ISSN 2581 – 3781

AJCSE
ASIAN JOURNAL OF COMPUTER SCIENCE ENGINEERING

Available Online at www.ajcse.info
Asian Journal of Computer Science Engineering 2025;10(4):1-9

REVIEW ARTICLE

Machine Learning and Deep Learning Techniques for Secure Credit Card Transaction Fraud Detection

Dr. Bal Krishna Sharma*

Department of Computer Sciences and Applications, Mandsaur University, Mandsaur, Madhya Pradesh, India

Received: 12-11-2025; Revised: 10-04-2026; Accepted: 02-05-2026

ABSTRACT

Fraudulent financial activities in digital payment systems pose a significant threat to individuals, businesses, and financial institutions worldwide, resulting in substantial economic losses and undermining consumer confidence. With the rapid expansion of online transactions, traditional rule-based detection methods have become insufficient to counter sophisticated and evolving fraud schemes. Machine learning (ML) and deep learning (DL) techniques provide effective solutions by automatically identifying complex patterns and anomalies in large volumes of transactional data. Supervised ML models, such as decision trees, logistic regression, and Naïve Bayes, offer efficient and interpretable classification of suspicious activities, while DL methods, including artificial neural networks, convolutional neural networks, and long short-term memory networks, excel at detecting subtle, non-linear, and sequential patterns. Leveraging these approaches enables real-time monitoring, adaptive behavioral modeling, and reduction of false positives, thereby enhancing fraud detection accuracy and reliability. Emerging trends such as federated learning, hybrid detection frameworks, and explainable AI further improve model transparency, privacy, and robustness in operational environments. This paper reviews the state-of-the-art ML and DL methodologies for secure financial transaction fraud detection, highlights key datasets, behavioral patterns, and challenges, and discusses innovative strategies shaping the next generation of fraud prevention systems.

Key words: Credit card fraud, deep learning, digital payment security, fraud prevention, machine learning, real-time transaction

INTRODUCTION

Credit card fraud refers to activities aimed at obtaining illicit benefits without the cardholder's permission. Common types of credit card fraud include unauthorized transactions and cash-out schemes. With the rapid development of Internet technology, the convenience of credit cards has led to their widespread use in all aspects of social life, significantly expanding the cardholder population and providing strong support for economic growth.[1] Despite robust legal frameworks in place to protect this domain, credit card fraud still occurs, causing direct economic losses to financial institutions and potentially damaging cardholders' credit records, thereby affecting their quality of life. However, the advantages of credit cards are burdened with serious security threats.[2] The possibilities of fraud are endless: stolen card details, account hijacking, and phishing can be used to help malicious users to make unauthorized transactions.[3] As an identity theft, credit card fraud may lead to significant losses and loss of consumer confidence in the banking systems. The dynamic character of fraud and the use of digital payments rapidly has posed a desperate demand to enhance more robust and versatile detection systems.

Detection of fraud is crucial so that it can ensure safe transactions, safeguard the consumers, and uphold the reputation of financial institutions. Efficient fraud detecting prevents losses of financial resources, reduces possible losses, and maintains the trust of users in financial payment systems based on credit.[4] The conventional methods of fraud detection, like reviews of transactions by humans or the use of rules, are not always effective in fighting fraud in the present

Address for correspondence:
Bal Krishna Sharma
E-mail: bksharma7426@gmail.com

day. Fraudsters are ever-evolving to avoid old-fashioned policies, and this makes the traditional ways very slow, tedious, and ineffective. Besides, manual detections are becoming progressively unfeasible as the amount of digital transactions and the complexity thereof increase.[5] Consequently, there exists a strong need to have smart systems that can detect and react to the emerging fraud tendencies in real time.

Machine learning (ML) and deep learning (DL) methods have become effective instruments to detect credit card fraud because complex patterns and anomalies in large volumes of transactional data are automatically identified. The methods will allow financial institutions to go beyond traditional fixed rules and use flexible, data-driven fraud detection systems.[6,7] Turnover ML techniques are logistic regression, decision trees, and random forests, which are able to simulate transaction behavior and identify suspicious activities. More complex DL methods, including neural networks and deep autoencoders, are capable of learning very non-linearity and subtle patterns and improving detection performance.

Through these methods, the fraud detection systems are able to dynamically change in response to the changing fraud tactics, cut down on false positives, and optimize the use of investigative resources. In addition, both ML and DL can be used to monitor transaction in real-time to ensure that financial institutions can identify and stop fraud before it can cause severe losses to the company. Since the digital payments market is constantly evolving, a combination of ML and DL in fraud prevention systems is a crucial move that will guarantee secure, reliable, and trustworthy credit card transactions.

Structure of the Paper

The paper is organized as follows. Section II defines credit card fraud: Its types, fraud patterns, and associated challenges. Section III presents ML and DL approaches for fraud detection, comparing different models and their strengths. Section IV discusses fraud prevention methods, system limitations, and emerging trends. Section V offers a literature review summarizing prior studies, their findings, and research gaps. Finally, Section VI concludes with key insights and recommendations for future work.

CONCEPT OF CREDIT CARD

Credit card fraud is a type of financial fraud that involves the unauthorized use of another person's credit card information to make fraudulent transactions or gain unauthorized access to funds.[8] It is a widespread and significant problem that affects individuals, businesses, and financial institutions worldwide. Credit card fraud can occur through various means, including physical theft, online scams, data breaches, and card skimming devices. The impact of credit card fraud is substantial, leading to financial losses for individuals, businesses, and financial institutions. Fraudulent transactions can result in unauthorized charges, identity theft, and compromised personal and financial information.[9,10] The consequences of credit card fraud extend beyond financial losses, as victims often experience stress, inconvenience, and the need to go through lengthy procedures to resolve fraudulent activities.

Types of Credit Card Fraud

There are several divisions that the main types of credit card fraud may fall under in Figure 1. These comprise both digital and physical ways that cards can be used without authorization:

- Application fraud: A fraudster gains access to an application system by stealing personal data, including a login and password, and fabricating an account. Usually, identity theft is the cause of this.
- Electronic or manual credit card imprints: The moment the scammer scans the information on

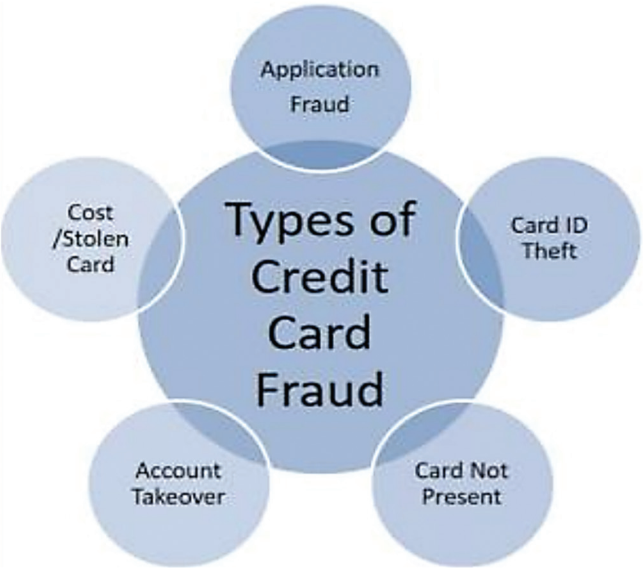

Figure 1: Types of credit card fraud[11]

the magnetic surface of the card. This data is very confidential, and if someone manages to obtain it, they might use it to commit fraud.

- CNP (card not present): The fraudster can use the card without being physically present as long as they know the account number and expiration date.
- Counterfeit card Fraud: A common way to try it is via skimming. All of the actual card's data is included on a fake magnetically swipe card. The phony card may be employed to make transactions and is completely functioning.
- Lost and Stolen card fraud: In the event that Fraudsters may obtain the card and use it to make purchases if the actual cardholder loses it. It is challenging to do this through a machine since a PIN is required, but the fraudster finds online transactions to be rather easy.
- Card ID theft: This fraud and application fraud are comparable. When someone commits identity theft, they get the initial version card's information in order to use it or create a new account. The most difficult kind of scam to identify is this one.

Fraud Patterns and Behavioral Characteristics

The main fraud patterns and behavioral attributes have been identified in contemporary financial and digital ecosystems. To make the understanding clearer, the particular details and examples are provided below.

- Credit card number generators: Fraudsters are able to use programs that exploit the Luhn algorithm to generate valid card numbers or stolen databases, making them able to engage in unauthorized transactions.[12]
- Keyloggers and sniffers: Naughty programs obtain keystroke and network information to steal credit card information. They are distributed in infected downloads, spam messages, or misleading links.
- Site cloning, spyware, and fake merchants: Scammers will clone banking websites or make counterfeit online shops, which will allow them to steal personal data by tricking people to fill in their personal details, and spyware will monitor their online traffic to steal information.
- Physical stolen card information: Cards that are stolen physically or skimming devices enable fraudsters to make unauthorized purchases over the internet or in stores.
- Credit card/card verification value 2 (CC/CVV2) black-market purchases: With acquired credit card numbers and secure code passwords, fraudsters purchase them on black-market websites to conduct a fraudulent online transaction without the technical knowledge.

Key Challenges in Fraud Detection

Real-time fraud detection presents several unique challenges:

- High volume and velocity of data: Modern systems must process thousands of transactions per second, requiring scalable and low-latency solutions.
- Imbalanced data: Fraudulent transactions typically represent a small fraction of total transactions, making it difficult to train models that can detect them without overfitting.[13]
- Evolving fraud tactics: Fraudsters continuously adapt their methods, necessitating detection systems that can quickly learn and adjust.
- False positives: Excessive false alerts can frustrate users and degrade customer experience, while false negatives result in actual financial loss.[14]
- Data privacy and security: Real-time systems must ensure the confidentiality and integrity of sensitive user data, often in compliance with regulations like GDPR or CCPA.[15]

Overcoming these challenges requires a combination of advanced analytics, robust infrastructure, and intelligent algorithms – a role ideally suited for ML.

ML AND DL APPROACHES IN FRAUD DETECTION

This section explores how ML and DL techniques enhance fraud detection by identifying hidden patterns, anomalies, and suspicious behaviors within transactional data. It reviews commonly used algorithms, compares their effectiveness, and highlights how advanced neural networks improve real-time detection accuracy, scalability, and adaptability against evolving fraud strategies.

ML Models for Fraud Detection

Machine learning algorithms use the cognitive abilities of data-driven decision making in order to detect intricate patterns of fraudulent activities.

- Decision trees: Decision trees stand out as a prominent supervised learning algorithm, primarily utilized in classification scenarios. This algorithm is adaptable to both categorical and continuous input output variables.[16] The fundamental principle involves partitioning the dataset into two or more homogeneous subsets, guided by the most significant attributes or independent variables, with the aim of creating distinct groups.
- Naive Bayes (NB): NB classifiers use probabilistic classifiers that rely on Bayes conditional probability to categorize data into their most likely classes. This method is often used in the identification and prevention of fraudulent activities. The classifiers are appealing because to their efficacy and interpretability, especially when working with input data that has a high level of dimensionality.[17] Their efficacy in intricate decision-making is heightened as they facilitate the integration of expert knowledge into ambiguous statements. The presumption of conditional independence among the features in the dataset, however, may significantly diminish their predictive efficacy. When confronted with duplicate attributes, this assumption often results in reduced precision.
- Logistic regression: There are more and more statistical models that discriminate data mining functions such as study, regression analysis, and multiple logistic logic.[18] Logistic regression (LR) is a set of predictive variables that are valuable to predicting the presence or deficiency of attribute or outcome. This is parallel to linear regression model, but it is suite for model with reliant on variable dichotomies.

DL Approaches for Fraud detection

DL approaches for credit card fraud detection (CCFD) leverage neural networks to identify complex, hidden patterns in transaction data, enabling more accurate, real-time detection of fraudulent activities compared to traditional methods.

- Artificial neural network (ANN): ANN is most influential classifiers with different characteristics among hidden patterns. ANN functions similarly to the human brain. The first layer is the input layer and the last layer is output layer.[19] It may have either any number of hidden layers. If neural networks have more hidden layer of stability, it is intensive learning. Each layer has dissimilar neurons and every neuron is associated with heavier edges.[20] Every neuron of output has its private unit of action. This function is named the activation function. E.g., various beginning functions are used: Linear function, step function, threshold function, sigmoid function, and so on. There is commonly applied function is the public sigmoid function.
- Convolution neural network (CNN): CNN is a measure of intensive education. The feature map represents the hidden layer within the mapping. Each feature map represents a feature. The feature map in the compressing neurons of the process is called convolution. The feature of the sub-sample reduces the map parameters. The fully connected layer is the same neural network.
- Long short-term memory (LSTM) networks: LSTMs are a special type of recurrent neural network (RNN) designed to learn long-range dependencies in sequential data. LSTMs are highly effective in fraud detection tasks that involve identifying fraudulent sequences of transactions over time. They are capable of handling long-term dependencies in time-series data. These networks are less prone to vanishing gradient issues, making them more reliable in complex sequence modeling. However, these networks are computationally expensive and can struggle with very large and complex datasets without proper tuning.

Table 1 describes the ML and DL models comparison from the CCFD.

Key Datasets for Credit Card Fraud

The datasets that are commonly utilized in CCFD studies include the following: real or simulated transaction records that allow for testing ML and DL models in a useful manner.

- ULB CCFD dataset: This is a dataset of 284,807 European transactions containing

Table 1: Comparison table of models for credit card fraud detection

Model	Strengths	Limitations	Applications in fraud detection
Decision Trees	Easy to interpret and visualize, handles both categorical and numerical data, and offers fast training and classification.	Prone to overfitting and sensitive to small variations in the dataset.	Quick rule-based fraud detection and baseline classification of simple fraud patterns.
Naïve Bayes	Efficient with high-dimensional data, simple to implement, computationally fast, and allows integration of expert probabilistic knowledge.	Assumes independence among features, which can reduce accuracy, and performs poorly when attributes are highly correlated.	Real-time fraud prediction and early detection using probabilistic patterns in transactions.
Logistic Regression	Simple, interpretable, works well for linearly separable data, and offers fast computation.	Struggles with complex non-linear patterns and relies heavily on effective feature engineering.	Binary fraud classification and benchmarking other models for transaction risk.
Artificial Neural Networks	Able to learn complex non-linear relationships and hidden patterns, flexible in architecture, and effective with large datasets.	Requires large amounts of training data, can overfit without regularization, and is less interpretable than classical models.	Identifying hidden or subtle fraud patterns and modeling non-linear transaction behaviors.
Convolutional Neural Networks	Automatically extracts relevant features, effective in structured pattern recognition, and can capture spatial correlations when data is transformed appropriately.	Not naturally designed for tabular transaction data unless represented as matrices or images, and involves high computational cost.	Detecting patterns in transformed transaction data, e.g., feature maps or embeddings.
Long short-term memory Networks	Captures long-term dependencies in sequential data, handles time-series patterns effectively, and avoids vanishing gradient issues seen in traditional recurrent neural networks.	Computationally expensive, memory-intensive, and can struggle with very large or complex datasets without optimization.	Detecting sequential fraud patterns over time and modeling evolving customer behavior.

Table 2: Comparative review of machine learning and deep learning approaches for credit card fraud detection (CCFD)

References	Study on	Approach	Key findings	Challenges/ limitations	Future directions
Gaav *et al.* (2025)	Systematic mapping review of 40 studies on CCFD	PRISMA 2020-guided review of ML/DL methods, datasets, optimization strategies	SL models (RF, DT, SVM, XGBoost) performed strongly; DL models (CNN, LSTM) effective for high-dimensional data; ensembles improved accuracy	Heavy reliance on ECCT 2013 dataset; inconsistent use of optimization strategies; accuracy overused as metric; low interpretability of complex models	Cross-dataset evaluation; standardized metrics (recall, F1, MCC, AUPRC); federated learning; explainable AI; self-supervised learning
Dastidar *et al.* (2024)	Survey on online fraud detection directions	Taxonomy of domain, focus on ML methods and GANs for data generation	Identified key research directions (imbalance handling, evolving behavior, context learning); GANs proposed for synthetic data generation	Lack of high-quality datasets; imbalance and evolving fraud patterns persist	Develop data generation frameworks (GANs, VAEs); benchmark fraud-specific datasets; adaptive fraud detection with evolving behavior
Mienye *et al.* (2024)	DL-based models for CCFD	Review of CNN, RNN, LSTM, gated recurrent unit architectures	DL architectures robust for fraud detection; comparative performance across DL models	Class imbalance; training complexity; lack of practical deployment evaluation	Explore hybrid DL models; improved training with imbalance-aware techniques; better evaluation metrics; deployment-focused research
Sulaiman, *et al.* (2024)	Overview of recent ML/DL for credit card fraud	Literature review addressing imbalance, concept drift, verification latency	Highlights ML/DL effectiveness in mitigating major fraud detection issues	Persistent issues of imbalance, concept drift, and delayed verification; real-time detection remains difficult	Develop adaptive models for concept drift; real-time detection frameworks; scalable solutions for latency
Btoush *et al.* (2023)	Review of ML/ DL approaches for credit card cyber fraud	Synthesized 181 studies (2019–2021)	ML/DL increasingly adopted; comprehensive comparison of techniques; identified gaps in performance	Existing models resource-intensive, time-consuming, and limited generalization	Develop lightweight, scalable, and real-world deployable models; standardized benchmarks; industry–academia collaboration
Bin Sulaiman *et al.* (2022)	Comparative analysis of ML techniques with a focus on confidentiality	Proposed hybrid ANN + federated learning solution	Hybrid + FL improves accuracy while ensuring privacy	Privacy-preserving approaches still limited; computational complexity; lack of large-scale validation	Enhance federated learning-based fraud detection; privacy-preserving DL models; scalability testing

LSTM: Long short-term memory, GAN: Generative adversarial network, CNN: Convolution neural network, CCFD: Credit card fraud detection, GANs: Generative adversarial network, ANN: Artificial neural network, ML: Machine learning, DL: Deep learning, RF: Random forest: DT: Decision tree: MCC: Matthews correlation coefficient, AUPRC: Area under the precision-recall curve, VAEs: Variational autoencoders

0.172% fraud, and using features transformed by PCA (V1-V 28). It has been regarded as one of the popular benchmarks of ML-based fraud detection.[21]

- PaySim mobile money Transaction Dataset: PaySim is a simulator of mobile financial transactions and has approximately 6 million transactions.[22] It simulates realistic fraud behavior, including cash-out and transfer fraud, in terms of synthetic yet very realistic transaction patterns.
- IEEE-CIS fraud detection dataset: This is a big dataset consisting of 590,540 transactions that have device, identity, and network metadata.[21] It is very appropriate in detail DL models because it has a great diversity of features.
- BankSim synthetic banking dataset: BankSim is an agent-based simulation model, which is designed to simulate realistic behavior of card transactions. It consists of both dishonest and un-dishonest operations,[23] and it could be helpful in assessing supervised and not supervised fraud detection.

FRAUD PREVENTION, LIMITATIONS, AND EMERGING TRENDS

The prevention activity is aimed at detecting abnormal behavior, reinforcing verification, and data integrity of transactions. Nevertheless, the problems of uneven data distribution, the continuously evolving structure of the fraud, inadequate visibility of the decisions, and the necessity to process them in a short period of time remain. The new trends are expected to increase the precision, credibility, cooperation, and general stability in fraud detection.

Fraud Prevention Techniques

Discusses ways in which suspicious activity can be identified, and the security of credit card transactions can be maintained, which are listed below:

- Real-time transaction monitoring is an underlying component of fraud prevention and enables ML and DL models to analyze user behavior, spending patterns, geolocation consistency, and device fingerprints on a continuous basis.[24,25] Real-time detection will mitigate loss of money and avoid mounting fraudulent transactions in interlinked accounts.
- Adaptive and behavior-based modeling is important as they learn the habits of each customer with time. In case a transaction significantly deviates with what historical behavior has shown, the system alerts the human to review it, or provides automated responses to challenge like OTP verification. Such customization highly increases the accuracy of fraud prevention measures.
- The inclusion of anomaly detection systems enhances the resistance to fraud by determining the transactions that do not conform to the normal statistical profiles, even when they are not found to correspond to known fraud signatures.[26] It particularly aids in identifying new or emerging fraudulent schemes that cannot be identified by the supervised classifiers.
- Strong data validation and integrity checks can also be used to avoid spoofed or tampered inputs into the system. To have reliable model predictions, it is critical to make sure that transaction metadata such as IP address, device identifiers, timestamps, and merchant identifiers are not subject to manipulation.
- Multi-factor authentication and biometric authentication, and tokenization are also used as an extra security layer. The use of ML-based risk scoring, together with these approaches, makes sure that payment transactions where risk is high are heavily verified, and low-risk payment transactions go on a seamless path.[27]

Limitations

Indicates the most critical issues and limitations that influence the accuracy and reliability of the fraud detection mechanisms below:

- Class imbalance problems: Fraud is vastly underrepresented relative to legitimate transactions, and models can have a hard time learning patterns of minority cases and thus fail to detect them.
- Fraud changing tactics: Fraudsters continuously evolve their tactics, and this has led to models specifically trained on historical data becoming irrelevant unless they are updated regularly.
- Absence of model transparency: It is common with most ML and, in particular, DL models to be black boxes, which restricts institutions to be able to justify or explain to the government and clients fraud decisions.

- Live processing limits: Fraud detection should occur in milliseconds, and sophisticated models cannot work effectively in high-volume transaction systems.

Emerging Trends

Publicizes innovation and future trends to improve the efficiency and durability of fraud detection.

- Graph-based and relationship-aware models: New systems are based on the use of the graph neural networks (GNNs) to detect and analyze the relationship among cards, devices, merchants, and users to enhance the detection of organized fraud networks and linked suspicious activity.[7]
- Explainable AI (XAI) implementation: Banks are implementing XAI systems such as SHapley Additive exPlanations (SHAP) and local interpretable model-agnostic explanations (LIME) to give more straightforward explanations behind the choices of fraud, to comply with regulatory demands, and enhance consumer confidence with automated systems.
- Hybrid detection frameworks: Combination of the supervised models and unsupervised anomaly detection is also on the rise. These hybrid systems not only pick up the old trends of fraud but also the odd tendencies never witnessed before.
- Federated learning approaches: Institutions are beginning to collaborate through federated learning,[28] which enables them to train common fraud models without exposing sensitive customer data and to increase the accuracy without impacting privacy.

LITERATURE REVIEW

The existing literature on CCFD indicates the development of ML and DL approaches. Models are effective, but problems such as the problem of class imbalance, problem of bias of the dataset, the problem of scalability, interpretability, and privacy are still research challenges illustrate in Table 2.

Gaav *et al.* (2025) emphasize the fact that CCFD remains a critical research topic because fraud is a complex phenomenon. They are a systematic mapping review (in the framework of PRISMA 2020 guidelines) of 40 publications, with a specific emphasis on methodologies, ML methods, and metrics of validation. Random forest and support vector machine (SVM) were also supervised learning models that performed well; DL systems were also accurate in capturing complex trends in fraud, but they had a problem with class imbalance. The use of the Ensemble Classifier using Clustering and Trees (ECCT) 2013 data restricts external validity. Recall was enhanced by optimization policies, but evaluation measures were disproportionately used. Future studies ought to focus on the cross-dataset assessments and new paradigms to improve fraud-detection systems.[29]

Dastidar *et al.* (2024) highlight the rise in online payment fraud, resulting in significant financial losses. As payment providers implement preventive measures, fraudsters adapt their tactics, necessitating advanced fraud detection tools. With millions of daily transactions, relying solely on human investigation is impractical, prompting research into data-driven and ML methods. This work reviews recent advancements in online fraud detection, addressing challenges like data skewness and evolving behaviors. The authors develop a taxonomy of research directions and identify gaps, particularly the scarcity of high-quality credit card data. They propose a data generation framework using generative adversarial networks to aid future research.[7]

Mienye *et al.* (2024), study reviews the recent DL-based literature and presents a concise description and performance comparison of the widely used DL techniques, including CNN, simple RNN, LSTM, and gated recurrent unit. In addition, an attempt is made to discuss suitable performance metrics, common challenges encountered when training credit card fraud models using DL architectures, and potential solutions, which are lacking in previous studies and would benefit DL researchers and practitioners. Meanwhile, the experimental results and analysis using a real-world dataset indicate the robustness of the DL architectures in CCFD.[30]

Sulaiman, *et al.* (2024) address the growing problem of credit card fraud in association with the development of electronic payment systems and high-tech methods of fraud. Financial institutions have turned to finding technological solutions to add to the security and privacy of users. This review discusses the recent studies on how to identify fraudulent transactions, how to overcome the difficulties associated with balancing the classes, concept drift, and verification latency using ML and DL models. It seeks to educate both academic and industrial researchers, which will facilitate the creation of effective fraud detection mechanisms to protect credit card deals against misuse.[31]

Btoush *et al.* (2023) emphasize that there is an imperative to boost cybersecurity in the banking industry as cyberattacks, especially credit card fraud, have increased. Conventional methods of detection, for example, anomaly detection and rule-based methods are usually inefficient and inaccurate. The paper highlights the increased relevance of ML, and DL methods in fighting these problems. It conducts the review of 181 research articles published in 2019–2021, offering the perspectives on the effective methods of CCFD. The review detects the current issues and gaps, and provides suggestions of future research to assist not only scholars but also the banking industry formulate innovative solutions.[32]

Bin Sulaiman *et al.* (2022), despite the ease of online business and e-payment systems, the sheer popularity of credit cards has spawned more fraud. They state the significance of ML techniques in preventing and detecting fraud through the analysis of the customer data. Their study entails a comparative investigation on the ML in CCFD and data confidentiality. They suggest a hybrid method that employs ANN in a federated learning system, which has been found to be effective in both obtaining higher accuracy in CCFD but preserving privacy.[33]

Table 1 presents the comparison of the selected studies on ML methods of fraud detection and defines their focus, approaches, findings, limitations, and directions.

Table 1: Comparative Analysis of Research Gaps in Machine Learning Approaches for CCFD of its entities. Deeply, it is an environment that consists of a virtual and a physical machine. Each machine (model) is represented as a simulation, a mirror, or a twin of the other. Hence, the digital twin can list the life cycle of the physical entity, which can be a human, an object, or a process. Each digital twin is connected to its counterpart by a unique key; therefore, a relationship between two entities can be established. A digital twin is a partition of a cyber-physical system, which is a set of physical systems connected to virtual cyberspace through the network.[11] The communication between a physical entity and its digital twin can be represented directly by physical connections or indirectly through a cloud system. Furthermore, it can be a seamless connection and continuous data exchange.[26]

CONCLUSION AND FUTURE WORK

The detection of fraudulent activities in payment systems remains a critical and evolving challenge due to the adaptive strategies employed by fraudsters. Advanced ML and DL techniques have demonstrated significant potential in addressing this issue, offering scalable, automated, and adaptive solutions for real-time fraud detection. Classical models such as decision trees, logistic regression, and Naïve Bayes provide interpretability and computational efficiency, while neural networks, CNNs, and LSTM architectures capture complex non-linear and sequential patterns that are often undetectable using traditional methods. Integration of these approaches allows for adaptive monitoring, anomaly detection, and predictive modeling, reducing false positives and enhancing transactional security. Nevertheless, persistent challenges include class imbalance, evolving fraud patterns, model interpretability, latency in real-time processing, and privacy concerns. Future research should focus on developing hybrid frameworks that combine supervised and unsupervised approaches, adopting explainable AI for transparency and regulatory compliance, and implementing federated learning for privacy-preserving, collaborative model training across institutions. In addition, cross-dataset validation, scalable deployment strategies, and creation of benchmark datasets are crucial for developing robust and generalizable detection systems. Addressing these challenges will enable financial institutions to secure digital transactions, protect consumers, and maintain trust in the increasingly complex and interconnected financial ecosystem.

REFERENCES

1. Bian C. Credit card fraud detection: Machine learning and deep learning advances, challenges, and future directions. ITM Web Conf 2025;78:02023.
2. Prajapati V. Enhancing threat intelligence and cyber defense through big data analytics: A review study. J Glob Res Math Arch 2025;12:1-6.
3. Bahnsen AC, Aouada D, Stojanovic A, Ottersten B. Feature engineering strategies for credit card fraud

detection. Expert Syst Appl 2016;51:134-42.

4. Gupta S, Sati V. Design and analysis of advanced machine learning methods for financial fraud identification in credit card activities. J Glob Res Multidiscip Stud 2025;1:8-16.
5. Soni P, Kumar M. Review on Credit Card Fraud Detection Techniques. In: Proceedings 2022 Fifth International Conference on Computational Intelligence and Communication Technologies (CCICT). Vol. 45. New York: IEEE; 2022. p. 520-5.
6. Thakkar KB, Kapadia HP. The Roadmap to Digital Transformation in Banking: Advancing Credit Card Fraud Detection with Hybrid Deep Learning Model. In: 2025 2nd International Conference on Trends in Engineering Systems and Technologies (ICTEST). IEEE; 2025. p. 1-6.
7. Dastidar KG, Caelen O, Granitzer M. Machine learning methods for credit card fraud detection: A survey. IEEE Access 2024;11:158939-65.
8. Majumder RQ. A review of anomaly identification in finance frauds using machine learning systems. Int J Adv Res Sci Commun Technol 2025;5:101-10.
9. Kurakula SR. The role of AI in transforming enterprise systems architecture for financial services modernization. J Comput Sci Technol Stud 2025;7: 181-6.
10. Adebayo OS, Favour-Bethy TA, Otasowie O, Okunola OA. Comparative review of credit card fraud detection using machine learning and concept drift techniques. Int J Comput Sci Mob Comput 2023;12: 24-48.
11. Wawge SJ. A survey on the identification of credit card fraud using machine learning with precision, performance, and challenges. Int J Innov Sci Res Technol 2025;10:3345-52.
12. Sethi N, Gera A. A revived survey of various credit card fraud detection techniques. Int J Comput Sci Mob Comput 2014;3:780-91.
13. Manoharan G, Dharmaraj A, Sheela SC, Naidu K, Chavva M, Chaudhary JK. "Machine Learning-Based Real-Time Fraud Detection in Financial Transactions," in 2024 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI), IEEE, May 2024, pp. 1–6. doi: 10.1109/ACCAI61061.2024.10602350.
14. Shah SB. Advancing Financial Security with Scalable AI: Explainable Machine Learning Models for Transaction Fraud Detection. In: 2025 4th International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE). IEEE; 2025. p. 1-7.
15. Verma V. Security compliance and risk management in AI-driven financial transactions. Int J Eng Sci Math 2023;12:107-21.
16. Sangit PN, Sangam S. The role of deep learning in credit card fraud detection: A state-of-the-art review. Cureus J Comput Sci 2025;2:1-9.
17. Sam U, Moses G, Olajide T. Credit Card Fraud Detection using Machine Learning Algorithms [Preprint]; 2023.
18. Thangavel S, Srinivasan S, Naga SB, Narukulla K. Distributed machine learning for big data analytics: Challenges, architectures, and optimizations. Int J Artif Intell Data Sci Mach Learn 2023;4:18-30.
19. Dattangire R, Vaidya R, Biradar D, Joon A. Exploring the Tangible Impact of Artificial Intelligence and Machine Learning: Bridging the Gap between Hype and Reality. In: 2024 1st International Conference on Advanced Computing and Emerging Technologies (ACET); 2024. p. 1-6.
20. Goyal R, Manjhvar AK. Review on credit card fraud detection using data mining classification techniques and machine learning algorithms. IJRAR Int J Res Anal Rev 2020;7:972-5.
21. Sorournejad S, Zojaji Z, Atani RE, Monadjemi AH. A Survey of Credit Card Fraud Detection Techniques: Data and Technique Oriented Perspective. New York: Academic Publishing; 2016. p. 1-26. Available from: https://arxiv.org/abs/1611.06439
22. Malali N. Exploring Artificial Intelligence Models for Early Warning Systems with Systemic Risk Analysis in Finance. In: 2025 International Conference on Advanced Computing Technologies (ICoACT). IEEE; 2025. p. 1-6.
23. Patel D. Enhancing banking security: A blockchain and machine learning-based fraud prevention model. Int J Curr Eng Technol 2023;13:576-83.
24. Kali H. Optimizing credit card fraud transactions identification and classification in banking industry using machine learning algorithms. Int J Recent Technol Sci Manag 2024;9:85-96.
25. Alraddadi AS. A survey and a credit card fraud detection and prevention model using the decision tree algorithm. Eng Technol Appl Sci Res 2023;13:11505-10.
26. Balagolla EM, Fernando WP, Rathnayake RM, Wijesekera MJ, Senarathne AN, Abeywardhana KY. Credit Card Fraud Prevention using Blockchain. In: 2021 6th International Conference for Convergence in Technology (I2CT); 2021. p. 1-8.
27. Prajapati N. The role of machine learning in big data analytics: Tools, techniques, and applications. ESP J Eng Technol Adv 2025;5:16-22.
28. Ande BR. Federated learning and explainable AI for decentralized fraud detection in financial systems. J Inf Syst Eng Manag 2025;10:48-56.
29. Gaav TA, Adoga HU, Moses T. Recent advances in credit card fraud detection: An analytical review of frameworks, methodologies, datasets, and challenges. J Futur Artif Intell Technol 2025;2:343-69.
30. Mienye ID, Jere N. Deep learning for credit card fraud detection: A Review of algorithms, challenges, and solutions. IEEE Access 2024;12:96893-910.
31. Sulaiman SS, Nadher I, Hameed SM. Credit card fraud detection challenges and solutions: A review. Iraqi J Sci 2024;65:2287-303.
32. Btoush EA, Zhou X, Gururajan R, Chan KC, Genrich R, Sankaran P. A systematic review of literature on credit card cyber fraud detection using machine and deep learning. PeerJ Comput Sci 2023;9:e1278.
33. Bin Sulaiman R, Schetinin V, Sant P. Review of machine learning approach on credit card fraud detection. Hum Centric Intell Syst 2022;2:55-68.