International Journal of Environmental Sciences
ISSN: 2229-7359
Vol. 11 No. 15s, 2025
https://www.theaspd.com/ijes.php

Anomaly Prediction Based On LSTM And Autoencoders Using Federated Learning In Financial Transactions- Survey

Gaurav Kumar[1], Dr. Pushpendra Kumar Verma[2]
[1]Research Scholar, SoCSA, IIMT University, Meerut, India 250002, gauravkumar.mrt@gmail.com
[2]Associate Professor, SoCSA, IIMT University, Meerut, India 250002, dr.pkverma81@gmail.com, https://orcid.org/0000-0003-2777-5626

Abstract
As more and more financial activities transition to digital platform, recognizing unusual transaction patterns has become an important and challenging task. Conventional centralized machine learning models for fraud detection bring with them significant challenges like data privacy and scaling. This survey investigates the promising combination of Long Short-Term Memory (LSTM) networks, Autoencoders and Federated Learning (FL) act as a powerful privacy-preserving solution for anomaly detection on financial transactions. Long Short-Term Memory (LSTM) models are a state-of-the-art choice for learning long range relations on sequential data whereas autoencoders are very efficient models which learn lower-dimensional state representations and pinpoint anomalous behavior. Federated Learning, in contrast, presents a decentralized model training mode in which collaborative learning can be conducted among banks and financial institutions without sharing confidential transaction information. This review discusses the state of the art, the key advances and the potential synergies of these methodologies. This inspires practical implementations of scalable and trustworthy AI-driven financial anomaly systems, as the movement towards an increasingly federated data ecosystem mandates secure and scalable solutions.
Keywords: *Anomaly Detection, LSTM Networks, Autoencoders, Federated Learning, Financial Fraud, Data Privacy.*

1. INTRODUCTION

The unchecked growth of online and mobile banking systems has led to an extraordinary increase on the volume, size and variety of financial data transactions. Digitization, as much as it increases operational efficiency and enables globalization, has also created an environment full of frauds. Fraud detection in these transactions is a difficult exercise because of the dynamicity and the changes in the patterns in which fraud takes place, the limited and insufficiently balanced distribution of fraud data, and the confidentiality of the information on finances.
The traditional rule/model-based fraud detection systems have severe adaptation and scalability limit detection issues. Such limitations also apply to the machine-learning methods. Machine learning in the prevailing architecture requires a centralization of data pooling, a fact that raises essential issues of privacy, data ownership, and consent with regard to legislative privacy, like GDPR and HIPAA [1]. Recent breakthroughs Used in financial technologies have brought the theory of deep learning- namely use of LSTM networks and Autoencoders to the scene as well as an inference scheme of sequence learning and representation learning. LSTM networks can handle any sequence, which includes transaction history, by maintaining time-dependent connections over long periods [2]. In its turn, autoencoders are also effective at finding anomalies through reconstructive error assessment. Such models, used with sufficient training, will reveal potential shifts in the user or transaction behavior that go undetected after the standard methods, improving the accuracy of fraud detection [3][4]. The introduction of Federated Learning is a paradigm shift in the machine-learning practices of distributed-data. Unlike the conventional preposition of concentrating sensitive data, FL allows the training of localized models at specific data sources. Such a design will boost the privacy and security of data, a consideration that is paramount in financial deals where reliability and compliance to financial rules are a must [5]. In the current review, the synergistic use of Least Short-Term Memory (LSTM) networks, Autoencoders and Federated Learning to anomalous event forecast in complicated transaction systems of a financial establishment are explored. Blending of these approaches has the promise to enhance prediction accuracy, maintain confidentiality of users and perform real-time fraud detection in complex, large-scale financial environments. The article provides a comprehensive literature review, synthesizes the recent developments and addresses methodological aspects of practical application, such as model convergence, efficiency of information dispersion, heterogeneity of the data and vulnerabilities to adversaries.

1.1. Objective

The present survey paper explores the pitfalls, constraints, and network performance implication which arise when using the federated learning (FL) approach to the anomaly detection in financial transactions in conjunction with long-short-term memory (LSTM) based autoencoder. Financial fraud detection systems face unique challenges, most remarkably, strict data privacy laws, non-identically distributed (non-IID) data distributions across organizations, and the necessity of real time adjustments to the fast-evolving fraud dynamics. Through the adoption of FL, the investigation is aimed at regulating the issues of privacy by allowing the training of the model jointly but at the same time prohibiting the transport of untreated data. However, the solution also entails challenges that include communication bottlenecks, resource-intensive calculations and some sort of trade-offs between privacy protection, say, differential privacy and model accuracy. The evaluation of the hybrid FL structures and privacy-preserving methods such as the federated meta-learning and secure aggregation will be the key aims to overcome these drawbacks. Finally, a practical implication of the research aims at providing findings that can inform the use of scalable and privacy-compatible FL models to detect financial fraud.

1.2. Overview of Financial Fraud and Anomaly Detection

The financial fraud, which includes credit card fraud, money laundering, identity theft and insider trading is a threat that continues to mutate and affect the banking institutions, the government and the individual users in a serious way. The association of certified fraud examiners (ACFE) has estimated that the worldwide cost of fraud is more than trillions of dollars annually. On the one hand, the growth in digital payment services that have appeared with online banking, mobile payment systems, and online stores has also left the scope of possible criminal activity since the perpetrators of crimes can potentially increase the range of possible victims [6]. Anomaly detection can be defined as the process of systematically identifying transactional anomalies that differ significantly either with the typical behavior of a single user or of the general trend in the transactions recorded in a given financial system. Such anomalies could be the indication of fraudulent or other aberrations of system malfunctions. Practically, anomaly detection systems work as warning systems, warning investigators about a possibility of fraudulent behavior, before damage is necessarily caused [7].

1.2.1 Traditional Approaches

The conventional methods that were used by financial companies in fraud identification involved the rule-based systems and statistical models [8]. However, these methodologies have some weaknesses. Rule based systems are anchored on predetermined, rigid, and if-then rules that fraudsters can easily beat down, and produce high false positives. Statistical models like logistic regression can deal better with previous data, but they cannot effectively detect non-linear trends, and are not capable of adjusting to new forms of fraud. Such methods are becoming inappropriate in a world of modern and advanced plans in large digitized dealings. To solve this, institutions are resorting to complex solutions, such as LSTM networks to analyze the patterns in time and autoencoders to detect anomalies. Moreover, federated learning has shown its prominence as a technique of privacy maintenance which allows collaborating between institutions without exchange of sensitive data [9]. In unison, the techniques provide enhanced flexibility, on-time learning, and precision--that are crucial in the current fast-changing financial market.

1.2.2 Machine Learning

The very spread of machine learning has extended the collection of algorithms of identifying financial misconduct, providing additional flexibility and the greater reliance on data. Ensemble decision trees and SVMs have been shown to outperform conventional rule-based fraud detection systems in case supervised learning techniques form part of the testing environment [10] [11]. They are effective due to the ability to discover complicated patterns and non-linearity's and consequently enhance the accuracy of prediction. nonetheless these methods are based on large labeled data, where instances of fraud are often limited as compared to true transactions. This uniqueness will threaten to institutionalize discrimination and may hinder the detection of non-observed fraudulent activities. In addition, the models, which are developed based on old data, could fail with emerging tactics when retraining is less common and expensive. Therefore, other forms of paradigms- unsupervised and semi-supervised learning have come to the fore. K-means clustering is an example of an anomaly-detecting technique that finds anomalies as deviations of transaction behaviors, and autoencoders together with one-class SVMs anomaly-detecting techniques flag anomalies through reconstruction errors and one-class outlier detection. A practical compromise is provided by semi-supervised strategies in which the learning process proceeds based on normative transactions and then deviations are identified [9]. All these practices can increase fraud detection by enabling the system to adapt to new hazards and reduce the dependence on labelling, which is labor-intensive.

1.3. Deep Learning in Anomaly Detection: LSTM and Autoencoders

The benefits of deep learning have led to its foundations becoming a revolutionary platform in the detection of anomalies, especially in cases that the classical statistical procedures together with the classical machine-learning methods are impaired by limitations related to the exploration of complex, high-dimensional and non-linear databases about financial transactions. Relative to the traditional models, deep-learning structures are capable of automatically identifying complex correlations and learning latent characteristics unaided by manually engineered changes or inflexible suppositions. In this domain, the LSTM networks and Autoencoders continue to be among the most commonly embraced tools. Both have proved to be quite useful in time modeling and painting of representations on normal behavior patterns and thus these two are very appropriate in the process of finding out anomalies in either transaction that are financial oriented as in the discussion ahead. figure 1.

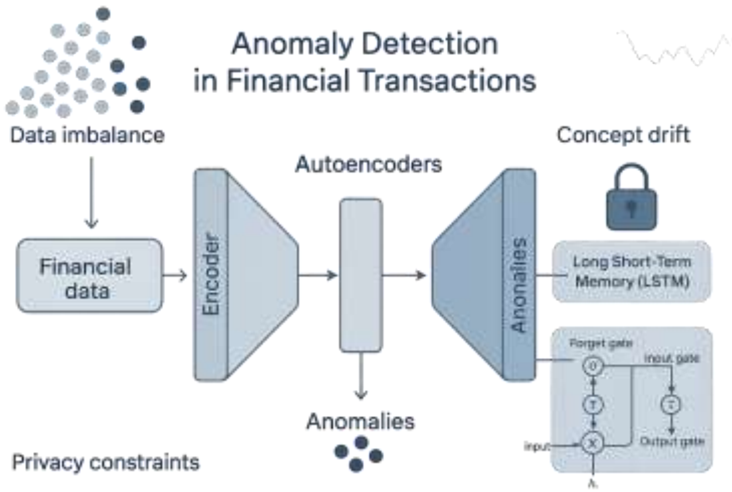

Fig 1: Anomaly detection in financial transactions

1.3.1. Long Short-Term Memory (LSTM) Networks

The Long Short-Term Memory networks have also proven to be especially successful in terms of detecting financial fraud due to the fact that they bypass the limitations that are characteristic of the traditional Recurrent Neural Networks being subjected to sequential data [12]. Special kinds of gating structures, which are delivered through the ability to deploy input, forget and output gates allow specific control over the flow of information and by so doing long-term dependencies, which exist within the transactional history are maintained. This aspect makes LSTMs unrivalled at both capturing static attributes of transactions, as well as capturing dynamic temporal patterns like spending rates and trends. LSTMs can learn an extrapolation of common financial behavior to spot invisible anomalies that can alert about fraud, all in a noise-tolerant manner. Their ability to support complex seasonality and attempt to do analysis in real time makes them important in the detection of the individual level as well as population level fraud. These advantages, however, come at the expense of adversities such as; they are computationally intensive, they require precise hyper parameter tuning, and they are vulnerable to input sequence quality measures that require intelligent deployment to result in reasonable trade-offs between accuracy and functioning performance in real world financial systems.

1.3.2. Autoencoders

An autoencoder is an eminent unsupervised method of detecting financial frauds as it builds a condensed model of typical transactional behavior [13] [14]. Here, the neural network architecture has been seen to do well in reconstruction of a normal financial behaviour and produce significant reconstruction errors on anything anomalous, thereby acting as an anomaly detection mechanism as well. Different instantiations of autoencoders can be tailored to a particular detection concern: in basic autoencoders the key task is dimensionality reduction; de-noising autoencoder versions make them more robust; VAEs add ideas of probabilistic modelling; recurrent autoencoders operate on sequence data with LSTM cells. The framework also offers a number of benefits to financial institutions including its ability to identify emerging types of fraud where labelled examples are unavailable, its adaptability to changes in types of threats as well as the scalability to different levels of transactional analysis. Moreover, their unsupervised nature makes them especially applicable in the real-world application scenario where it is difficult to label and exhaust the conventional fraud.

1.4. Federated Learning Architecture

1.4.1 Core Principles of Federated Learning

The decentralized process of training artificial intelligence models in the area of financial fraud detection, which allows combining efforts to develop co-created models without transferring raw data. The paradigm eliminates data silo effect by spreading training across institutes and provides data privacy due to the usage of encrypted model updates, therefore, it is easier to comply with the compliance policies like GDPR, PCI-DSS. The general process entails rounds where local models are trained using local, confidential datasets and their parameters are collectively consolidated, through such approaches as Federated Averaging (FedAvg), to enhance a global model. It is further enhanced by advanced security and performance features like differential privacy and the adaptive optimization. The framework enables banks to strike the right balance between global perspective through collective intelligence and customization at local level-such as dealing with urban card frauds as opposed to rural skimming of the ATMs. Therefore, the privacy-preserving architecture provides adaptable, highly scalable, regulation-compatible systems of detecting fraud.

Such a technique is especially disruptive insofar as it allows training machine learning models to take advantage of geographically diversified sources of data without jeopardizing privacy or enforcing data sovereignty. The advantage is particularly critical in the financial industry where data sensitivity and compliance limits tend to degrade centralized machine learning projects. Federated learning (FL) architecture is shown in figure 2. The goal of FL is the development of the model with consideration of such constraints as the capacities of local data storage and computation restrictions and frequent updates of the parameters of the model which are to be transmitted to a cloud parameter server.

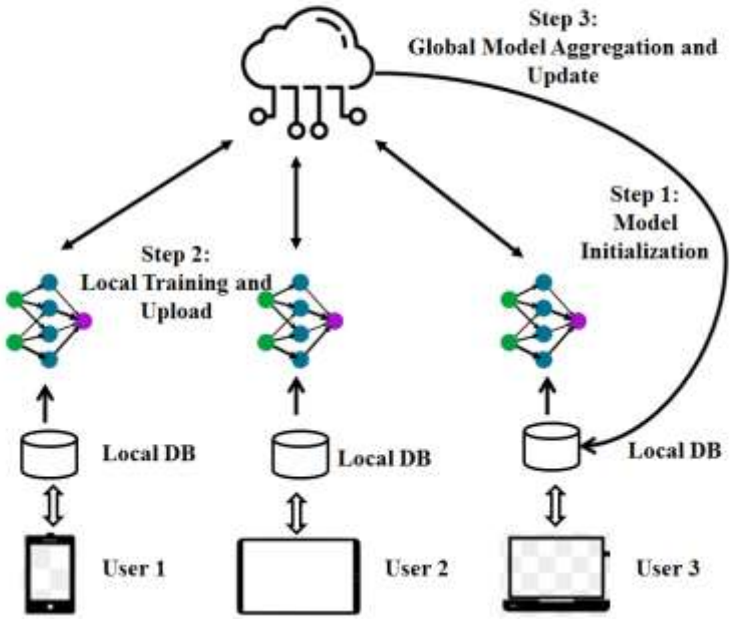

Fig 2: Federated Learning System Architecture

1.4.2 Privacy preserving in Federated Learning

Federated learning is a system that incorporates various methods of privacy protection to allow the realization of secure detection of financial fraud in the framework of strict regulatory demands. Differential privacy randomly adds noise to update of models, algorithmically enforcing the impossibility of grouping individual transactions, even as it maintains the accuracy of the detectors, so long as parametric parameterization is well trained to trade privacy implied and its performance outcomes. Secure aggregation, in its turn, uses the cryptographic protocols to compound update data of several institutions without revealing information of any of them, which allows even the competing banks to cooperate securely. Homomorphic encryption can be used when security requirements are the most stringent since computations can be performed on data which has to be fully encrypted, and secure multi-party computation can allocate processing across parties that are highly dissimilar to prevent any party being able to recreate confidential information. Collectively, the strategies can establish nested privacy safeguards to cover a variety of risk scenarios, where financial institutions can work cautionary fraud-detection models and maintain high levels of data secrecy and regulatory standards through their federated networks. The choices of the component involve the trade-offs about the strength of security component and performance of such components and the real life banking requirements.

1.5 Principles and Challenges

As financial services are increasingly digitized, transactional data that can be analyzed has considerably grown. As much as such abundance of data allows creation of complex models to detect fraud, it also increases information privacy, protection and regulatory compliance issues. An innovative solution to such problems is Federated Learning, a collaborative solution where Multimodal Training is possible, but without any need to exchange or centralize raw data externally [15] [16].

Nonetheless, there are unique challenges of applying federated learning in the financial context and need special care. Banking data in general is not homogenous, which causes a high level of variability in patterns of transaction, customer behavior and the nature of fraud between different institutions thus making it difficult to provide a universally effective, one size fits all solution. The training is also a very resource-intensive process in terms of network consumption since there will be constant transmission of updated complex models across the bank network, which may result in an overloading problem in the communication infrastructure especially with high-end detection models. Despite the privacy guaranteed to be maintained, the security mechanism is still vulnerable to unknown security exploits where confidential data can be deduced based on shared updates, so other security precautions to prevent such exploits are required, and they invariably systematically slow down the processing mechanism. Collaborative training can also be disrupted by operational disruptions, e.g. where the participating banks temporarily disconnect themselves to the network. There is also the layer of legal and governance: the clarification of ownership, accountability, and compliance is still a topic of discussion among institutions that are experimenting with this technology. Such intertwined limitations demand both careful and perceptive planning procedures in order to exploit all the potential of federated learning in the financial industry.

1.6 Federated Learning Limitations and Threat Models in Federated Learning

Among the limitations imposed by federated learning, which enables the training of models in a decentralized manner and maintains data privacy, there are the following. Client node heterogeneity may be caused by unequal availability of computational resources, network bandwidth and underlying data distributions, which may hamper efficiency and even cause bias in the resulting trained models. The high communication overhead is another limitation as several communication cycles between server and clients are involved and this may turn out to be resource demanding particularly where the bandwidth is low. Even in local data retention, the privacy is not complete: the model updates can lead to an inference attack by disclosing confidential information. These issues are also very hard to mitigate since malicious customers can corrupt the model by uploading corrupted updates. In addition, even in non-IID (non-independent and identically distributed) data, whether a high model accuracy could be maintained and convergence could be achieved is an open research question [17] [18]. Taken together, these problems indicate that additional algorithms and protocols are needed that could make federated learning more efficient, secure, and flexible to be deployed in practice settings.

Table 1: Threat Models in Federated Learning

Threat Model	**Adversary Type**	**Objective**	**Attack Method**	**Potential Impact**	**Mitigation Strategies**
Honest-but-curious server	Semi-honest central party	Extract sensitive info from updates	Analyze aggregated gradients	Privacy leakage of client data	Secure Aggregation, Homomorphic Encryption

Malicious clients	Rogue participants	Poison model or steal information	Submit false updates, analyze gradients	Model corruption, privacy breaches	Robust aggregation (Krum, Median), Client screening
External attackers	Network eavesdroppers	Intercept communications	MITM attacks, data tampering	Data theft, model integrity compromise	TLS encryption, Digital signatures
Gradient leakage	Curious server/clients	Reconstruct training data	Gradient inversion attacks	Complete data reconstruction	Differential Privacy, Gradient masking
Membership inference	Data analysts	Identify training set members	Analyze model outputs/updates	Privacy violations, regulatory risks	Strong DP guarantees, Output perturbation
Model inversion	Skilled adversaries	Extract sensitive features	Reverse-engineer model decisions	Exposure of transaction attributes	Model hardening, Input perturbation

1.7 Trade-Offs Between Privacy and Performance

The performance of federated learning is measured through a combination of traditional machine learning metrics and system-specific indicators that reflect its decentralized nature. At the core, the model is assessed through metrics including accuracy, F1-score, AUC and loss functions like cross-entropy or mean squared error., which help assess the quality of predictions across all clients. However, since data is non-uniformly distributed, personalization accuracy, how well the global model adapts to local client data is also a critical measure. In terms of communication efficiency, federated learning systems are assessed by the quantity of communication rounds required for convergence, the total volume of information sent, and the overall network bandwidth consumed. System efficiency includes metrics like local computation time per client, energy usage (especially for mobile or edge devices), and the impact of stragglers or idle clients who slow down training. Moreover, robustness and fairness are increasingly important: the variance in model performance across clients can indicate imbalances, and the system's ability to withstand malicious updates or client dropouts is crucial for reliable deployment. These multifaceted performance metrics provide a more holistic understanding of how well federated learning works in real-world scenarios. Different techniques require balancing these trade-offs is crucial for practical FL deployment. Implementing privacy-preserving techniques in FL inevitably introduces trade-offs between privacy, model performance and efficiency as given in table 2.

Table 2: Trade-offs

Technique	Privacy Benefit	Trade-off	Impact
Differential Privacy (DP)	Protects individual data points via noise injection	Noise reduces model accuracy	May degrade performance in noise-sensitive models (e.g., LSTMs, anomaly detection)
Homomorphic Encryption (HE)	Facilitates calculations on data that is encrypted	Significant computational demands	Slower training, impractical for real-time or large-scale deep learning
Secure Multi-Party Computation (SMPC)	Prevents single-party data exposure	Increased communication latency	Challenging for high-dimensional models due to coordination delays
Secure Aggregation (SecAgg)	Hides individual client updates	Requires cryptographic key management	Scalable but adds complexity in key distribution and synchronization
Blockchain (for auditability)	Immutable, transparent record of transactions	Adds architectural complexity	Higher storage and consensus delays, but enhances trust in FL processes

2. LITERATURE REVIEW

With the study developments in anomaly prediction using federated learning, [19] study improves federated anomaly detection by utilizing autoencoders along with a global threshold based on summary statistics. By consolidating data from both standard and irregular datasets, it enhances the precision of the threshold. and outperforms existing methods on multiple datasets despite Non-IID data challenges. [20] propose an AI agent-based framework combining LSTM, autoencoders, and federated learning for financial transaction anomaly prediction. Achieves an 89% accuracy improvement over rule-based systems, with real-time detection and scalability demonstrated in a banking case study. [21] introduces a gradient-based and autoencoder-driven framework to detect poisoned data in federated learning. It improves detection accuracy by 15% and maintains low false positives, validated on MNIST and CIFAR-10 datasets, showing strong performance across sectors like healthcare and finance. [22] design a filtered aggregation algorithm in federated learning to improve anomaly detection by down-weighting unreliable local models. This enhances model accuracy and privacy, especially in sensitive domains like finance. [23] introduces an autoencoder-classifier hybrid using the FedSam framework for intrusion detection. It improves anomaly detection in federated learning by effectively handling heterogeneous client data in cybersecurity contexts. [24] presents Ensemble SVDD and Support Vector Election (SVM) based anomaly detection methods for federated learning. Though not focused on financial data, these techniques show strong performance across distributed environments. In defending data privacy attacks, [25] focuses on anomaly detection in data on water levels collected over time from IoT sensors using deep LSTM Autoencoders, rather than financial transactions or federated learning. It emphasizes an unsupervised approach that leverages reconstruction error to identify anomalies. The study also proposes an unconventional method for calculating reconstruction error, which reduces false positives and improves anomaly detection accuracy, particularly in noisy datasets. [26] investigates the use of LSTM and Bi-LSTM models for identifying anomalies., showing strong performance in capturing temporal patterns. However, it does not involve federated learning or focus on financial transaction data. [27] Combines autoencoders and LSTM networks used for identifying anomalies in electric vehicle time series data. While it improves accuracy, it does not incorporate federated learning or address financial contexts. [28] introduces Liquid Time-Constant Autoencoders (LTC-AEs) for semi-supervised anomaly detection, outperforming several baseline models. Still, it lacks application to federated learning or financial transaction anomaly prediction.

For FL model performance enhancement, [29] proposes an anomaly detection method combining Deep Reinforcement Learning (DRL), Variational Autoencoders (VAE), Active Learning, and LSTM to identify new anomaly classes with limited labeled data. It shows strong results on time series datasets but does not involve federated learning or focus on financial transactions. [30] uses LSTM for real-time anomaly detection in IoT healthcare, emphasizing accuracy and data security. While effective in medical contexts, it does not incorporate autoencoders, federated learning, or financial applications. [31] introduces LogLVAE, which combines LSTM and VAE for log-based anomaly detection. Though it excels in detecting anomalies in system logs, it does not address federated learning or financial transaction data. [32] proposes a Conv-LSTM Encoder-Decoder model for unsupervised human anomaly detection. It effectively learns spatiotemporal features to detect behavioral anomalies with high accuracy, but it does not involve federated learning or financial transaction data. [33] design FedAA (Federated Learning with Attention Aggregation) for detecting anomalies in IoT networks using autoencoders. While not focused on financial transactions or LSTM integration, FedAA improves model robustness and defense against data poisoning, showing strong performance across multiple IoT datasets. With focused on the fact that the performance, [34] introduces trust-based anomaly detection in federated learning using Reputation and Trust metrics, aimed at detecting anomalies in edge units, particularly in financial applications. It supports any server aggregation method but does not involve LSTM or autoencoders. [35] applies Bidirectional LSTM and autoencoders for anomaly detection in commercial load data, outperforming benchmark methods. However, it does not incorporate federated learning or focus on financial transactions. [36] proposes an unsupervised LSTM-Autoencoder approach for general time series anomaly detection based on reconstruction error. It shows strong results but lacks a focus on federated learning or financial data. [37] survey studies highlighting the growing adoption of federated learning in financial fraud detection [38] discusses deep learning advancements in anomaly detection. [39] compares

AE-LSTM and DNN-LSTM for detecting anomalies in space applications, demonstrating the superior performance of AE-LSTM.

3. METHODS

The survey employed a systematic literature review of peer-reviewed studies (2023–2024) from IEEE Xplore, Springer, and Google Scholar. Key search terms included Federated Learning, Anomaly Detection, LSTM, Autoencoders, Financial Fraud, Privacy-preserving Learning, and IoT Security. Inclusion criteria prioritized studies using LSTM, autoencoders, FL, or hybrid models with experimental validation, while excluding works without measurable outcomes. Selected papers were categorized by methodology (e.g., LSTM variants, autoencoders, FL frameworks) and performance metrics like accuracy and F1-score.

3.1 Selection Criteria

Inclusion: Peer-reviewed studies addressing anomaly detection with LSTM, Autoencoders, FL, MPC (Multi-Party Computation), or hybrid models.

Exclusion: Articles lacking experimental evaluation or not reporting measurable outcomes.

Relevant studies were included after applying these criteria. The selected works were categorized based on the methods used (e.g., LSTM variants, Autoencoders, FL-based models) and the reported results (accuracy, F1-score, detection improvement, privacy preservation).

3.2 Accuracy

Accuracy evaluates the ratio of accurate predictions, including the correctly recognized normal transactions (true negatives) and fraud instances (true positives), among all transactions assessed, computed as

Accuracy = (True Positives + True Negatives) / Total Predictions

Total predictions consist of True positives refer to instances that have been accurately predicted as positive, while true negatives are instances accurately classified as negative. False positives are cases that have been mistakenly labeled as positive, and false negatives are those that have been incorrectly classified as negative. It serves as a straightforward indicator of overall model reliability, where high accuracy (e.g., 99.7% in LSTM-Autoencoder models) suggests strong general performance. However, this metric becomes highly misleading in imbalanced datasets like financial transactions, where fraud cases are extremely rare (e.g., <0.1% of transactions). In such scenarios, a model could achieve deceptively high accuracy (e.g., 99.9%) by simply labeling all transactions as "normal" while failing to detect any actual fraud a critical flaw that renders accuracy insufficient as a standalone metric for fraud detection systems.

3.3 F1 Score

The F1 Score assess a model's capability to uphold equilibrium between accuracy (the ratio of identified anomalies which are true fraud) and recollect (rate of genuine fraud acts accurately detected), determined as the harmonic mean:

F1 = 2 × (Precision × Recall) / (Precision + Recall)

This metric is defined as the harmonic mean of precision and recall. Precision refers to the proportion of correctly predicted positive cases to the overall number of predicted positives, while recall (also known as sensitivity) evaluates the proportion of actual positives that the model has correctly identified. This measure is vital in fraud detection, where both false positives (wrongly blocking legitimate transactions that can harm user trust) and false negatives (failing to detect actual fraud, leading to financial losses) have significant consequences. An F1 Score near 1.0 (99%) achieved in advanced frameworks like hybrid LSTM-autoencoders signals an optimal equilibrium between these competing priorities. Crucially, the F1 Score is a much dependable metric instead of accuracy when dealing with imbalanced datasets., as it remains robust even when fraud incidence is exceptionally rare (e.g., 0.01% of transactions), where accuracy metrics often mislead by favoring trivial "always normal" predictions.

4. RESULT

The surveyed works demonstrate significant progress in anomaly detection, particularly through the combination of LSTM, Autoencoders, and privacy-preserving frameworks like FL and MPC. The best models (e.g., LSTM-AE + FL) achieved >99% F1 while using encryption/aggregation to preserve privacy demonstrating that performance and security can coexist. Below, we summarize the findings by method category:

Method	Peak Accuracy/F1	Other Notable Results
FAF-LSTM [40]	+39.22% accuracy	Stealthy attack detection in FIoT
LSTM-AE Hybrid [42]	99% F1-score	OC-SVM & IF integration
LSTM-AE [46]	99.7% accuracy	High detection with AE
Fed-LSTM [47]	98.9% accuracy	Outperforms RNN, SVM, CNN
LSTM-GAN [48]	Anomaly Score 0.76	1.25% anomalies detected
FL for HPC [49]	F-score from 0.31 to 0.84	Data collection time reduced
MPC with FL [41]	AUPRC 0.7	Privacy-preserving enhancement
Specialized Neural Nets [43]	40% accuracy boost	35% detection time reduction
Deep Encoder NN [51]	90.81% F1 Score	High precision
Random Forest NN [52]	95% accuracy	yielded highest accuracy
Logistic Regression, Naïve Bayes [53]	98.99% accuracy	Reduce detection time
FL-Anomaly Network Detection [54]	97% accuracy	Increased precision
Isolation Forest [55]	26% accuracy	Increase fraud detection

5. DISCUSSION

5.1 LSTM and LSTM-based Approaches

LSTM remains a core technique due to its capacity for sequential data modeling where [40] define FAF-LSTM for Federated IoT (FIoT) environments, achieving up to 39.22% improvement in anomaly detection compared to isolated LSTM models, particularly effective for stealthy attacks. [44] applied LSTM-based unsupervised anomaly detection, reporting an F1-score improvement from 0.307 to 0.815 and AUC increase from 0.368 to 0.77. [47] implemented Fed-LSTM, which surpassed RNN, SVM, and CNN with a 98.9% accuracy, showing the superiority of FL-integrated LSTM. [48] leveraged LSTM-GANs for enhanced anomaly detection, integrating reconstruction loss, latent distance, and discriminator score. The method detected 106 anomalies, accounting for 1.25% of the dataset, with a mean anomaly score of 0.7621.

5.2 Autoencoders and Hybrid LSTM-AE Models

Autoencoders, especially when combined with LSTM, demonstrate powerful anomaly detection performance like [45] achieved an impressive 99% F1-Score in anomaly detection by combining LSTM-AE, One-Class SVM (OC-SVM), and Isolation Forest (IF). [46] reported 99.7% accuracy and 89.1% F1-score using LSTM-AE, emphasizing the strength of this hybrid in outlier detection. [42] enhanced LSTM and Autoencoders with MSD (Mean Squared Deviation) and MAD (Median Absolute Deviation) methods, reaching a 97% F1-score using homomorphic encryption (HE-128 bit) with low computational overhead. [43] demonstrated a 35% reduction in detection time and 40% accuracy improvement over traditional anomaly detection methods by integrating Autoencoders with specialized neural networks.

5.3 Federated Learning and Privacy-Preserving Techniques

Preserving data privacy without compromising detection accuracy is critical where [41, 50] applied Multi-party Computation (MPC) with FL, boosting AUPRC from 0.6 to 0.7 while minimizing privacy leakage during training. [49] showcased FL's effectiveness in anomaly detection for High-Performance Computing (HPC) systems, reducing training data collection time from 4.5 months to 1.2 weeks and improving F-score from 0.31 to 0.84.

6. CONCLUSIONS AND FUTURE SCOPE

The financial sector's digital transformation has ushered in both remarkable conveniences and increasingly sophisticated fraud threats, exposing critical gaps in traditional detection systems that rely on centralized data processing and struggle to adapt to evolving attack patterns. The advancement of LSTM networks, autoencoders, and federated learning can be regarded as an impressive step on fraud detection since these methods may combine temporal pattern recognition, effective data compaction, and privacy-preserving cooperation. New scholarly studies have affirmed the fact the such an arrangement enables the financial system to substantiate their countermeasures on a shared basis and engage in practice as per the strict GDPR and PCI-DSS standards. Training the system with highly divergent, decentralized data sets trains it to identify new forms of emerging fraud that traditional approaches are unable to do. Its privacy-by-design architecture additionally ensures the institutional trust by the implementation of data security. No matter that, however, wider application is limited by a number of aspects: the computational cost of LSTM-autoencoder frameworks on the mobile banking infrastructure, the dialectic in data privacy and data quality of analysis, hazy network connectivity that can disturb the training process, and a lack of standardized benchmarking practices. In modern studies attempts are made to mitigate these shortcomings through federated meta-learning adaptive privacy designs, a hybrid architecture, and explainability models. Specifically, it is worth mentioning the blockchain-driven collaboration that brings the transparent and accountable process of data exchange across intrafirm boundaries. These technologies are only improving, and as they do, fraud prevention shows the potential to achieve success in addition to building an ethical AI paradigm in finance where security, privacy, and regulatory compliance are used in parallel with each other. Whether federated learning will be the new standard of trusted and collaborative fraud detection in the digital economy will be based on how well the industry can solve the technical and operational problems connected with it.

REFERENCES

[1] Agrawal, S., Sarkar, S., Aouedi, O., Yenduri, G., Piamrat, K., Alazab, M., Gadekallu, T. R. (2022). Federated Learning for intrusion detection system: Concepts, challenges and future directions. *Computer Communications*, 195, 346-361. https://doi.org/10.1016/j.comcom.2022.09.012

[2] Ullah, I., & Mahmoud, Q. H. (2022). Design and Development of RNN Anomaly Detection Model for IoT Networks. *IEEE Access*, 10, 62722–62750. https://doi.org/10.1109/ACCESS.2022.3176317

[3] Pan, X. (2022). Time series data anomaly detection based on LSTM-GAN. *Frontiers in Computing and Intelligent Systems*, 1(2), 35–37. https://doi.org/10.54097/fcis.v1i2.1701

[4] Rezaiezadeh Roukerd, F., & Rajabi, M. M. (2024). Anomaly detection in groundwater monitoring data using LSTM-Autoencoder neural networks. *Environmental Monitoring and Assessment*, 196, 692. https://doi.org/10.1007/s10661-024-12848-z

[5] Ahmad, W., Vashist, A., Sinha, N., Prasad, M., Shrivastava, V., & Muzamal, J. H. (2025). Enhancing Transparency and Privacy in Financial Fraud Detection: The Integration of Explainable AI and Federated Learning. In W. Feng, N. Rahimi, & V. Margapuri (Eds.), *Software and Data Engineering. SEDE 2024* (pp. 135-150). Springer, Cham. https://doi.org/10.1007/978-3-031-75201-8_10

[6] Crépey, S., Lehdili, N., Madhar, N., & Thomas, M. (2022). Anomaly Detection in Financial Time Series by Principal Component Analysis and Neural Networks. *Algorithms*, 15(10), 385. https://doi.org/10.3390/a15100385

[7] Darban, Z. Z., Webb, G. I., Pan, S., Aggarwal, C. C., & Salehi, M. (2022). Deep learning for time series anomaly detection: A survey. *arXiv preprint arXiv:2211.05244*. https://doi.org/10.48550/arXiv.2211.05244

[8] Sanober, S., Alam, I., Pande, S., Arslan, F., Rane, K. P., Singh, B. K., & Shabaz, M. (2021). An Enhanced Secure Deep Learning Algorithm for Fraud Detection in Wireless Communication. *Wireless Communications and Mobile Computing*, 2021, 6079582. https://doi.org/10.1155/2021/6079582

[9] Bukhari, S. M. S., Zafar, M. H., Houran, M. A., Qadir, Z., Moosavi, S. K. R., & Sanfilippo, F. (2024). Enhancing cybersecurity in Edge IIoT networks: An asynchronous federated learning approach with a deep hybrid detection model. *Internet of Things*, 27, 101252. https://doi.org/10.1016/j.iot.2024.101252.

[10] Antwarg, L., Miller, R. M., Shapira, B., & Rokach, L. (2021). Explaining anomalies detected by autoencoders using Shapley Additive Explanations. *Expert Systems with Applications*, 186, 115736. https://doi.org/10.1016/j.eswa.2021.115736

[11] Lin, T. H., & Jiang, J. R. (2021). Credit Card Fraud Detection with Autoencoder and Probabilistic Random Forest. *Mathematics*, 9(21), 2683. https://doi.org/10.3390/math9212683.

[12] Singh, M. T., Prasad, R. K., Michael, G. R., Kaphungkui, N. K., & Singh, N. H. (2024). Heterogeneous Graph Auto-Encoder for Credit Card Fraud Detection. *arXiv preprint arXiv:2410.08121*. https://doi.org/10.48550/arXiv.2410.08121

[13] Bampoula, X., Siaterlis, G., Nikolakis, N., & Alexopoulos, K. (2021). A Deep Learning Model for Predictive Maintenance in Cyber-Physical Production Systems Using LSTM Autoencoders. *Sensors*, 21(3), 972. https://doi.org/10.3390/s21030972

[14] Jeon, S., Kang, J., Kim, J., & Cha, H. (2023). Detecting structural anomalies of quadcopter UAVs based on LSTM autoencoder. *Pervasive and Mobile Computing*, 88, 101736. https://doi.org/10.1016/j.pmcj.2022.101736.

[15] Nardi, M., Valerio, L., & Passarella, A. (2022). Anomaly Detection through Unsupervised Federated Learning. *arXiv preprint arXiv:2209.04184*. https://doi.org/10.48550/arXiv.2209.04184.

[16] Sater, R. A., & Hamza, A. B. (2021). A Federated Learning Approach to Anomaly Detection in Smart Buildings. *ACM Transactions on Internet of Things*, 2(4), Article 28. https://doi.org/10.1145/3467981.

[17] Aljunaid, S. K., Almheiri, S. J., Dawood, H., & Khan, M. A. (2025). Secure and Transparent Banking: Explainable AI-Driven Federated Learning Model for Financial Fraud Detection. *Journal of Risk and Financial Management*, 18(4), 179. https://doi.org/10.3390/jrfm18040179.

[18] Zheng, R., Sumper, A., Aragüés-Peñalba, M., & Galceran-Arellano, S. (2024). Advancing Power System Services With Privacy-Preserving Federated Learning Techniques: A Review. *IEEE Access*, 12, 76753-76780. https://doi.org/10.1109/ACCESS.2024.3407121

[19] Laridi, S., Palmer, G. M., & Tam, K.-M. M. (2024). Enhanced federated anomaly detection through autoencoders using summary statistics-based thresholding. *Dental Science Reports*, 14(1). https://doi.org/10.1038/s41598-024-76961-2.

[20] Rayarao, S. R. (2024). Revolutionizing Transaction Security with AI Agents: A Predictive Approach to Anomaly Detection. *SSRN*. http://dx.doi.org/10.2139/ssrn.5076974

[21] Alsulaimawi, Z. (2024). Federated Learning with Anomaly Detection via Gradient and Reconstruction Analysis. *arXiv.Org, abs/2403.10000*. https://doi.org/10.48550/arxiv.2403.10000.

[22] Bhat, P., M M, M. P., & Pai, R. M. (2023). Anomaly detection using Federated Learning: A Performance Based Parameter Aggregation Approach. *2023 3rd International Conference on Intelligent Technologies (CONIT)*, 1-6. https://doi.org/10.1109/CONIT59222.2023.10205549.

[23] Vucovich, M., Tarcar, A. K., & Rebelo, P. (2023). Anomaly Detection via Federated Learning. *2023 33rd International Telecommunication Networks and Applications Conference (ITNAC)*, 259-266. https://doi.org/10.1109/ITNAC59571.2023.10368517

[24] Frasson, M., & Malchiodi, D. (2024). Support Vector Based Anomaly Detection in Federated Learning. *arXiv preprint arXiv:2407.03920*. https://doi.org/10.48550/arxiv.2407.03920.

[25] Githinji, S., & Maina, C. W. (2023). Anomaly Detection on Time Series Sensor Data Using Deep LSTM-Autoencoder. *2023 IEEE AFRICON*, 1-6. https://doi.org/10.1109/AFRICON55910.2023.10293676.

[26] Fadili, Y., El Yamani, Y., Kilani, J., El Kamoun, N., Baddi, Y., & Bensalah, F. (2024). An Enhancing Timeseries Anomaly Detection Using antitrust-Based Anomaly Detection in Federated Edge Learning. *2024 IEEE World AI IoT Congress (AIIoT)*, 273-279. https://doi.org/10.1109/AIIoT61789.2024.10578967.

[27] R. Sathe and S. Shinde,(2024), "A Deep Learning Framework for Effective Anomaly Detection in Time Series Data," *2024 4th Asian Conference on Innovation in Technology (ASIANCON)*, Pimari Chinchwad, India, 2024, pp. 1-7, doi: 10.1109/ASIANCON62057.2024.10837697.

[28] R. S. Sailesh, M. S. K, P. J and S. S,(2024), "LTC-AE: Liquid Time Constant Autoencoders for Time Series Anomaly Detection," 2024 *IEEE International Conference on Information Technology, Electronics and Intelligent Communication Systems (ICITEICS)*, Bangalore, India, 2024, pp. 1-6, doi: 10.1109/ICITEICS61368.2024.10624814.

[29] B. Golchin and B. Rekabdar, (2024), "Anomaly Detection In Time Series Data Using Reinforcement Learning, Variational Autoencoder, and Active Learning," *2024 Conference on AI, Science, Engineering, and Technology (AIxSET)*, Laguna Hills, CA, USA, 2024, pp. 1-8, doi: 10.1109/AIxSET62544.2024.00007.

[30] Neeraj Varshney; Parul Madan; Anurag Shrivastava; Arun Pratap Srivastava; C Praveen Kumar; Akhilesh,(2023) "Real-Time Anomaly Detection in IoT Healthcare Devices With LSTM," *International Conference on Artificial Intelligence for Innovations in Healthcare Industries (ICAIIHI),* Raipur, India, 2023, pp. 1-6, doi: 10.1109/ICAIIHI57871.2023.10489823.

[31] X. Zhang, X. Chai, M. Yu and D. Qiu,(2023) "Anomaly Detection Model for Log Based on LSTM Network and Variational Autoencoder," *2023 4th International Conference on Information Science, Parallel and Distributed Systems (ISPDS)*, Guangzhou, China, pp. 239-244, doi: 10.1109/ISPDS58840.2023.10235370.

[32] S. A. Roseline, S. Karthik and I. N. V. D. Sruti, (2024) "Intelligent Human Anomaly Detection using LSTM Autoencoders," *2024 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI)*, Chennai, India, , pp. 1-7, doi: 10.1109/ACCAI61061.2024.10602454.

[33] Ly Vu Le , Tuan Phong Tran ,Van Cuong Nguyen ,Quang Uy Nguyen , (2024), Mitigating Poisoning Attacks To Federated Learning In IOTs Anomaly Detection With Attention Aggregation, Vol. 13 No. 02 (2024) ,DOI: https://doi.org/10.56651/lqdtu.jst.v13.n02.925.ict.

[34] R. Zatsarenko, S. Chuprov, D. Korobeinikov and L. Reznik,(2024), "Trust-Based Anomaly Detection in Federated Edge Learning," *2024 IEEE World AI IoT Congress (AIIoT)*, Seattle, WA, USA, 2024, pp. 273-279, doi: 10.1109/AIIoT61789.2024.10578967.

[35] Zhu, F., Li, M., Liu, Y., Liu, J., Wang, Z., & Chen, Y. (2024). Anomaly Detection in Commercial Load Data Using Bidirectional LSTM and Autoencoders. *2024 IEEE 3rd International Conference on Electrical Engineering, Big Data and Algorithms (EEBDA)*, 902-904. https://doi.org/10.1109/EEBDA60612.2024.10485863.

[36] Li, W., Du, Q., & Chen, T. (2023). Decentralized Federated Learning-Enabled Relation Aggregation for Anomaly Detection. *Information*, 14(12), 647. https://doi.org/10.3390/info14120647.

[37] Harris, T., & Martinez, E. (2024). Leveraging Deep Learning for Anomaly Detection in the Interbank Bond Market. *Journal of Computer Technology and Software*, 3(4). https://ashpress.org/index.php/jcts/article/view/72.

[38] Li, G., & Jung, J. J. (2023). Deep learning for anomaly detection in multivariate time series: Approaches, applications, and challenges. *Information Fusion*, 91, 93-102. https://doi.org/10.1016/j.inffus.2022.10.008.

[39] Akbarian, H., Mahgoub, I., & Williams, A. (2023). Autoencoder-LSTM Algorithm for Anomaly Detection. *2023 IEEE 20th International Conference on Smart Communities: Improving Quality of Life using AI, Robotics and IoT (HONET)*, 1-6. https://doi.org/10.1109/HONET59747.2023.10374710.

[40] Li, Y., Zhang, R., Zhao, P., & Wei, Y. (2024). Feature-Attended Federated LSTM for Anomaly Detection in the Financial Internet of Things. *Applied Sciences*, 14(13), 5555. https://doi.org/10.3390/app14135555.

[41] Arora, S., Beams, A., Chatzigiannis, P., Meiser, S., Patel, K., & Raghuraman, S. (2024). Privacy-Preserving Financial Anomaly Detection via Federated Learning & Multi-Party Computation. *2024 Annual Computer Security Applications Conference Workshops (ACSAC Workshops)*, 270-279. https://doi.org/10.1109/ACSACW65225.2024.00038.

[42] Shrestha, R., Mohammadi, M., Sinaei, S., Salcines, A., Pampliega, D., Clemente, R., & Lindgren, A. (2024). Anomaly Detection based on LSTM and Autoencoders using Federated Learning in Smart Electric Grid. *Journal of Parallel and Distributed Computing*, 104951. https://doi.org/10.1016/j.jpdc.2024.104951.

[43] Immadisetty, A. (2024). Machine Learning for Real-Time Anomaly Detection. *International Journal For Multidisciplinary Research*, 6(6). https://doi.org/10.36948/ijfmr.2024.v06i06.33087.

[44] Farooq, E., & Borghesi, A. (2024). LSTM-Based Unsupervised Anomaly Detection in High-Performance Computing: A Federated Learning Approach. 7735–7744. https://doi.org/10.1109/bigdata62323.2024.10825337.

[45] Mohammadi, M., Shrestha, R., Sinaei, S., Salcines, A., Pampliega, D., Clemente, R., & Sanz, A. L. (2023). Anomaly Detection Using LSTM-Autoencoder in Smart Grid: A Federated Learning Approach. https://doi.org/10.1145/3616131.3616138.

[46] Abdennebi, A., Tuncay, A., Yilmaz, C., Koyuncu, A., & Gungor, O. (2023). LSTM-AE for Anomaly Detection on Multivariate Telemetry Data. *2023 IEEE/ACIS 21st International Conference on Software Engineering Research, Management and Applications (SERA)*, 90-97. https://doi.org/10.1109/SERA57763.2023.10197673.

[47] Sahu, A., El-Ebiary, Y. A. B., Saravanan, K. A., Thilagam, K., Devi, G. R., Gopi, A., & Taloba, A. I. (2024). Federated LSTM Model for Enhanced Anomaly Detection in Cyber Security: A Novel Approach for Distributed Threat. *International Journal of Advanced Computer Science and Applications (IJACSA)*, 15(6). http://dx.doi.org/10.14569/IJACSA.2024.01506125.

[48] Chen, G. (2024). An improved BiGAN model for anomaly detection in finance. *Applied and Computational Engineering*, 53, 90-95. https://doi.org/10.54254/2755-2721/53/20241281.

[49] Farooq, E., & Borghesi, A. (2023). A Federated Learning Approach for Anomaly Detection in High Performance Computing. *2023 IEEE 35th International Conference on Tools with Artificial Intelligence (ICTAI)*, 496-500. https://doi.org/10.1109/ICTAI59109.2023.00079.

[50] Arora, S., Beams, A., Chatzigiannis, P., Meiser, S., Patel, K., Raghuraman, S., & Zamani, M. (2023). Privacy-Preserving Financial Anomaly Detection via Federated Learning & Multi-Party Computation. *arXiv.Org, abs/2310.04546*. https://doi.org/10.48550/arxiv.2310.04546.

[51] Li, W., Liu, X., & Zhou, S. (2024). Deep Learning Model Based Research on Anomaly Detection and Financial Fraud Identification in Corporate Financial Reporting Statements. The Journal of Combinatorial Mathematics and Combinatorial Computing, 123(1), 343–355. https://doi.org/10.61091/jcmcc123-24.

[52] Rafi, S. M. S., Arafat, Md. E., Islam, Md. R., Jalil, M., Jony, M. A. M., & Hossen, F. (2024). Machine Learning in Financial Fraud Detection: New Models for Predictive Analysis and Mitigating Business Risks. Deleted Journal, 2(6). https://doi.org/10.62127/aijmr.2024.v02i06.1116.

[53] Jain, Y., Rathore, CA. D. S., Johrawanshi, A., Maheshwari, A., Pandey, A., & Saxena, N. (2024). Machine Learning Approaches for Identifying Fraudulent Banking Transactions: A Financial Management Perspective. 1903–1909. https://doi.org/10.1109/ictacs62700.2024.10841041

[54] Alhammadi, R., Gawanmeh, A., Atalla, S., Alkhatib, M. Q., & Mansoor, W. (2023). Performance Evaluation of Federated Learning for Anomaly Network Detection. 116–122. https://doi.org/10.1109/csce60160.2023.00024

[55] Xu, J., Yang, T., Zhuang, S., Li, H., & Lu, W. (2024). AI-Based Financial Transaction Monitoring and Fraud Prevention with Behaviour Prediction. https://doi.org/10.20944/preprints202407.1107.v1