Enhancing Financial Risk Management with Federated AI

Vineet Dhanawat *, Varun Shinde, Vishal Karande, Kartik Singhal

Posted Date: 27 November 2024

doi: 10.20944/preprints202411.2087.v1

Keywords: Federated Learning; Explainable AI; Fraud Detection; Data Privacy; Imbalanced Datasets; Financial Institutions; Model Transparency; Collaborative Learning; Customer Confidentiality; Risk Management

 doi:10.20944/preprints202411.2087.v1

Article

Enhancing Financial Risk Management with Federated AI

Vineet Dhanawat [1,*], Varun Shinde [2], Vishal Karande [3] and Kartik Singhal [1]

[1] Meta Platforms Inc., Menlo Park, US
[2] Cloudera Inc., Austin, US
[3] Google Inc., Mountain View, US
* Correspondence: vineetdhanawat@gmail.com

Abstract: Fraudulent transactions are a persistent challenge for financial institutions, demanding robust detection systems to maintain customer trust. Key obstacles include the rarity of fraud cases, leading to imbalanced datasets, and strict privacy regulations limiting data sharing. Additionally, fraud detection must be transparent to preserve user trust. This research addresses these issues by combining Federated Learning (FL) and Explainable AI (XAI), allowing institutions to collaboratively train models without sharing data, thus protecting privacy while ensuring model transparency and interpretability.

Keywords: Federated Learning; Explainable AI; fraud detection; data privacy; imbalanced datasets; financial institutions; model transparency; collaborative learning; customer confidentiality; risk management

1. Introduction

In the field of digital banking, ensuring the trustworthiness and security of financial interactions remains a critical concern [1]. While the shift to digital platforms has simplified many financial processes, it has simultaneously introduced numerous cyber risks. One of the most pressing issues is financial fraud, particularly in sectors like online banking and credit card transactions, which poses substantial threats to both global economies and individual financial safety [2]. These fraudulent actions not only tarnish the credibility of financial institutions but also jeopardize personal financial stability. A report by Alexander et al. [3] highlights that fraudulent activities result in billions of dollars in annual losses, underscoring the urgent need for improved mechanisms for risk management.

Financial institutions are continuously developing strategies to mitigate various forms of financial risk, with a major focus on fraud prevention. However, the evolving nature of these risks and the complexity of fraud tactics present ongoing challenges. Banking fraud, in particular, stands out as a critical area for study [4]. Unlike other forms of financial deceit, banking fraud involves more sophisticated techniques that make detection difficult [5]. Common tactics include account takeovers, unauthorized transactions, or even the creation of fraudulent accounts using fake identities [6]. These events have significant implications for victims, not only resulting in financial losses but also causing long-term emotional distress. To effectively mitigate such risks, research must employ comprehensive, data-driven approaches.

AI in risk management is increasingly valuable for analyzing large datasets and predicting fraud. Machine learning models, trained on vast but sensitive and imbalanced financial data, are central to this approach [7]. However, the rarity of fraudulent transactions and the dynamic nature of fraud patterns make model robustness challenging, especially across institutions. Federated Learning (FL) offers a promising solution by addressing these issues and enabling collaborative fraud detection without compromising data privacy.

FL represents a novel approach to decentralized AI that maintains data privacy by enabling model training on local devices without sharing raw data [8,9]. This method contrasts with traditional ML approaches that rely on centralized data repositories. By facilitating collaboration between multiple financial institutions, FL enhances risk management by pooling insights from a wider array of sources, without compromising data privacy. Within the field of financial risk management, FL proves invaluable, as it allows institutions to share knowledge about emerging fraud patterns without

 doi:10.20944/preprints202411.2087.v1

exchanging sensitive data. The model updates rather than the raw data are communicated, which enhances efficiency and maintains the confidentiality of customer information.

A major challenge in AI-driven risk management is the "black box" nature of models, making decision processes opaque. This study proposes XAI with FL to enhance transparency and trust while preserving privacy in personalized financial services. This approach combines FL's privacy strengths with XAI's transparency to address both efficiency and ethical transparency in AI-based risk management.

1. Develop an FL-based risk management system that ensures data privacy by centralizing only model updates while maintaining the confidentiality of financial information.
2. Build a predictive AI model to identify risk patterns in financial transactions, ensuring both security and precision in personalized financial services.
3. Employ XAI techniques to provide transparency in the decision-making process, fostering trust in the system's predictions and recommendations.
4. Demonstrate the effectiveness of the proposed system through a web-based application, offering a user-friendly interface to showcase the operational capabilities.

2. Literature Review

Technology has significantly transformed risk management in financial services, introducing advanced techniques to counter new risks arising from digital platforms [10]. While digital advancements have fueled growth, they have also led to increased cyber threats and fraud, such as data breaches and digital scams. Understanding the motivations behind fraudulent behavior remains key to mitigating these risks [11]. The widely recognized "fraud triangle" framework explains fraud as a convergence of motivation, rationalization, and opportunity. Researchers have further explored this model by examining how individuals execute and conceal fraudulent acts [12].

As financial institutions seek to manage the overwhelming volume of transactions and associated risks, AI and its subfields like ML and Deep DL have emerged as powerful tools in the detection and management of financial risks [13]. ML, a core subset of AI, uses statistical algorithms to identify patterns and anomalies in large datasets [14], while DL, an advanced form of ML, leverages neural networks to detect intricate relationships within the data [15]. These techniques are particularly useful in handling vast amounts of transaction data, as they enable systems to learn from historical data and make predictive decisions. For instance, complex architectures like Convolutional Neural Networks (CNNs) and Restricted Boltzmann Machines (RBMs) have proven to be effective in understanding large-scale data patterns, especially in environments where risk management requires processing massive datasets.

Various ML and DL techniques have been explored for their potential to mitigate financial risks. Shamsolmoali et al. [16] investigated the effectiveness of Support Vector Machines, k-nearest Neighbors, and ensemble models in detecting fraudulent financial transactions. Their research revealed challenges such as the imbalance of transaction data, where legitimate transactions significantly outnumber fraudulent ones, and the need for continuous updates to maintain model accuracy. Randhawa et al. [17] extended this research by examining algorithms like SVM and Random Forest, while Sharma et al. [18] explored the use of transformer-based models in financial risk detection. These models encode data before reconstructing it, with any discrepancies potentially signaling fraudulent activities. RBMs, highlighted by Pumsirirat [19], excel at learning probability distributions from unlabeled data, making them ideal for identifying unusual patterns within imbalanced datasets.

Traditional ML-based risk management has largely relied on centralized systems, where client data is collected and processed on a central server [20]. While effective, this approach poses privacy, latency, and security concerns, especially in the regulated financial sector. Legal restrictions also limit data sharing, complicating centralized data collection. Decentralized methods like Federated Learning (FL) address these issues by enabling collaborative learning across institutions without exchanging raw

 doi:10.20944/preprints202411.2087.v1

data [21]. Initially designed for mobile apps, FL transmits model updates rather than data, protecting customer privacy while improving financial risk management.

Beyond privacy, the effectiveness of risk management models is key in deciding between centralized and decentralized approaches. Recurrent Neural Networks (RNNs), like Long Short-Term Memory (LSTM) networks, are commonly used for risk detection but struggle with long-term dependencies in complex financial data [22]. Balancing privacy and performance is crucial; centralized systems provide control but risk data confidentiality, whereas decentralized approaches like FL enhance privacy and flexibility. As the industry evolves, decentralized models are likely to become more prominent in financial risk management.

FL addresses challenges posed by traditional centralized systems by enabling AI models to train on local data without data transmission, enhancing privacy while facilitating collaborative learning across institutions [23]. In FL, a global model is trained across decentralized servers or devices, sharing only aggregated updates with a central server. This approach allows financial institutions to benefit from collaborative insights without compromising data privacy. FL's adaptability to both independent and non-independent data distributions makes it well-suited for financial services, where transaction patterns vary across institutions. Yang [24] highlights the importance of privacy in financial risk management, noting that the difficulty of obtaining new data sources complicates efforts to improve risk detection models.

Incorporating XAI into FL-based frameworks provides additional transparency, ensuring that risk management systems are not only accurate but also trustworthy. This study proposes an innovative risk management framework that integrates FL with XAI to provide a more robust, transparent, and privacy-preserving approach to managing financial risks.

3. Proposed Methodology

3.1. System Framework

In the proposed framework, the personalized financial service risk management system leverages FL for collaborative model development, ensuring both data privacy and enhanced fraud detection. The core of the system architecture is a decentralized network where financial institutions, such as banks, serve as local nodes. Each bank maintains its own ML model, M_i, trained on sensitive, private datasets. The updates from these locally trained models—denoted by parameter sets θ_i—are transmitted to a central aggregator (the server), which constructs the global model, M_{global}.

The system operates through rounds of updates. Each local model, M_i, is initialized and trained on a node's private data. Instead of sharing raw data, only the parameter updates θ_i from each node are communicated to the central server, ensuring privacy. The central server aggregates these updates to refine the global model, represented mathematically by:

$$M_{\text{global}}^{(t+1)} = A(\theta_1^{(t)}, \theta_2^{(t)}, \ldots, \theta_N^{(t)}) \tag{1}$$

where A is an aggregation function, and t denotes the iteration step. The most commonly used function is the weighted averaging scheme:

$$M_{\text{global}}^{(t+1)} = \frac{1}{N} \sum_{i=1}^{N} \alpha_i \theta_i^{(t)} \tag{2}$$

where N is the total number of institutions (nodes), and α_i represents the weight for each node's contribution based on its data size or importance.

 doi:10.20944/preprints202411.2087.v1

3.2. Framework for Privacy-Preserving Updates

At each node i, the local ML model's parameters θ_i are updated based on its local dataset $\mathcal{D}_i$. The update is conducted using Stochastic Gradient Descent (SGD), expressed as:

$$\theta_i^{(t+1)} = \theta_i^{(t)} - \eta \nabla L_i(\theta_i^{(t)}, \mathcal{D}_i) \tag{3}$$

Where η is the learning rate, and $\nabla L_i(\theta_i, \mathcal{D}_i)$ is the gradient of the loss function L_i, calculated with respect to the local dataset $\mathcal{D}_i$.

The global aggregation step in FL leverages these local updates. For a weighted average approach, the central server performs the following operation:

$$\theta_{\text{global}}^{(t+1)} = \sum_{i=1}^{N} \frac{n_i}{n_{\text{total}}} \theta_i^{(t+1)} \tag{4}$$

where n_i is the data size of the i-th node, and n_{total} is the total size of the combined datasets, $n_{\text{total}} = \sum_{i=1}^{N} n_i$.

3.3. Explainability with XAI

Integrating XAI into the system is crucial for enhancing the transparency and trustworthiness of the financial risk management models. XAI techniques such as Shapley Additive Explanations (SHAP) are incorporated to provide interpretability. SHAP values quantify the contribution of each feature to the model's decision-making process. The SHAP value $\phi_j(f)$ for a feature j in model f is computed by:

$$\phi_j(f) = \sum_{S \subseteq N \setminus \{j\}} \frac{|S|!(|N| - |S| - 1)!}{|N|!} [f(S \cup \{j\}) - f(S)] \tag{5}$$

Where S is a subset of the feature set N, excluding j, and $f(S)$ is the model's prediction using only features in subset S. The formula accounts for all possible subsets to ensure fairness in evaluating feature contributions.

The use of SHAP within FL allows each client to compute feature importances locally, contributing to the global model's transparency without compromising privacy.

3.4. Model Implementation

The implementation details of the proposed method are illustrated in 1. The implementation process encompasses several critical steps: conducting preliminary checks, processing data, developing the FL framework, and integrating XAI techniques. Each of these steps is crucial for ensuring the effectiveness and reliability of the proposed fraud detection system.

 doi:10.20944/preprints202411.2087.v1

Algorithm 1 Fraud Detection Using FL and Explainable AI

Initialize: Global model M_{global} with random weights, maximum epochs
while transaction data is available **do**
  if no transaction data **then**
    Return to the beginning
  else
    Preprocess transaction data D_i for each client node i
    for each node i **do**
      Compute local model M_i using gradient descent:

$$\theta_i^{(t+1)} = \theta_i^{(t)} - \eta \nabla L_i(\theta_i^{(t)}, D_i)$$

      Send $\theta_i^{(t+1)}$ to the central server
    end for
    if no model update is available **then**
      Wait and periodically check
    else
      Update global model using Federated Averaging:

$$M_{\text{global}}^{(t+1)} = \frac{1}{N} \sum_{i=1}^{N} \alpha_i \theta_i^{(t+1)}$$

      Use updated M_{global} to identify patterns associated with fraudulent activities
      for each transaction **do**
        Classify transactions using sigmoid activation function:

$$y = \frac{1}{1 + e^{-z}}$$

      end for
      Use SHAP to explain model decisions:
      for each transaction **do**
        Compute SHAP values $\phi_j(f)$ as:

$$\phi_j(f) = \sum_{S \subseteq N \setminus \{j\}} \frac{|S|!(|N| - |S| - 1)!}{|N|!} [f(S \cup \{j\}) - f(S)]$$

      end for
      Provide transparency report for classified transactions
    end if
  end if
end while

The dataset employed in this study is derived from reference [25], comprising realistic data modeled after a contemporary real-world dataset for fraud detection. It encompasses a total of 630,000 entries distributed across 18 distinctive features. This comprehensive dataset includes diverse data types: eighteen columns consisting of integer values, ten feature numbers, and five columns containing categorical data. This rich composition facilitates a unique analysis of fraudulent activities, providing a robust foundation for implementing and evaluating the proposed techniques. The major column characteristics are shown in Figure 1.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 27 November 2024 doi:10.20944/preprints202411.2087.v1

Figure 1. Characteristics of the dataset.

3.5. Data Preprocessing

The dataset in this study exhibited a significant class imbalance, addressed by applying the Synthetic Minority Over-sampling Technique (SMOTE) [26], which generates synthetic samples for the minority class to balance the dataset and improve model robustness. Missing data was handled based on type: mean imputation for numerical attributes and model-based imputation for categorical ones. Outliers in floating-point columns were removed using the Interquartile Range (IQR) method, eliminating data points beyond 1.5 times the IQR from Q1 or Q3 [27]. A correlation matrix (see Figure 2) was then visualized as a heatmap to explore linear relationships among numeric attributes.

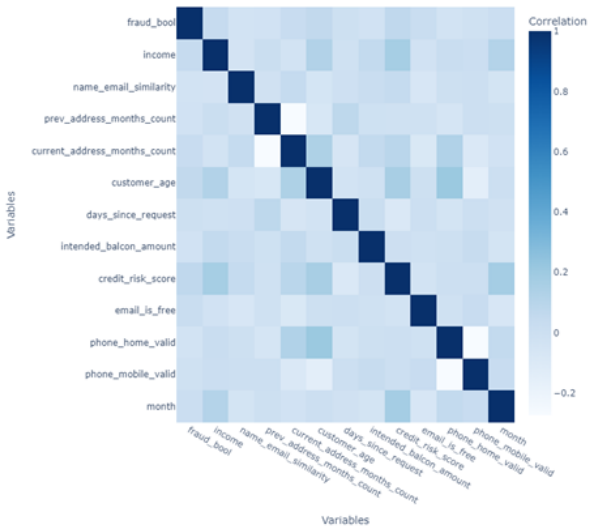

Figure 2. Fraud dataset correlation matrix.

3.6. Deep Learning Model and XAI

The DL model utilized in this study consists of a three-layer dense neural network designed for binary classification tasks. The initial layer comprises 64 neurons with a ReLU activation function, which receives its input from the feature dimensions of the validation dataset. The subsequent layer contains 32 neurons, also activated by ReLU. The final layer features a single neuron activated by a sigmoid function tailored for binary classification. The model employs the Adam optimization

 doi:10.20944/preprints202411.2087.v1

algorithm for weight adjustments and uses binary cross-entropy to evaluate prediction losses. Figure 2 shows the correlation metrics of the selected features.

Data for this research was split after preprocessing, adhering to the standard practice of allocating 80% for training and 20% for testing, which ensures unbiased partitioning. The dataset was divided into three segments to integrate these datasets into the FL framework. Performance assessment of the ML model utilized a multi-pronged metric approach, applying the confusion matrix. Additional metrics included Accuracy, Precision, Recall, and F1-Score, which provides a balance between Precision and Recall, essential in addressing class imbalances. Feature importance within the model was visualized using the SHAP method, which clarifies the impact of each feature relative to a specified baseline, enhancing interpretability [28]. This setup uses modern DL frameworks, and the simulation illustrates how individual client-side models contribute to the global model's learning process. Post-training, SHAP values elucidate model decisions, enhancing their interpretability. The infrastructure was constructed using a Kaggle-based notebook. A web application framework for server-client interactions was developed using Flask and API, while TensorFlow supported DL operations.

4. Results and Analysis

The results of the proposed AI-driven risk management system, which integrates FL and XAI, reveal its strong capacity for improving risk prediction in personalized financial services. As demonstrated in Figures 3, 4, and 5, the model's performance across key metrics such as accuracy, precision, recall, and F1-score indicates its robustness in identifying and managing financial risks.

Figure 3 displays the confusion matrix for the proposed model, showing its ability to differentiate between high-risk and low-risk transactions with a high degree of accuracy.

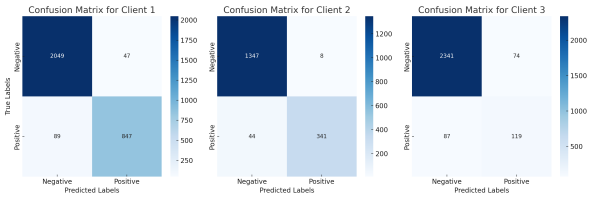

Figure 3. Confusion matrix of the proposed model.

In Figure 4, the precision of the model increases steadily over the training epochs, reaching a value of approximately 0.87. This suggests the model becomes increasingly reliable in identifying high-risk transactions, ensuring that fewer false positives are flagged as risks. Precision is essential in personalized financial services, as misclassifying legitimate transactions can lead to unnecessary customer inconvenience and operational costs. The stabilization of precision after around 50 epochs shows the model's ability to maintain high prediction quality over time.

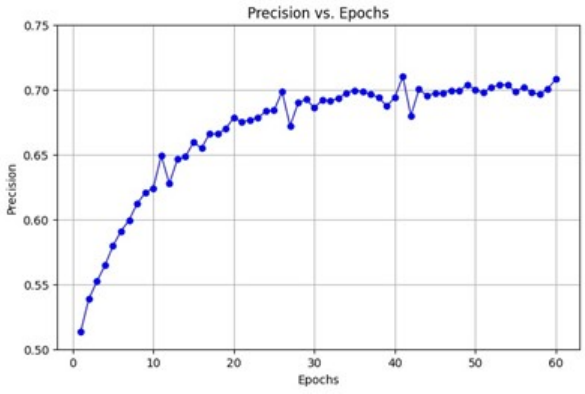

Figure 4. Precision of the model vs. training epochs.

 doi:10.20944/preprints202411.2087.v1

The model's overall accuracy is depicted in Figure 5, where it rises from an initial value of 0.70 to an impressive 0.95 after approximately 60 epochs. This increase highlights the system's capability to improve its risk detection performance as it learns from both historical and real-time data. High accuracy in risk management ensures that most high-risk transactions are flagged, minimizing potential financial losses.

The performance comparison of multiple models, as shown in Figure 5, demonstrates the superiority of the FL-based approach in terms of both average accuracy and stability. While other models may show performance variability, the FL model consistently achieves accuracy close to 95%. This underscores the benefit of decentralized learning across institutions, where the collective intelligence of multiple financial entities enhances the predictive power of the global model.

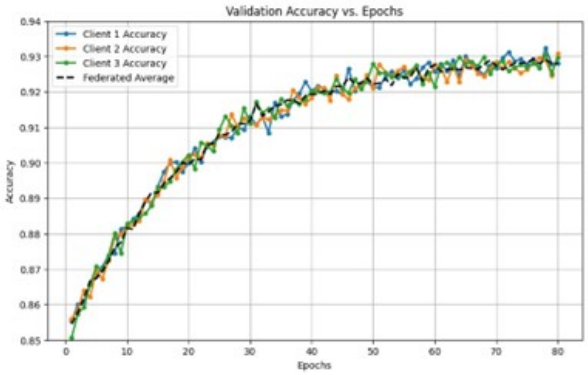

Figure 5. Comparison of accuracy across different models.

The integration of XAI through Shapley Additive Explanations (SHAP) adds an extra layer of trust to the system by providing transparency in decision-making. Figure 6 showcases SHAP values, where the color gradient (from red to blue) represents the positive or negative impact of each feature on the model's predictions. Features with higher SHAP values have a more significant impact on the decision-making process. For instance, in cases where certain transaction attributes exhibit higher SHAP values (e.g., values around 2.0 or above), they positively influence the model's risk prediction. This capability to explain the influence of specific features ensures that financial institutions can audit and understand the reasoning behind the risk assessment decisions, which is vital in a regulated environment.

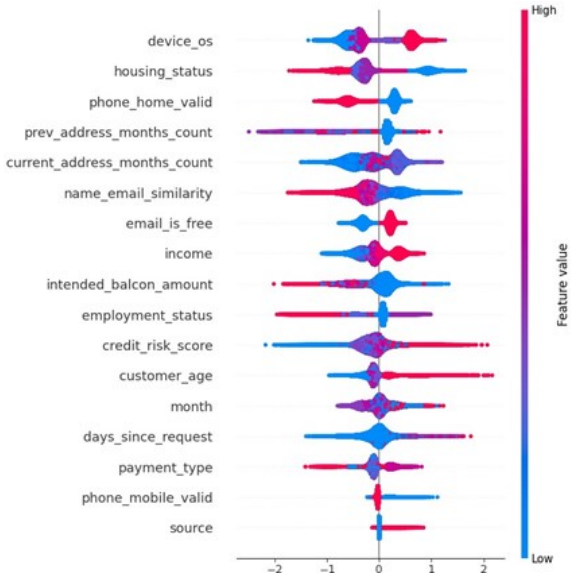

Figure 6. SHAP values explaining the model's predictions.

 doi:10.20944/preprints202411.2087.v1

The evaluation of the proposed system used multiple metrics. For example, accuracy reached 95%, precision was around 0.87, and recall improved to 0.89. The F1-score, which balances precision and recall, reached 0.88, indicating the system's capability to efficiently handle both the identification of high-risk transactions and the avoidance of false positives. These metrics confirm that the AI system is both sensitive to risks and selective in avoiding unnecessary false flags.

5. Conclusion

This research has demonstrated the potential of FL in revolutionizing risk management within personalized financial services. By decentralizing model training, FL ensures that sensitive financial data remains private while allowing financial institutions to collaborate effectively. Through the local training of models on private datasets and the aggregation of model updates, institutions are able to contribute to a global model without sharing raw data, thereby preserving confidentiality. This decentralized approach enhances both data security and the model's performance by incorporating diverse, institution-specific insights into the global risk management framework.

References

1. Smith, J.; Liu, C. Secure Transactions, Secure Systems: Regulatory Compliance in Internet Banking. Technical report, EasyChair, 2024.
2. Carminati, M.; Caron, R.; Maggi, F.; Epifani, I.; Zanero, S. BankSealer: A decision support system for online banking fraud analysis and investigation. *computers & security* **2015**, *53*, 175–186.
3. Dyck, A.; Morse, A.; Zingales, L. How pervasive is corporate fraud? *Review of Accounting Studies* **2024**, *29*, 736–769.
4. Abdallah, A.; Maarof, M.A.; Zainal, A. Fraud detection system: A survey. *Journal of Network and Computer Applications* **2016**, *68*, 90–113.
5. Shinde, V.; Dhanawat, V.; Almogren, A.; Biswas, A.; Bilal, M.; Naqvi, R.A.; Rehman, A.U. Copy-move forgery detection technique using graph convolutional networks feature extraction. *IEEE Access* **2024**.
6. Kumar, S. A study of identity theft: intentions, connected frauds, methods and avoidance. *ACADEMICIA: An International Multidisciplinary Research Journal* **2021**, *11*, 2044–2050.
7. Bhattacharyya, S.; Jha, S.; Tharakunnel, K.; Westland, J.C. Data mining for credit card fraud: A comparative study. *Decision support systems* **2011**, *50*, 602–613.
8. Rajesh, L.T.; Das, T.; Shukla, R.M.; Sengupta, S. Give and take: Federated transfer learning for industrial iot network intrusion detection. 2023 IEEE 22nd International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom). IEEE, 2023, pp. 2365–2371.
9. Guan, H.; Yap, P.T.; Bozoki, A.; Liu, M. Federated learning for medical image analysis: A survey. *Pattern Recognition* **2024**, p. 110424.
10. Bolton, R.J.; Hand, D.J. Statistical fraud detection: A review. *Quality control and applied statistics* **2004**, *49*, 313–314.
11. Van Driel, H. Financial fraud, scandals, and regulation: A conceptual framework and literature review. *Business History* **2019**.
12. Trompeter, G.M.; Carpenter, T.D.; Desai, N.; Jones, K.L.; Riley, R.A. A synthesis of fraud-related research. *Auditing: A Journal of Practice & Theory* **2013**, *32*, 287–321.
13. Faruqui, N.; Achar, S.; Racherla, S.; Dhanawat, V.; Sripathi, P.; Islam, M.M.; Uddin, J.; Othman, M.A.; Samad, M.A.; Choi, K. Cloud IaaS Optimization Using Machine Vision at the IoT Edge and the Grid Sensing Algorithm. *Sensors* **2024**, *24*. doi:10.3390/s24216895.
14. Shinde, V.; Singhal, K.; Almogren, A.; Dhanawat, V.; Karande, V.; Rehman, A.U. Ensemble Voting for Enhanced Robustness in DarkNet Traffic Detection. *IEEE Access* **2024**.
15. Raghavan, P.; El Gayar, N. Fraud detection using machine learning and deep learning. 2019 international conference on computational intelligence and knowledge economy (ICCIKE). IEEE, 2019, pp. 334–339.
16. Zareapoor, M.; Shamsolmoali, P.; others. Application of credit card fraud detection: Based on bagging ensemble classifier. *Procedia computer science* **2015**, *48*, 679–685.
17. Randhawa, K.; Loo, C.K.; Seera, M.; Lim, C.P.; Nandi, A.K. Credit card fraud detection using AdaBoost and majority voting. *IEEE access* **2018**, *6*, 14277–14284.

 doi:10.20944/preprints202411.2087.v1

18. Sharma, M.A.; Raj, B.G.; Ramamurthy, B.; Bhaskar, R.H. Credit card fraud detection using deep learning based on auto-encoder. ITM Web of Conferences. EDP Sciences, 2022, Vol. 50, p. 01001.
19. Pumsirirat, A.; Liu, Y. Credit card fraud detection using deep learning based on auto-encoder and restricted boltzmann machine. *International Journal of advanced computer science and applications* **2018**, *9*.
20. Kamei, S.; Taghipour, S. A comparison study of centralized and decentralized federated learning approaches utilizing the transformer architecture for estimating remaining useful life. *Reliability Engineering & System Safety* **2023**, *233*, 109130.
21. McMahan, B.; Moore, E.; Ramage, D.; Hampson, S.; y Arcas, B.A. Communication-efficient learning of deep networks from decentralized data. Artificial intelligence and statistics. PMLR, 2017, pp. 1273–1282.
22. Benchaji, I.; Douzi, S.; El Ouahidi, B. Credit card fraud detection model based on LSTM recurrent neural networks. *Journal of Advances in Information Technology* **2021**, *12*.
23. Bharati, S.; Mondal, M.; Podder, P.; Prasath, V. Federated learning: Applications, challenges and future directions. *International Journal of Hybrid Intelligent Systems* **2022**, *18*, 19–35.
24. Yang, W.; Zhang, Y.; Ye, K.; Li, L.; Xu, C.Z. Ffd: A federated learning based method for credit card fraud detection. Big Data–BigData 2019: 8th International Congress, Held as Part of the Services Conference Federation, SCF 2019, San Diego, CA, USA, June 25–30, 2019, Proceedings 8. Springer, 2019, pp. 18–32.
25. Huang, H.; Liu, B.; Xue, X.; Cao, J.; Chen, X. Imbalanced credit card fraud detection data: A solution based on hybrid neural network and clustering-based undersampling technique. *Applied Soft Computing* **2024**, *154*, 111368.
26. Elreedy, D.; Atiya, A.F.; Kamalov, F. A theoretical distribution analysis of synthetic minority oversampling technique (SMOTE) for imbalanced learning. *Machine Learning* **2024**, *113*, 4903–4923.
27. Abdiweli, A.J. Simulation study on the performance of robust outlier labelling methods. PhD thesis, Kampala International University, College of Economics and management, 2023.
28. Yang, Q.; Liu, Y.; Chen, T.; Tong, Y. Federated machine learning: Concept and applications. *ACM Transactions on Intelligent Systems and Technology (TIST)* **2019**, *10*, 1–19.