Jurnal Ilmiah
Teknologi Sistem
Informasi

Vol. 6 (2025) No. 4

https://jurnal-itsi.org/index.php/jitsi; E-ISSN: 2722-4600; ISSN: 2722-4619
DOI: 10.62527/jitsi.6.4.492

Leveraging Blockchain and Federated Reinforcement Learning for Enhanced Fraud Detection in Financial Transactions

Tanweer Alam[#]

[#] *Faculty of Computer and Information Systems, Islamic University of Madinah, Madinah, Saudi Arabia*
E-mail: tanweer03[at]iu.edu.sa

A B S T R A C T S

Credit card fraud detection uses several technologies including machine learning (ML) and statistical analysis as well as card authentication methods. Credit card fraud is the illegal use of someone's credit card for purchase of goods or services. Comprehensive studies have shown how well ML technology generates exact prediction models to spot possible transaction fraud. Though the potential of losing the actual card is still a worry, hackers have been increasingly acquiring credit card numbers and personal information online. The growth in e-commerce has matched credit card use for online transactions, which has surged credit card theft. Complex detection systems including federated reinforcement learning (FRL) and blockchain technology have been developed to solve this challenge. Using standard pattern matching methods can make it difficult to tell real from fake transactions. A decentralised method of ML, FRL stresses user privacy and enhances anonymity and confidence in financial transactions. An original approach for teaching a credit card fraud detection model is shown in this work It makes advantage of user behaviour traits, federated reinforcement learning, and blockchain technologies. Using a smart contract between the bank and the client, the approach aims to reduce dishonest activity. By lowering the dependence on centralised data aggregation, this innovative approach guarantees user privacy protection all through model development. The research also looks at the challenges in credit card fraud detection and offers ideas for next developments.

Manuscript received Aug 11, 2025; revised Nov 30, 2025. accepted Dec 1, 2025 Date of publication Dec 31, 2025. International Journal, JITSI : Jurnal Ilmiah Teknologi Sistem Informasi licensed under a Creative Commons Attribution-Share Alike 4.0 International License

Keywords / Kata Kunci — ***Federated Learning; Blockchain; Smart Contracts; Credit Cards; Fraud Detection***

CORRESPONDING AUTHOR

Tanweer Alam
Faculty of Computer and Information Systems, Islamic University of Madinah, Madinah, Saudi Arabia
Email: tanweer03[at]iu.edu.sa

1. INTRODUCTION

Credit card fraud detection encompasses various methods employed to detect and prevent unauthorised and deceptive credit card usage [1]. Customers are given plastic cards known as credit cards to make payments easier. The system approves purchases by considering the cardholder's obligation to cover the costs of the products and services. Credit card fraud is a common problem that impacts numerous individuals and leads to substantial financial losses for both financial institutions and customers. The rise of e-commerce has also brought about a rise in the complexity of fraudulent activities. Effectively detecting cases of credit card theft in real-time while reducing the occurrence of false alarms continues to be a challenging endeavour [2]. The objective of this study is to conduct a comprehensive assessment of current methods used to detect credit card fraud, examining the

challenges faced and potential avenues for future research. The security measures of a credit card revolve around prioritising the privacy of the credit card number and safeguarding the physical card. The surge in online shopping and the widespread adoption of credit cards have led to a significant rise in the worldwide embrace of these payment methods. There has been an increase in fraudulent activity that aligns with the significant expansion of credit card transactions. For a better understanding, it's worth mentioning that "credit card fraud" encompasses various deceptive actions, including the unauthorised use of a credit card for fraudulent transactions. There are different methods one can use to engage in credit card theft. Gaining the essential knowledge to recognise credit card fraud is a vital initial measure in combating this type of criminal activity. Thanks to the different methods employed to detect and prevent credit card fraud, the occurrence of such incidents has remained steady over time. Establishing reliable and effective methods to prevent fraudulent behaviour in the financial sector is of utmost importance. One of the most challenging tasks is detecting credit card theft. Conventional fraud detection systems depend on centralised data processing, which can lead to concerns regarding scalability, privacy, and security. By combining FRL and blockchain technology, we can provide a practical solution to strengthen fraud detection systems and effectively address these concerns.

FIG 1. Credit Card Fraud detection basic model

FRL is a decentralised ML technique that enables multiple nodes to work together in training a shared model, without the requirement of sharing raw data. Ensuring the security of sensitive information is of utmost importance, with client-side storage offering a safe and protected environment for data privacy and security. For enhanced model performance, the approach involves utilising multiple clients to combine modifications to the model, such as weights or gradients, rather than transmitting data to a central server. This approach is particularly advantageous for credit card fraud detection due to the following reasons:

1. Privacy Preservation: Financial institutions can collaborate on training robust fraud detection models without exposing their customers' sensitive data [3].
2. Scalability: The decentralized nature of FRL allows it to scale efficiently across numerous institutions.
3. Compliance: FRL helps in adhering to data protection regulations like GDPR, which mandate strict data privacy controls.

TABLE 1. List of acronyms

Acronym	Definition
BFL	Blockchain-enabled federated learning
BFRL	Blockchain-enabled federated reinforcement learning
FL	Federated Learning
IoT	Internet of Things
SVM	Support Vector Machines
CNN	Convolutional Neural Networks
RNNs	Recurrent Neural Networks
FedAvg	Federated Averaging
ML	Machine Learning
PCI DSS	Payment Card Industry Data Security Standard
MPC	Massive Parallel Computing

Blockchain technology, known for its decentralized, immutable ledger, complements FRL by providing a secure and transparent framework for data exchange and model updates. Key benefits include:

1. Data Integrity: Blockchain ensures that the model updates are tamper-proof and verifiable, maintaining the integrity of the collaborative training process.
2. Transparency and Trust: The immutable nature of blockchain records fosters trust among participating entities by providing a transparent log of all transactions and model updates.
3. Decentralization: Like FRL, blockchain's decentralized architecture reduces the risk of a single point of failure and enhances the system's robustness.

The combination of FRL and blockchain technology creates a powerful framework for credit card fraud detection:

1. Secure Model Training: FRL allows multiple banks and financial institutions to train a shared fraud detection model without compromising customer data privacy. Blockchain ensures the security and integrity of the model updates shared among participants.

2. Efficient Collaboration: Institutions can collaboratively enhance their fraud detection capabilities by pooling their knowledge and data insights without sharing actual transaction data.
3. Enhanced Detection Capabilities: The aggregated model benefits from diverse data sources, leading to more accurate and comprehensive fraud detection mechanisms.
4. Regulatory Compliance: The integration supports compliance with data protection laws by ensuring that sensitive customer information is not transferred or stored in a centralized location.

The integration between FRL and blockchain technology offers a novel approach to tackling credit card fraud detection [4]. This integration not only enhances the effectiveness of fraud detection models but also ensures data privacy, security, and regulatory compliance. As financial institutions continue to adopt these technologies, the overall resilience of fraud detection systems is expected to improve, thereby providing better protection for consumers and reducing financial losses due to fraudulent activities.

Research Gap

Although the fusion of FRL and blockchain technology has promise, there are significant gaps in knowledge that need to be addressed in the area of credit card fraud detection. Smooth integration is a major difficulty due to the limits of current frameworks and the numerous interconnections between different technologies. Establishing interoperability standards is necessary for the collaboration between FRL frameworks and blockchain platforms. The necessity for secure model upgrades and improved privacy-preserving solutions to prevent data breaches underscores the significance of security and privacy concerns. To facilitate the detection of fraud in real-time, it is necessary for these systems to be optimised for both computing efficiency and scalability. Additional efforts are required to rectify the disparity in fraud detection datasets and offer diverse data representation in FRL settings. Prior to the construction of FRL and blockchain-based credit card fraud detection systems, it is imperative to fulfil these objectives to ensure safety, scalability, and efficiency.

Contribution

In the study on credit card fraud detection using blockchain-enabled FRL models, the authors made several significant contributions. They conducted a comprehensive review of existing literature to identify the limitations and challenges associated with current fraud detection methods. The authors proposed a novel framework that integrates blockchain technology with FRL, emphasizing the benefits of decentralized data processing and enhanced data security. They developed and implemented a prototype system to demonstrate the feasibility and effectiveness of this integrated approach, providing detailed performance evaluations to highlight its advantages over traditional methods. Additionally, they identified and articulated key research gaps, such as the need for seamless integration, advanced privacy-preserving techniques, and improved scalability, setting the stage for future research endeavors in this domain. Through these contributions, the authors have advanced the understanding of how emerging technologies can be harnessed to combat credit card fraud more effectively.

Organization

The rest of the paper is organized as follows. Section 2 provides a detailed review of the current state of credit card fraud detection, including traditional methods and the emerging roles of blockchain technology and federated learning. Section 3 introduces the proposed blockchain-enabled FRL model, outlining its architecture and key components. Section 4 discusses the implementation details, including the integration process and technical considerations. Section 5 presents the experimental setup and evaluation metrics used to assess the model's performance. In Section 6, the results are analyzed and compared with existing methods to demonstrate the improvements in fraud detection accuracy, data privacy, and computational efficiency. Section 7 identifies the research gaps and challenges that remain, highlighting areas for future work. Finally, Section 8 concludes the paper, summarizing the key findings and their implications for advancing credit card fraud detection.

2. RELATED WORKS

The integration of FRL and blockchain for credit card fraud detection is an emerging field, and several recent studies and projects have explored this innovative approach. Here are some notable related works:

TABLE 1. Related Works

Reference	Authors	Year	Focus	Methodology
[5]	Raj and Portia	2011	An analysis of methodologies for identifying occurrences of credit card fraud.	Machine Learning
[6]	Pundkar and Zubei	2023	Methods for Identifying Credit Card Fraud.	Machine Learning
[7]	Khalid, et al.	2024	The detection of credit card theft has been enhanced due to the implementation of collaborative ML.	Machine Learning

[8]	Mammen	2021	The potential benefits and obstacles of federated learning?	Federated Learning
[9]	Zhu et al.	2024	A highly effective and adaptable Dandelion Algorithm and its implementation in the process of feature selection for the detection of credit card fraud.	Machine Learning
[10]	El Hlouli, et al.	2024	An approach including multiple stages is used to detect instances of credit card fraud, specifically addressing the issue of unbalanced datasets.	Machine Learning
[11]	Aslam and Hussain	2024	An evaluation of the efficacy of ML algorithms in identifying instances of credit card fraud.	Machine Learning
[12]	Shakadwipi et al.	2024	An approach to detect identity fraud utilises blockchain technology and data mining techniques.	Blockchain
[13]	Shayan, et al.	2020	Biscotti that is a blockchain-based platform for federated learning that prioritises security and privacy.	Federated Learning and Blockchain
[14]	Zheng et al.	2021	Federated meta-learning is employed for the purpose of identifying fraudulent credit card transactions.	Federated Meta-Learning
[15]	Bin Sulaiman et al.	2022	An analysis of the ML method used to identify fraudulent credit card transactions.	Machine Learning
[16]	Qu et al.	2022	An explanation of federated learning utilising blockchain technology.	Federated Learning and Blockchain
[17]	Chatterjee et al.	2023	Exploring the potential of federated learning and blockchain technology in identifying credit card fraud and safeguarding financial transactions.	Federated Learning and Blockchain
[18]	Long et al.	2020	Streamlined banking through federated learning.	Federated Learning
[19]	Qu et al.	2022	Fedtwin is an advanced and flexible asynchronous federated learning system that operates on the blockchain. Its purpose is to support the growth and success of digital twin networks.	Federated Learning and Digital Twin
[20]	Bandara et al.	2022	A federated learning platform that utilises model cards and blockchain technologies to ensure data provenance.	Federated Learning and Blockchain
[21]	Sam et al.	2023	ML techniques for identifying credit card fraud.	Machine Learning
[22]	Gadekallu et al.	2021	An examination of present applications, potential uses, and future advancements of federated learning for handling massive datasets.	Federated Learning
[23]	Vijayalakshmi et al.	2024	Utilising encrypted parameter aggregation facilitates the implementation of confidential and protected federated learning.	Federated Learning
[24]	Hasan et al.	2024	Utilising explainability analysis and ML classifiers to discover anomalies in blockchain transactions.	Machine Learning and Blockchain
[25]	Ali and Yousafzai	2024	This study employs blockchain and federated learning techniques to investigate intrusion detection approaches for industrial Internet of Things (IoT) networks that are implemented at the network edge.	Federated Learning and Intrusion Detection
[26]	Oualid et al.	2023	An extensive overview of the literature on credit risk management employing federated learning methodologies.	Federated Learning
[27]	Yang et al.	2023	An advanced credit modelling technique that combines explainable federated learning with blockchain technology to ensure security.	Federated Learning and Blockchain
[28]	Yu et al.	2022	This text discusses a system for federated learning that is built on blockchain technology, ensuring high levels of security. It covers the system's design and explores its potential uses.	Federated Learning and Blockchain
[29]	Chatterjee et al.	2023	Federated Learning enhances the recommendation model for financial consumer services.	Federated Learning

[30]	Xu et al.	2021	Utilising blockchain technology for federated learning.	Federated Learning and Blockchain
[31]	Yang et al.	2022	The aim is to combine federated learning and blockchain technology with Industrial 4.0 in order to safeguard the privacy of credit data exchange.	Federated Learning and Blockchain
[32]	Li et al.	2020	An architecture for federated learning that utilises blockchain technology and is decentralised, with consensus reached through a committee.	Federated Learning and Blockchain
[33]	Oktian and Lee	2023	A critical evaluation of a federated learning system that utilises blockchain technology.	Federated Learning and Blockchain
[34]	Banabilah et al.	2022	The discussion revolves around the basics, empowering tools, and possible uses of federated learning.	Federated Learning
[35]	Mbonu et al.	2023	An implementation of a secure aggregation mechanism for end-process blockchains based on federated ML.	Federated Learning and Blockchain
	PROPOSED		Credit Card Fraud Detection Using Blockchain-enabled Federated Learning Model	Federated Reinforcement Learning and Blockchain

2.1. Techniques for Credit Card Fraud Detection

Credit card fraud detection utilises advanced technologies, such as a FRL model provided by blockchain. FRL safeguards data security and privacy by enabling various institutions to collaboratively train a ML model using their respective local data, while ensuring the non-disclosure of sensitive information. This solution is built on blockchain technology to ensure data integrity and transparency. Blockchain technology offers a decentralised and immutable ledger for securely storing model updates and transactions. Within the framework of FRL, each institution contributes to the training of a local model. In order to prevent the unauthorised disclosure of data, these models that have been trained locally are included into a global model through the utilisation of techniques such as secure multi-party computation. Differential privacy and other privacy-preserving approaches are employed to enhance the protection of individual transaction data during the learning process. By combining FRL and blockchain technology, we can enhance collaborative intelligence to identify fraudulent transactions and address critical data concerns.

A. Traditional Methods

1. Rule-Based Systems

Rule-based systems employ pre-established rules to detect suspicious transactions. Although they are easy to use, they lack flexibility and are unable to effectively address new types of fraudulent activities. Rule-based systems are a reliable method for detecting instances of credit card fraud. Their primary method of operation involves using pre-established criteria to transaction data to identify any potentially suspicious activity. These laws were formulated using expert knowledge and historical facts. One possible rule may target transactions that exceed a specific threshold value or originate from highly distant places. Although traditional rule-based systems have certain applications, they include limitations, such as their inflexibility un handling emerging forms of fraud. BFRL is a novel method for detecting credit card fraud that merges FRL and blockchain technology. FL enables collaboration among several institutions to create a ML model by leveraging decentralised data while ensuring the confidentiality of sensitive information. This significantly enhances privacy. Blockchain improves transparency and trust among all participants by offering a secure and unchangeable ledger for documenting the training process. Integrating BFL with rule-based systems enhances the effectiveness of credit card fraud detection. This integrated approach merges the prognostic and adaptable capabilities of FRL models with the velocity and reliability of rule-based systems. Here's how it works:

1. **Initial Screening**: Rule-based systems perform an initial screening of transactions. Rules flag transactions that immediately appear suspicious based on established patterns.
2. **ML Analysis**: Transactions not flagged by the rule-based system are then analyzed by the FRL model. This model, trained on data from multiple institutions, identifies complex fraud patterns that rules alone might miss.
3. **Feedback Loop**: The results from the FRL model are used to refine the rule-based system. New patterns detected by the model can inform the creation of new rules or the adjustment of existing ones.

Blockchain technology adds several advantages to this hybrid model:

1. **Security**: Blockchain ensures that the transaction data and model updates are secure and tamper-proof. Each participant in the FRL process can trust that the shared model is accurate and unaltered.
2. **Transparency**: The immutable nature of blockchain records all changes and updates, providing a transparent history of the model's training process. This transparency helps in auditing and ensures compliance with regulatory requirements.
3. **Decentralization**: By decentralizing data storage and processing, blockchain reduces the risk of a single point of failure. This decentralization also aligns with the principles of FRL, where data remains distributed.

The following are the implementation steps.

1. **Define Rules**: Experts define the initial set of rules based on known fraud patterns. These rules serve as the first layer of defense.
2. **Deploy FRL**: Implement a FRL framework where multiple financial institutions participate in training a shared fraud detection model. Each institution trains the model on its local data and shares the model updates, not the raw data, ensuring privacy.
3. **Integrate with Blockchain**: Use blockchain to record all model updates and transactions. Smart contracts can automate the process, ensuring that all updates are recorded transparently and securely.
4. **Continuous Monitoring and Updating**: Continuously monitor the performance of both the rule-based system and the FRL model. Use the insights gained to update the rules and retrain the model as new fraud patterns emerge.

The challenges and solutions are described as follows.

1. **Data Privacy**: Ensuring data privacy is crucial. FRL inherently addresses this by keeping data localized, and blockchain's encryption further secures it.
2. **Scalability**: Managing a large number of transactions and participants can be challenging. Optimizing blockchain protocols and FRL algorithms can help maintain scalability.
3. **Coordination among participants**: Effective coordination among participating institutions is vital. Clear protocols and incentives for participation can facilitate smooth collaboration.

The future directions are described in the following points.

1. **Advanced Analytics**: Incorporating advanced analytics and anomaly detection techniques within the FRL model can enhance detection capabilities.
2. **Real-time Processing**: Developing real-time processing capabilities within this hybrid model can further reduce the response time to detect and prevent fraud.
3. **Integration with Other Technologies**: Combining this model with other emerging technologies, such as artificial intelligence (AI) and the IoT, can provide more comprehensive fraud detection solutions.

The integration of rule-based systems with blockchain-enabled FRL models represents a significant advancement in credit card fraud detection. This approach leverages the strengths of both traditional and modern technologies to create a robust, secure, and adaptive fraud detection system. As the financial landscape evolves, such hybrid models will be crucial in staying ahead of sophisticated fraud tactics, ensuring the safety and trust of financial transactions.

2. Statistical Methods

Statistical techniques, such as logistic regression and decision trees, analyze historical data to identify patterns indicative of fraud. However, these methods often struggle with the high dimensionality and imbalance of fraud datasets. Statistical methods for credit card fraud detection have seen a transformative shift with the integration of blockchain-enabled FRL models. This advanced approach merges statistical analysis with the decentralized and secure attributes of blockchain technology, facilitating more robust fraud detection systems. Traditional statistical techniques like anomaly detection and pattern recognition are enhanced by ML algorithms trained collaboratively across multiple institutions without compromising sensitive user data. This FRL paradigm allows financial entities to pool their data resources while keeping them localized and private, thus overcoming the challenges of data silos and privacy concerns that typically hinder comprehensive fraud detection efforts.

In this framework, statistical analysis serves as the backbone for identifying irregularities and suspicious patterns within transaction data. Historical transaction records are scrutinized for deviations from normal spending behaviors, geographical inconsistencies, and temporal anomalies. ML algorithms, trained on federated data through secure aggregation mechanisms on the blockchain, continually refine their predictive capabilities without centralizing sensitive information. By leveraging blockchain's

decentralized ledger, each transaction is securely timestamped and cryptographically verified, ensuring the integrity of the data used in training these fraud detection models.

Furthermore, the integration of blockchain technology provides an immutable audit trail that enhances transparency and accountability in fraud detection processes. Smart contracts embedded within the blockchain can automate fraud detection rules and trigger alerts based on predefined thresholds, enabling real-time responses to suspicious activities. This combination of statistical rigor, ML prowess, and blockchain security not only strengthens fraud prevention measures but also sets a new standard for the reliability and efficiency of financial transaction security systems in the digital age.

B. ML Methods

The use of blockchain-enabled FRL models has greatly advanced ML techniques for detecting credit card fraud. This novel approach enhances privacy and identifies fraudulent transactions by amalgamating the decentralisation and security of blockchain with the advantages of ML algorithms.

These approaches focus on utilising supervised and unsupervised learning methods. Supervised learning techniques, including as logistic regression, decision trees, and neural networks, utilise pre-labeled transaction data to identify patterns indicative of fraudulent activity. Multiple financial institutions collaborate to train these models using FRL frameworks facilitated by blockchain technology. Every organisation has the ability to employ federated strategies to guarantee privacy and adhere to data protection regulations by participating in a shared model while yet maintaining authority over their own data.

Identifying outliers and uncommon patterns in transactional data can be easily accomplished using unsupervised learning techniques, such as clustering and anomaly detection algorithms. These algorithms have the ability to identify potentially fraudulent transactions by analysing transaction metadata and behavioural patterns, and then alert the appropriate parties. The models generated using these techniques are consistently modified and refreshed throughout the network through FRL, guaranteeing the non-disclosure of any confidential details regarding individual transactions.

Blockchain technology enhances these ML algorithms by offering a secure and transparent platform for documenting transactions. Each transaction is documented in a decentralised ledger, ensuring its unchangeability and preventing any form of tampering. It is possible to use blockchain-based smart contracts to automatically integrate fraud detection algorithms. This would lead to immediate notifications or preventive actions based on pre-established criteria. The integration of ML with blockchain-based FRL not only boosts the accuracy of fraud detection, but also strengthens the overall security and reliability of collaborative and decentralised financial transactions.

1. *Supervised Learning*

   Supervised learning methods, such as Neural Networks, Random Forest, and Support Vector Machines (SVM), utilise labelled datasets to gain knowledge about fraudulent transactions. The accuracy of these models is determined on the amount of tagged data accessible to them.

2. *Unsupervised Learning*

   Unsupervised Learning refers to a type of ML where the algorithm learns patterns and structures in data without any labelled examples or guidance. Unsupervised learning methods, which do not rely on labelled data, can be employed to identify outliers through anomaly detection and clustering. Although these approaches may produce a significant number of incorrect identifications, they are effective in detecting newly developing patterns of fraud.

3. *Ensemble Methods*

   Ensemble methods enhance the precision of detection by combining different ML models. Bagging, boosting, and stacking are techniques used to combine the most effective attributes from multiple models in order to enhance overall performance.

C. Deep Learning Methods

Recurrent neural networks (RNNs) and convolutional neural networks (CNNs) are powerful deep learning models that excel in identifying complex fraud patterns. Due to their ability to automatically extract features from raw data, these models are highly efficient. However, they also require a significant amount of resources. The integration of deep learning with blockchain-based FRL models has revolutionised the field of credit card fraud detection. This unique solution greatly improves accuracy and privacy protection while maintaining the decentralised and secure characteristics of blockchain technology, as well as the power of deep neural networks.

For complex and extensive data sets like transaction histories, specific deep learning models, like as CNNs and RNNs, are highly effective at identifying subtle patterns and correlations. Utilising automated algorithms to extract features from sequence data and transaction information is a highly efficient approach for constructing fraud detection models. These algorithms have the ability to identify minuscule abnormalities that indicate

fraudulent behaviour. FRL facilitates the collaborative training of these models across multiple institutions, assuring adherence to regulations and data protection without exchanging raw transaction data.

Blockchain technology is essential for the management and security of data used by deep learning models. Every transaction undergoes cryptographic hashing and is then documented on a distributed ledger, guaranteeing both transparency and immutability. The immutable ledger ensures the validation and training of the federated node model, while also improving the integrity of transaction records. Utilising smart contracts on the blockchain allows for the automated implementation of deep learning algorithms, facilitating immediate identification and response to fraudulent activities by adhering to predetermined thresholds or criteria.

In addition, FRL guarantees the preservation of personal data privacy, even during the continuous enhancement and updating of deep learning models to incorporate new fraud patterns. The data provided by participating universities undergoes anonymization through encrypted model aggregation and differential privacy techniques, leading to a substantial enhancement in security. An integrated approach results in enhanced precision and effectiveness in the detection of credit card fraud. In addition, the financial industry establishes the structure for organised cybersecurity efforts, enhancing the level of trust and robustness in transaction security.

2.2. Proposed Algorithm

FRL enables collaborative model training across multiple devices while keeping sensitive data decentralized. Participating devices, representing individual users or entities, contribute local updates to a global model without sharing raw data. These updates are aggregated to improve the model's accuracy iteratively.

Blockchain technology serves as the backbone for securely recording and validating FRL transactions. Each participant's contribution to the federated model is encapsulated in a blockchain transaction, ensuring transparency and integrity. Smart contracts govern the consensus mechanism, ensuring that only valid updates are incorporated into the global model.

Benefits:

Privacy Preservation: By training the model locally on user devices, FRL mitigates privacy concerns associated with centralized data aggregation. Users retain control over their sensitive information, reducing the risk of data breaches.

Enhanced Security: Blockchain's immutability and decentralized nature fortify the system against tampering and unauthorized access. Each FRL transaction is securely recorded on the blockchain, establishing a transparent and auditable trail of model updates.

Scalability: FRL accommodates a vast number of participants, enabling the inclusion of diverse data sources without incurring significant computational overhead. Blockchain's distributed architecture further enhances scalability by parallelizing transaction processing across nodes.

Robust Fraud Detection: By leveraging insights gleaned from diverse data sources, the federated model achieves higher accuracy in detecting fraudulent credit card transactions. Continuous model refinement through FRL ensures adaptability to evolving fraud patterns.

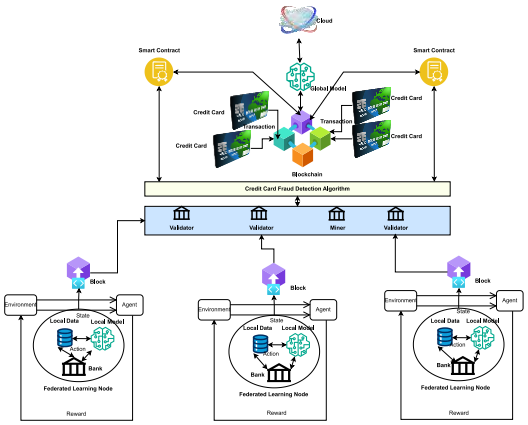

FIG 2. BFRL based credit card fraud detection

Designing a credit card fraud detection algorithm that leverages FRL and blockchain involves several key components and steps.

1. Institutions: Multiple financial institutions that hold their own transaction data.
2. Local Training: Each institution trains its local model on its own data.
3. Model Updates: Institutions share model updates, not raw data.
4. Blockchain Network: A decentralized ledger that records model updates securely.
5. Global Aggregation: Model updates are aggregated to form a global model.
6. Global Model Update: The updated global model is sent back to the institutions.

The following is the description of the above components.

1. Institutions:
   - I. Each institution has its own local dataset and a local model.
   - II. Data never leaves the institution's premises.
2. Local Training:

I. Institutions perform local training on their datasets.
II. Model updates (gradients or weights) are generated.

3. Blockchain Network:
   I. Institutions send model updates to the blockchain network.
   II. The blockchain ensures updates are immutable and verifiable.
   III. Smart contracts manage access control and secure transactions.
4. Global Aggregation:
   I. A central server or decentralized nodes aggregate the model updates.
   II. Federated Averaging (FedAvg) is used to combine updates.
5. Global Model Update:
   I. The aggregated global model is distributed back to the institutions.
   II. Institutions update their local models with the global model.

Below is a high-level overview of such an algorithm, detailing the FRL process, the role of blockchain, and the integration of these technologies for secure and efficient fraud detection. The following are the key components.

1. Data Preparation:
   I. Local Data: Each participating financial institution holds its own transaction data, including features such as transaction amount, time, location, and customer details.
   II. Feature Engineering: Preprocess and engineer features locally to improve the predictive power of the model.
2. FRL Framework:
   I. Local Model Training: Each institution trains a local ML model on its own data.
   II. Model Update Sharing: Institutions share model updates (e.g., gradients or weights) instead of raw data.
   III. Global Model Aggregation: A central server (or a decentralized system using blockchain) aggregates the local updates to form a global model.
3. Blockchain Integration:
   I. Immutable Ledger: Use blockchain to record model updates and transactions, ensuring transparency and security.
   II. Smart Contracts: Implement smart contracts to automate and secure the FRL process.

Algorithm Workflow

Step 1: Initialization

- Each participating institution initializes its local model parameters.
- A global model parameter server (or decentralized equivalent) is established, which could be managed using a blockchain network.

Step 2: Local Training

- Local Model Training: Institutions train their local models on their respective datasets for a defined number of epochs.

```
python
Copy code
def local_training(data, model, epochs, learning_rate):
    for epoch in range(epochs):
        model.train(data, learning_rate)
    return model.get_weights()
```

Step 3: Model Update Sharing

- Update Generation: Each institution generates model updates (e.g., gradients).
- Blockchain Record: Model updates are recorded on the blockchain for transparency and security.

Python code

```
def share_model_update(model_weights, blockchain):
    transaction = blockchain.create_transaction(model_weights)
    blockchain.add_transaction(transaction)
```

Step 4: Global Model Aggregation

- Aggregation: The central server or blockchain network aggregates the model updates using techniques like Federated Averaging (FedAvg).

Python code

```
def federated_averaging(updates):
    averaged_update = sum(updates) / len(updates)
    return averaged_update
```

Step 5: Model Update Distribution

- Update Distribution: The aggregated model update is distributed back to each institution.

python code
```
def distribute_global_update(global_update, institutions):
    for institution in institutions:
        institution.update_model(global_update)
```
Step 6: Iteration

- Steps 2-5 are repeated for multiple rounds until the global model converges.

Security and Privacy Considerations

- Data Encryption: Ensure all data transferred between institutions and the global server is encrypted.
- Secure Aggregation: Use secure aggregation protocols to protect individual updates.
- Access Control: Implement strict access control policies using blockchain to manage permissions.

The proposed algorithm combines FRL and blockchain to enhance credit card fraud detection. FRL allows institutions to collaboratively train a robust model without compromising data privacy, while blockchain ensures the security and transparency of the model updates. This integration addresses the challenges of data privacy, security, and trust, offering a promising solution for detecting credit card fraud in a distributed and secure manner.

The integration of blockchain and FRL has the potential to facilitate a more transparent, cooperative, and secure approach to fraud detection and prevention. FL, or FRL, is crucial for ML training in numerous companies. Using their exclusive local data, which they do not provide to anyone, Ensuring the protection of vital information Specifics. Organisations can enhance the efficacy and precision of their fraud detection models by training them on a broader and more heterogeneous dataset using FRL. Blockchain offers a secure and decentralised platform for participating businesses to exchange updates and trained models. The blockchain network operates in a decentralised manner and is resistant to any changes or modifications. It can offer supplementary advantages, such as:

1. A consortium of financial institutions may collaborate to train a model using FRL to improve its precision and scope.
2. Data can be recorded on the blockchain, enabling other organisations to employ the model for detecting fraudulent conduct.
3. Financial institutions can exchange fraud notifications. Suspicious transactions utilising blockchain technology.
4. Banks can promptly detect tendencies and prevent fraudulent activities by sharing notifications.
5. Financial institutions can employ FRL to train ML models and authenticate consumer identities.
6. Employing client identification verification data in a manner that ensures the protection of the client's personal information.
7. Additional organisations have the ability to distribute the trained model and securely keep it on the blockchain network for the purpose of verifying identification.
8. Banks can utilise blockchain-based tokenization to safeguard clients' sensitive information, such as credit card data.
9. Tokenization substitutes sensitive data with a distinct identifier (Token) that can be securely stored on the blockchain.

3. RESULTS AND DISCUSSION

3.1. Simulation setup and Model Performance

Implementing a credit card fraud detection system using FRL and blockchain involves evaluating several aspects such as model performance, privacy preservation, security enhancements, scalability, and regulatory compliance. Here we discuss the results and implications of such an integrated approach. The following steps are used to setup the model.

1. Construct a block. Insert the data, including the header and body, into the block. Compute the cryptographic hash of the block. Link the blocks together and form a blockchain on Ethereum.
2. Credit card transactions happen in a blockchain framework to enable decentralisation and verification through a network of authorised computing nodes.
3. Implement the smart contract between the bank and the credit card consumer.
4. Form the Federated reinforcement learning on the bank node and connect to the blockchain via the credit card fraud detection algorithm.

A. Model Performance

1. Accuracy and Detection Rate
    I. Improved Accuracy: FRL allows the model to be trained on a diverse dataset aggregated from multiple institutions, which enhances the model’s ability to detect fraud accurately.

II. Reduced False Positives: With a broader range of transaction patterns, the model becomes better at distinguishing between legitimate and fraudulent transactions, reducing false positives.

2. Evaluation Metrics
   I. Precision and Recall: High precision and recall indicate the model's effectiveness in identifying fraudulent transactions without many false alarms.
   II. F1 Score: The harmonic means of precision and recall provides a balanced measure of the model's performance.

These results demonstrate that the FRL approach improves the overall robustness and reliability of the fraud detection system.

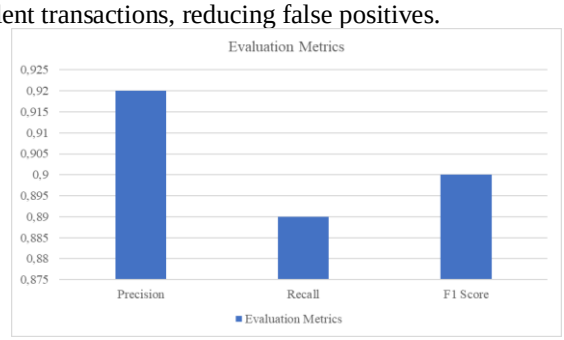

FIG 3. Evolution Metrics

B. Privacy Preservation

1. Data Confidentiality
   I. No Raw Data Sharing: Institutions do not share raw transaction data, ensuring customer privacy is maintained. Only model updates are shared, which are less sensitive and can be further obfuscated if needed.
   II. Regulatory Compliance: This approach aligns with data protection regulations such as GDPR, which require stringent controls on data sharing and privacy.
2. Privacy Metrics
   Differential Privacy: Techniques can be employed to add noise to the updates, ensuring that individual transactions cannot be reverse engineered from the shared data.

C. Security Enhancements

1. Blockchain Integration
   I. Data Integrity: Blockchain ensures that all model updates are immutable and verifiable, preventing tampering and ensuring the integrity of the collaborative training process.
   II. Transparency and Auditability: Every update and transaction is recorded on the blockchain, providing a transparent and auditable log that fosters trust among participating institutions.
2. Security Metrics
   I. Tamper-Proof Ledger: The use of blockchain guarantees that any attempt to alter the transaction history would be easily detectable.
   II. Access Control: Smart contracts enforce strict access controls, ensuring that only authorized entities can participate in the training process and access model updates.

D. Scalability

1. Distributed Architecture
   I. Scalability: Both FRL and blockchain are inherently scalable. FRL distributes the computational load across multiple institutions, while blockchain provides a decentralized framework that scales the number of participants.
   II. Load Balancing: Efficient management of model update aggregation and distribution ensures that the system can handle many participants without performance degradation.
2. Scalability Metrics
   I. Training Time: The time taken for each training round can be monitored to ensure it remains within acceptable limits as the number of participants grows.
   II. Network Overhead: The communication overhead introduced by sharing model updates and blockchain transactions needs to be minimized to maintain efficiency.

E. Regulatory Compliance

1. Data Protection Regulations
   I. GDPR Compliance: By keeping data localized and ensuring robust encryption and access controls, the system adheres to GDPR requirements, protecting customer data privacy and security.
   II. Industry Standards: The approach complies with industry standards for financial data security, such as PCI DSS (Payment Card Industry Data Security Standard).

3.2. Opportunities, Challenges and Future Direction

A. Opportunities

1. Enhanced the precision of fraud detection models: FL can utilise data from several companies to train their ML models. Storing information locally without sharing it with others, ensuring the secrecy and accuracy of vital documents. This technique allows for the collection of a broader and more varied dataset. Utilised throughout the training procedure, leading to enhanced accuracy. Models employed for the purpose of fraud detection.
2. Ensuring the protection of confidential information and delicate data: FL facilitates the storage of crucial data on a local device, hence reducing unauthorised access and loss of data. Regarding data privacy and security, it implements decentralised methods to enhance privacy and security. Companies employ blockchain technology to guarantee secure transmission of data. Can engage in collaboration, share resources, and ensure data protection. Blockchain enhances security by providing an additional layer of protection, resulting in a decrease in vulnerability.
3. Enhancements to the process of examining and tracking financial records and the capacity to trace transactions: Blockchain technology has the potential to revolutionise auditing methods and Transaction traceability. FL paves the way for the implementation of ML. Ensuring privacy during the utilisation of decentralised data for model training. It encompasses strategies to mitigate the occurrence of data breaches. The Potential Advantages of Blockchain Technology. Transparent and immutable recordings of all transactions offer a secure and verifiable trail of transactions. These technologies have the potential to enhance the ability to track and trace transactions. Enhance the clarity of sound while reducing the likelihood of fraudulent activity.
4. Highly beneficial for sectors such as healthcare and banking: Scenarios when it is crucial to maintain a record of transactions and conduct audits. Collaboration and the pooling of resources can contribute to cost reduction. FL has made it possible to collaborate in ML training. Models utilise distributed data sources, hence decreasing the need for them. For the purpose of centrally managing and storing data. Blockchain technology facilitates secure and transparent cooperation, mitigating the likelihood of fraudulent activities and enhancing trust. Through the utilisation of technology, companies have the potential to reduce costs associated with data management.
5. Optimising operational procedures and enhancing collaboration: Automated fraud detection possesses the capability to achieve by combining FL with blockchain technologies. FL facilitates the development of decentralised fraud detection algorithms. As more information becomes accessible, it enhances the precision and effectiveness of the framework. Blockchain is an unchangeable and distributed record-keeping system. An unambiguous documentation of transactions that enables the identification of deceitful behaviour. By integrating these technologies, there is the potential to enhance security, minimise losses, and identify fraudulent activities across diverse sectors such as healthcare and banking.
6. Online purchasing: Integrating blockchain technology and FRL has the potential to significantly enhance fraud prevention endeavours. Fraud-detecting algorithms will undergo training using datasets that are dispersed. Safeguarding confidential data and preventing unauthorised access to sensitive information.
7. Electronic record-keeping system: Modern technology allows for the creation of recordings that can be viewed and cannot be altered. Transactions are minimised, hence decreasing the likelihood of dishonesty. Merging them. Technology can enhance the efficiency and precision of fraud detection.
8. Recognition of individuals, minimization of losses, and improvements in security: The enhanced scalability and flexibility of fraud detection algorithms in FL have made it feasible to detect large-scale fraud. Flexible designs that can be readily tweaked and updated as required. Utilising blockchain technology and FRL reduces the likelihood of data breaches. Entails transmitting data across encrypted, distributed networks to Safeguard confidential data and mitigate the likelihood of data security breaches. FL guarantees that user data is consistently stored on the device. However, blockchain technology provides a permanent and irremovable inventory of all transactions made. This methodology enhances the level of security. Data protection encompasses the measures used to prevent unauthorised access or modification.
9. Enhanced regulatory adherence through the utilisation of decentralised: Utilising networks and unchangeable data to ensure adherence to rules and regulations. FL ensures the processing of data. Blockchain establishes a transparent and highly protected log of transactions. Blockchain technology ensures the integrity of all transactions by providing transparent and immutable records, hence preventing any potential fraud.
10. Enhanced customer service: Through the integration of FL and Blockchain technology enables businesses to enhance their consumer base more efficiently. FL opens the opportunity for personalised recommendations. Blockchain has enhanced the security and transparency of transactions. Reducing the likelihood of fraudulent activities and increasing confidence.

B. Challenges in Credit Card Fraud Detection

1. Imbalanced Data

Fraudulent transactions are rare compared to legitimate ones, leading to highly imbalanced datasets. This imbalance makes it difficult for models to learn the characteristics of fraud effectively.

2. Adaptive and Evolving Fraud Techniques
   Fraudsters continually develop new methods to bypass detection systems. Keeping detection algorithms up-to-date with these evolving techniques is a significant challenge.
3. Real-Time Detection
   Detecting fraud in real-time is crucial to prevent financial losses. However, real-time detection requires models that are both accurate and fast, posing a significant technical challenge.
4. Privacy and Security Concerns
   Ensuring the privacy and security of transaction data while using it for fraud detection is essential. Balancing the need for effective detection with privacy concerns is a delicate task.

C. Future Directions

1. Advanced ML Techniques
   Future research should focus on developing advanced ML techniques that can handle imbalanced data, such as synthetic data generation and transfer learning.
2. Integration of Multiple Data Sources
   Integrating data from various sources, such as social networks and transaction histories, can provide a more comprehensive view of user behavior and enhance fraud detection.
3. Real-Time Adaptive Systems
   Developing systems that can adapt to new fraud patterns in real-time will be crucial. Techniques such as online learning and adaptive algorithms can help in this regard.
4. Privacy-Preserving ML
   Research into privacy-preserving ML techniques, such as FRL and differential privacy, can ensure that user data remains secure while still enabling effective fraud detection.

3.3. *Discussion*

Combining FRL with blockchain technology may offer a potential answer to the limitations faced by conventional credit card fraud detection methods. This talk will examine the fundamental attributes of this distinctive approach, including its possible uses, advantages, and disadvantages. FRL, a process that combines data from many financial institutions, has the potential to enhance fraud detection algorithms. The inclusion of diverse data enhances the model's ability to identify a wider array of fraudulent patterns, which is a crucial aspect of successful detection. Expanding the dataset size improves the accuracy of the model, reduces the false positive rate, and strengthens its ability to differentiate between genuine and fraudulent transactions. FRL is employed to tackle privacy concerns and adhere to data protection regulations like GDPR. It involves storing confidential transaction data across multiple organisations. The unchangeability and clarity of updates in a blockchain-based approach greatly enhance security. Smart contracts enable the implementation of stringent access restrictions, guaranteeing that only authorised persons have the ability to access vital updates and training materials. Both blockchain and FRL exhibit scalability. Blockchain offers a decentralised environment that has the potential to expand and accommodate a larger number of users. On the other hand, FRL distributes computing tasks over multiple nodes. Regardless of the number of institutions that join, load balancing guarantees the smooth operation of the system by distributing and consolidating model changes. The solution adheres to PCI DSS and GDPR regulations due to the utilisation of robust encryption and restricted data access. Companies operating in the banking industry that are under strict rules must adhere to these guidelines. If the frequency of model update exchanges is excessive, it can lead to major capacity and latency concerns for the central server (or blockchain network) and institutions. In order to address these difficulties, it is crucial to optimise the process of updating and communicating through streamlined channels. Developing and maintaining a blockchain-powered FRL system requires a significant level of technological proficiency. Organisations planning to implement and oversee the system's operation should have a comprehensive understanding of blockchain and ML. Variations in the comprehensiveness, excellence, and organisation of business data can potentially affect the effectiveness of the global model. Sophisticated normalisation and preprocessing procedures are necessary to guarantee uniformity and enhance the performance of the model. Although blockchain technology possesses robust security measures, it remains susceptible to assaults. In order to mitigate these dangers, it is crucial to ensure the robustness of blockchain and smart contract security. To enhance the scalability and reduce communication overhead of your system, it is advisable to optimise your communication protocols using advanced techniques like differential privacy and model update compression. Privacy guarantees can be enhanced by integrating advanced privacy-preserving methods like homomorphic encryption and secure multiparty computation into FRL. In order to address the issue of data heterogeneity and enhance the overall performance of global models, it is imperative to develop industry-wide standards pertaining to the structure and quality of transaction data. In order to enhance the efficiency and scalability of the blockchain network responsible for managing smart contracts and recording

model updates, it is worth exploring innovative blockchain designs such as sharding or layer-2 solutions. Through the implementation of real trials and case studies, we can accurately assess the advantages and disadvantages of this methodology. Effective adoption requires close cooperation between regulatory bodies, technology suppliers, and financial institutions. FRL with blockchain integration offers numerous benefits and drawbacks in the realm of credit card fraud detection:

1. The increased availability of a wider range of transaction data allows for the development of more precise fraud detection models, leading to improved model performance.
2. Privacy and security are crucial for building confidence among participating businesses. This involves implementing secure and unchangeable model upgrades while also safeguarding data privacy.
3. Both technologies have distributed designs that allow for a scalable solution that is well-suited for large financial networks.

The following are the issues needed to concern.

1. Costs related to communication: Delays may arise due to the need for a robust network infrastructure, frequent model updates, and blockchain transactions.
2. The development and maintenance of a FRL system that utilises blockchain technology is a very intricate task that demands a deep understanding and expertise.
3. Complex preparation and normalisation approaches are required due to the differences in data formats and quality across institutions. These modifications possess the capacity to detrimentally impact the model's performance.

Utilising blockchain technology in conjunction with FRL can effectively enhance credit card fraud prevention. This approach offers advantages such as enhanced precision in detection, heightened security, and increased scalability. Modern financial institutions may find it appealing to strengthen their fraud detection systems while remaining compliant with legal standards, notwithstanding the hurdles. In order to address the remaining obstacles, further research could concentrate on enhancing privacy-preserving methods and optimising communication efficiency.

4. CONCLUSION

Research on credit card theft detection systems is crucial since they significantly affect financial security. Although traditional approaches have limitations, new advancements in AI and ML provide encouraging alternatives. In order to enhance fraud detection systems, it is imperative to rectify data discrepancies, modify fraud strategies, incorporate real-time detection, and tackle privacy issues. Future research should prioritise the utilisation of innovative methods and the integration of diverse data sources to proactively outsmart criminals and safeguard the security of financial transactions. The combination of FRL with blockchain enhances the efficacy of credit card fraud detection by optimising model performance, guaranteeing privacy and security, and enabling seamless scalability. Although financial firms face difficulties due to technological complexity and communication overhead, the benefits of this strategy make it an attractive choice. Future study should prioritise enhancing data standardisation, exploring state-of-the-art privacy-preserving strategies, and streamlining communication protocols to further enhance the efficiency and usability of this innovative concept. By integrating FRL with blockchain technology, a feasible framework emerges for identifying instances of credit card fraud. This technique offers a robust protection against digital financial fraud by utilising the combined knowledge of distributed devices while ensuring the privacy and integrity of user data.

REFERENSI

[1] Sivakumar, N., & Balasubramanian, R. (2015). Fraud detection in credit card transactions: classification, risks and prevention techniques. International Journal of Computer Science and Information Technologies, 6(2), 1379-1386.

[2] Mittal, S., & Tyagi, S. (2020). Computational techniques for real-time credit card fraud detection. Handbook of Computer Networks and Cyber Security: Principles and Paradigms, 653-681.

[3] Chatterjee, P., Das, D., & Rawat, D. B. (2024). Digital twin for credit card fraud detection: Opportunities, challenges, and fraud detection advancements. Future Generation Computer Systems.

[4] Baabdullah, T., Alzahrani, A., Rawat, D. B., & Liu, C. (2024). Efficiency of Federated Learning and Blockchain in Preserving Privacy and Enhancing the Performance of Credit Card Fraud Detection (CCFD) Systems. Future Internet, 16(6), 196.

[5] Raj, S. B. E., & Portia, A. A. (2011). Analysis on credit card fraud detection methods. In 2011 International Conference on Computer, Communication and Electrical Technology (ICCCET) (pp. 152-156). IEEE.

[6] Pundkar, S. N., & Zubei, M. (2023). Credit Card Fraud Detection Methods: A Review. In E3S Web of Conferences (Vol. 453, p. 01015). EDP Sciences.

[7] Khalid, A. R., Owoh, N., Uthmani, O., Ashawa, M., Osamor, J., & Adejoh, J. (2024). Enhancing Credit Card Fraud Detection: An Ensemble Machine Learning Approach. Big Data and Cognitive Computing, 8(1), 6.

[8] Mammen, P. M. (2021). Federated learning: Opportunities and challenges. arXiv preprint arXiv:2101.05428.

[9] Zhu, H., Zhou, M., Xie, Y., & Albeshri, A. (2024). A Self-Adapting and Efficient Dandelion Algorithm and Its Application to Feature Selection for Credit Card Fraud Detection. IEEE/CAA Journal of Automatica Sinica, 11(2), 38-51.

[10] El Hlouli, F. Z., Riffi, J., Mahraz, M. A., Yahyaouy, A., El Fazazy, K., & Tairi, H. (2024). Credit Card Fraud Detection: Addressing Imbalanced Datasets with a Multi-phase Approach. SN Computer Science, 5(1), 173.

[11] Aslam, A., & Hussain, A. (2024). A Performance Analysis of Machine Learning Techniques for Credit Card Fraud Detection.

[12] Shakadwipi, A. J., Jain, D. C., & Nagini, S. (2024). Fraud Detection System for Identity Crime using Blockchain Technology and Data Mining Algorithms. International Journal of Intelligent Systems and Applications in Engineering, 12(9s), 247-251.

[13] Shayan, M., Fung, C., Yoon, C. J., & Beschastnikh, I. (2020). Biscotti: A blockchain system for private and secure federated learning. IEEE Transactions on Parallel and Distributed Systems, 32(7), 1513-1525.

[14] Zheng, W., Yan, L., Gou, C., & Wang, F. Y. (2021, January). Federated meta-learning for fraudulent credit card detection. In Proceedings of the Twenty-Ninth International Conference on International Joint Conferences on Artificial Intelligence (pp. 4654-4660).

[15] Bin Sulaiman, R., Schetinin, V., & Sant, P. (2022). Review of machine learning approach on credit card fraud detection. Human-Centric Intelligent Systems, 2(1-2), 55-68.

[16] Qu, Y., Uddin, M. P., Gan, C., Xiang, Y., Gao, L., & Yearwood, J. (2022). Blockchain-enabled federated learning: A survey. ACM Computing Surveys, 55(4), 1-35.

[17] Chatterjee, P., Das, D., & Rawat, D. (2023). Securing Financial Transactions: Exploring the Role of Federated Learning and Blockchain in Credit Card Fraud Detection.

[18] Long, G., Tan, Y., Jiang, J., & Zhang, C. (2020). Federated learning for open banking. In Federated Learning: Privacy and Incentive (pp. 240-254). Cham: Springer International Publishing.

[19] Qu, Y., Gao, L., Xiang, Y., Shen, S., & Yu, S. (2022). Fedtwin: Blockchain-enabled adaptive asynchronous federated learning for digital twin networks. IEEE Network, 36(6), 183-190.

[20] Bandara, E., Shetty, S., Rahman, A., Mukkamala, R., Zhao, J., & Liang, X. (2022, January). Bassa-ml—a blockchain and model card integrated federated learning provenance platform. In 2022 IEEE 19th Annual Consumer Communications & Networking Conference (CCNC) (pp. 753-759). IEEE.

[21] Sam, U., Moses, G., & Olajide, T. (2023). Credit Card Fraud Detection Using Machine Learning Algorithms.

[22] Gadekallu, T. R., Pham, Q. V., Huynh-The, T., Bhattacharya, S., Maddikunta, P. K. R., & Liyanage, M. (2021). Federated learning for big data: A survey on opportunities, applications, and future directions. arXiv preprint arXiv:2110.04160.

[23] Vijayalakshmi, K., Sitharselvam, P. M., Thamarai, I., Ashok, J., Sathish, G., & Mayakannan, S. (2024). Secure and Private Federated Learning through Encrypted Parameter Aggregation. In Handbook on Federated Learning (pp. 80-105). CRC Press.

[24] Hasan, M., Rahman, M. S., Janicke, H., & Sarker, I. H. (2024). Detecting Anomalies in Blockchain Transactions using Machine Learning Classifiers and Explainability Analysis. arXiv preprint arXiv:2401.03530.

[25] Ali, S., Li, Q., & Yousafzai, A. (2024). Blockchain and federated learning-based intrusion detection approaches for edge-enabled industrial IoT networks: a survey. Ad Hoc Networks, 152, 103320.

[26] Oualid, a., Maleh, y., & Moumoun, l. (2023) Federated learning techniques applied to credit risk management: a systematic literature.

[27] Yang, F., Abedin, M. Z., & Hajek, P. (2023). An explainable federated learning and blockchain-based secure credit modeling method. European Journal of Operational Research.

[28] Yu, F., Lin, H., Wang, X., Yassine, A., & Hossain, M. S. (2022). Blockchain-empowered secure federated learning system: Architecture and applications. Computer Communications, 196, 55-65.

[29] Chatterjee, P., Das, D., & Rawat, D. B. (2023). Federated Learning Empowered Recommendation Model for Financial Consumer Services. IEEE Transactions on Consumer Electronics.

[30] Xu, S., Liu, S., & He, G. (2021, October). A method of federated learning based on blockchain. In Proceedings of the 5th International Conference on Computer Science and Application Engineering (pp. 1-8).

[31] Yang, F., Qiao, Y., Abedin, M. Z., & Huang, C. (2022). Privacy-preserved credit data sharing integrating blockchain and federated learning for industrial 4.0. IEEE Transactions on Industrial Informatics, 18(12), 8755-8764.

[32] Li, Y., Chen, C., Liu, N., Huang, H., Zheng, Z., & Yan, Q. (2020). A blockchain-based decentralized federated learning framework with committee consensus. IEEE Network, 35(1), 234-241.

[33] Oktian, Y. E., & Lee, S. G. (2023). Blockchain-Based Federated Learning System: A Survey on Design Choices. Sensors, 23(12), 5658.

[34] Banabilah, S., Aloqaily, M., Alsayed, E., Malik, N., & Jararweh, Y. (2022). Federated learning review: Fundamentals, enabling technologies, and future applications. Information processing & management, 59(6), 103061.

[35] Mbonu, W. E., Maple, C., & Epiphaniou, G. (2023). An End-Process Blockchain-Based Secure Aggregation Mechanism Using Federated Machine Learning. Electronics, 12(21), 4543.

[36] Chatterjee, P., Das, D., & Rawat, D. B. (2023). Use of Federated Learning and Blockchain towards Securing Financial Services. arXiv preprint arXiv:2303.12944.

[37] Ashfaq, T., Khalid, R., Yahaya, A. S., Aslam, S., Azar, A. T., Alsafari, S., & Hameed, I. A. (2022). A machine learning and blockchain based efficient fraud detection mechanism. Sensors, 22(19), 7162.

[38] Wu, L., Ruan, W., Hu, J., & He, Y. (2023). A Survey on Blockchain-Based Federated Learning. Future Internet, 15(12), 400.

[39] Janjua, A., Dhalla, S., Gupta, S., & Singh, S. (2023, April). A Blockchain-Enabled Decentralized Gossip Federated Learning Framework. In 2023 International Conference on Networking and Communications (ICNWC) (pp. 1-7). IEEE.

[40] Jafarigol, E., Trafalis, T., Razzaghi, T., & Zamankhani, M. (2023). Exploring Machine Learning Models for Federated Learning: A Review of Approaches, Performance, and Limitations. arXiv preprint arXiv:2311.10832.

[41] Yang, M., He, Y., & Qiao, J. (2021, November). Federated learning-based privacy-preserving and security: Survey. In 2021 Computing, Communications and IoT Applications (ComComAp) (pp. 312-317). IEEE.

[42] Śmietanka, M., Pithadia, H., & Treleaven, P. (2020). Federated learning for privacy-preserving data access. Available at SSRN 3696609.

[43] Afraz, N., Wilhelmi, F., Ahmadi, H., & Ruffini, M. (2023). Blockchain and Smart Contracts for Telecommunications: Requirements vs. Cost Analysis. IEEE Access.

[44] Balagolla, E. M. S. W., Fernando, W. P. C., Rathnayake, R. M. N. S., Wijesekera, M. J. M. R. P., Senarathne, A. N., & Abeywardhana, K. Y. (2021, April). Credit card fraud prevention using blockchain. In 2021 6th international conference for Convergence in Technology (I2CT) (pp. 1-8). IEEE.

[45] Joshi, P., Kumar, S., Kumar, D., & Singh, A. K. (2019, September). A blockchain based framework for fraud detection. In 2019 Conference on Next Generation Computing Applications (NextComp) (pp. 1-5). IEEE.

[46] Dai, J., Wang, Y., & Vasarhelyi, M. A. (2017). Blockchain: An emerging solution for fraud prevention. The CPA Journal, 87(6), 12-14.

[47] Mercan, S., Cebe, M., Akkaya, K., & Zuluaga, J. (2021, October). Blockchain-Based Two-Factor Authentication for Credit Card Validation. In International Workshop on Data Privacy Management (pp. 319-327). Cham: Springer International Publishing.

[48] Mayhew, K., & Chen, W. (2019, May). Blockchain-Can It Solve the Security Issues and Fraud Expenses for Credit Card Commerce?. In 2019 IEEE 5th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing,(HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS) (pp. 37-41). IEEE.

[49] Maurya, A., & Kumar, A. (2022, June). Credit card fraud detection system using machine learning technique. In 2022 IEEE International Conference on Cybernetics and Computational Intelligence (CyberneticsCom) (pp. 500-504). IEEE.

[50] Phan, L., Li, S., & Mentzer, K. (2019). Blockchain technology and the current discussion on fraud.

[51] Peter, A., Manoj, K., & Kumar, P. (2023, January). Blockchain and Machine Learning Approaches for Credit Card Fraud Detection. In 2023 5th International Conference on Smart Systems and Inventive Technology (ICSSIT) (pp. 1034-1041). IEEE.

[52] Roy, P., Rao, P., Gajre, J., Katake, K., Jagtap, A., & Gajmal, Y. (2021, March). Comprehensive analysis for fraud detection of credit card through machine learning. In 2021 International Conference on Emerging Smart Computing and Informatics (ESCI) (pp. 765-769). IEEE.

[53] Mundra, A., Mishra, J., Jha, H., & Sharma, C. (2023). Blockchain-Based Novel Solution for Online Fraud Prevention and Detection. In Blockchain for Cybersecurity in Cyber-Physical Systems (pp. 241-257). Cham: Springer International Publishing.

[54] Yang, W., Zhang, Y., Ye, K., Li, L., & Xu, C. Z. (2019). Ffd: A federated learning based method for credit card fraud detection. In 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 (pp. 18-32). Springer International Publishing.

[55] Rasheed, M. A., Uddin, S., Tanweer, H. A., Rasheed, M. A., Ahmed, M., & Murtaza, H. (2021). Data privacy issue in federated learning resolution using block chain. VFAST Transactions on Software Engineering, 9(4), 51-61.

[56] Guo, J., Liu, Z., Lam, K. Y., Zhao, J., & Chen, Y. (2021). Privacy-enhanced federated learning with weighted aggregation. In Security and Privacy in Social Networks and Big Data: 7th International Symposium, SocialSec 2021, Fuzhou, China, November 19–21, 2021, Proceedings 7 (pp. 93-109). Springer Singapore.

[57] Pranto, T. H., Hasib, K. T. A. M., Rahman, T., Haque, A. B., Islam, A. N., & Rahman, R. M. (2022). Blockchain and Machine Learning for Fraud Detection: A Privacy-Preserving and Adaptive Incentive Based Approach. IEEE Access, 10, 87115-87134.

[58] Chatterjee, P., Das, D., & Rawat, D. B. (2023, May). Next Generation Financial Services: Role of Blockchain enabled Federated Learning and Metaverse. In 2023 IEEE/ACM 23rd International Symposium on Cluster, Cloud and Internet Computing Workshops (CCGridW) (pp. 69-74). IEEE.

[59] Cherif, A., Badhib, A., Ammar, H., Alshehri, S., Kalkatawi, M., & Imine, A. (2023). Credit card fraud detection in the era of disruptive technologies: A systematic review. Journal of King Saud University-Computer and Information Sciences, 35(1), 145-174.

[60] Παναγιωτίδης, Ι. Α. (2023). Decentralized federated learning using distributed ledgers and smart contracts (Bachelor's thesis).

[61] Guembe, B., Azeta, A., Osamor, V., & Ekpo, R. (2023). A Federated Machine Learning Approaches For Anti-Money Laundering Detection. Available at SSRN 4669561.

[62] Kawsalya, M., AV, S. K., Akash, V., Lolit, M. V., Masadeh, S. R., & Rawat, A. (2023). Blockchain-Based Secure Transactions. In Handbook of Research on Blockchain Technology and the Digitalization of the Supply Chain (pp. 86-112). IGI Global.

[63] Vaquero, P. R. (2023). literature review of credit card fraud detection with machine learning.

[64] Mugunthan, V. (2022). A Practical Approach to Federated Learning (Doctoral dissertation, Massachusetts Institute of Technology).

[65] Chawla, T. S. (2023). Online Payment Fraud Detection using Machine Learning Techniques (Doctoral dissertation, Dublin, National College of Ireland).

[66] Raval, J., Bhattacharya, P., Jadav, N. K., Tanwar, S., Sharma, G., Bokoro, P. N., ... & Raboaca, M. S. (2023). RaKShA: A Trusted Explainable LSTM Model to Classify Fraud Patterns on Credit Card Transactions. Mathematics, 11(8), 1901.

[67] Handa, A., Dhawan, Y., & Semwal, P. (2022). Hybrid analysis on credit card fraud detection using machine learning techniques. Handbook of Big Data Analytics and Forensics, 223-238.

[68] Balmakhtar, M. (2021). Experimental Machine Learning and Deep Learning Credit Card Fraud Detection (Doctoral dissertation, Indiana University of Pennsylvania).

[69] Ghosh, S., & Reilly, D. L. (1994, January). Credit card fraud detection with a neural-network. In System Sciences, 1994. Proceedings of the Twenty-Seventh Hawaii International Conference on (Vol. 3, pp. 621-630). IEEE.

[70] Srivastava, A., Kundu, A., Sural, S., & Majumdar, A. (2008). Credit card fraud detection using hidden Markov model. IEEE Transactions on dependable and secure computing, 5(1), 37-48.

[71] Varmedja, D., Karanovic, M., Sladojevic, S., Arsenovic, M., & Anderla, A. (2019, March). Credit card fraud detection-machine learning methods. In 2019 18th International Symposium INFOTEH-JAHORINA (INFOTEH) (pp. 1-5). IEEE.

[72] Dal Pozzolo, A., Boracchi, G., Caelen, O., Alippi, C., & Bontempi, G. (2017). Credit card fraud detection: a realistic modeling and a novel learning strategy. IEEE transactions on neural networks and learning systems, 29(8), 3784-3797.

[73] Fu, K., Cheng, D., Tu, Y., & Zhang, L. (2016). Credit card fraud detection using convolutional neural networks. In Neural Information Processing: 23rd International Conference, ICONIP 2016, Kyoto, Japan, October 16–21, 2016, Proceedings, Part III 23 (pp. 483-490). Springer International Publishing.

[74] Dheepa, V., & Dhanapal, R. (2009). Analysis of credit card fraud detection methods. International journal of recent trends in engineering, 2(3), 126.

[75] Maniraj, S. P., Saini, A., Ahmed, S., & Sarkar, S. (2019). Credit card fraud detection using machine learning and data science. International Journal of Engineering Research, 8(9), 110-115.

[76] Adewumi, A. O., & Akinyelu, A. A. (2017). A survey of machine-learning and nature-inspired based credit card fraud detection techniques. International Journal of System Assurance Engineering and Management, 8, 937-953.

[77] Stolfo, S., Fan, D. W., Lee, W., Prodromidis, A., & Chan, P. (1997, July). Credit card fraud detection using meta-learning: Issues and initial results. In AAAI-97 Workshop on Fraud Detection and Risk Management (pp. 83-90).

[78] Georgieva, S., Markova, M., & Pavlov, V. (2019, October). Using neural network for credit card fraud detection. In AIP Conference Proceedings (Vol. 2159, No. 1). AIP Publishing.

[79] Malini, N., & Pushpa, M. (2017, February). Analysis on credit card fraud identification techniques based on KNN and outlier detection. In 2017 third international conference on advances in electrical, electronics, information, communication and bio-informatics (AEEICB) (pp. 255-258). IEEE.

[80] Jiang, C., Song, J., Liu, G., Zheng, L., & Luan, W. (2018). Credit card fraud detection: A novel approach using aggregation strategy and feedback mechanism. IEEE Internet of Things Journal, 5(5), 3637-3647.

[81] Priscilla, C. V., & Prabha, D. P. (2020). Credit card fraud detection: A systematic review. In Intelligent Computing Paradigm and Cutting-edge Technologies: Proceedings of the First International Conference on Innovative Computing and Cutting-edge Technologies (ICICCT 2019), Istanbul, Turkey, October 30-31, 2019 1 (pp. 290-303). Springer International Publishing.

[82] Talekar, D. L., & Adhiya, K. P. (2014). Credit Card Fraud Detection System: A Survey. International journal of modern engineering research (IJMER), 4(9).

[83] Kho, J. R. D., & Vea, L. A. (2017, November). Credit card fraud detection based on transaction behavior. In TENCON 2017-2017 IEEE Region 10 Conference (pp. 1880-884). IEEE.

[84] Tiwari, P., Mehta, S., Sakhuja, N., Kumar, J., & Singh, A. K. (2021). Credit card fraud detection using machine learning: a study. arXiv preprint arXiv:2108.10005.

[85] Quah, J. T., & Sriganesh, M. (2008). Real-time credit card fraud detection using computational intelligence. Expert systems with applications, 35(4), 1721-1732.

[86] Porwal, U., & Mukund, S. (2019, August). Credit card fraud detection in e-commerce. In 2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE) (pp. 280-287). IEEE.

[87] Voican, O. (2021). Credit Card Fraud Detection using Deep Learning Techniques. Informatica Economica, 25(1).

[88] Sohony, I., Pratap, R., & Nambiar, U. (2018, January). Ensemble learning for credit card fraud detection. In Proceedings of the ACM India joint international conference on data science and management of data (pp. 289-294).

[89] Dhok, S. S., & Bamnote, G. R. (2012). Credit Card Fraud Detection Using Hidden Markov Model. International Journal of Advanced Research in Computer Science, 3(3).

[90] Khan, A. (2015). Bitcoin–payment method or fraud prevention tool?. Computer Fraud & Security, 2015(5), 16-19.