," in *The 17th International Scientific and Practical Conference "System Analysis and Intelligent Systems for Management"*, eds. O. Tsopa, O. Dudka, and A. Merzlikin (International Science Group, 2023), 403–482.

14. M. M. Saeed, R. A. Saeed, M. Abdelhaq, R. Alsaqour, M. K. Hasan, and R. A. Mokhtar, "Anomaly Detection in 6G Networks Using Machine Learning Methods," *Electronics* 12, no. 15 (2023): 3300.

15. D. Varadam, S. P. Shankar, N. P. Nidhi, et al., "AI in 6G Network Security and Management," in *Reshaping CyberSecurity With Generative AI Techniques*, eds. B. Khan, H. Fatima, A. Qureshi, and S. Abdullah (IGI Global, 2025), 173–200.

16. Z. Zhou, M. Wang, J. Huang, S. Lin, and Z. Lv, "Blockchain in Big Data Security for Intelligent Transportation With 6G," *IEEE Transactions on Intelligent Transportation Systems* 23, no. 7 (2021): 9736–9746.

17. M. S. Akbar, Z. Hussain, M. Ikram, Q. Z. Sheng, and S. Mukhopadhyay, "6G Survey on Challenges, Requirements, Applications, Key Enabling Technologies, Use Cases, AI Integration Issues and Security Aspects," 2022, preprint, arXiv, 17, October, https://doi.org/10.48550/arXiv.2206.00868.

18. S. R. Gundu, P. Charanarur, K. K. Chandelkar, D. Samanta, R. C. Poonia, and P. Chakraborty, "Sixth-Generation (6G) Mobile Cloud Security and Privacy Risks for AI System Using High-Performance Computing Implementation," *Wireless Communications and Mobile Computing* 2022, no. 1 (2022): 4397610.

19. A. Kovari, "Synergizing 6G Networks, IoT, and AI: Paving the Way for Next-Generation Intelligent Ecosystems," *Journal of Engineering Science and Technology* 20, no. 1 (2025): 114–128.

20. D. R. Primmia, M. Mahabooba, J. Karpagam, K. Sharma, A. Singh, and S. Manoj, "The Development of 6-G Technology in Integration With AI Type of Synergy," in *2024 4th International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)* (IEEE, 2024), 248–253.

21. Growth Market Reports, "Airport 6G Network Readiness Market Market Research Report 2033," accessed July 16, 2025, https://datasetsearch.research.google.com/search?src=0&query=Integrating%20Big%20Data%20and%20AI%20%20in%206G&docid=L2cvMTF3eHR5X18yeg%3D%3D.