IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 1, May 2026
Impact Factor: 8.2

Fraud Detection in Online Transactions using Machine Learning

Sujata M. Sanap[1], Prof. Trupti Bhase[2], Prof. Sujata Salunkhe[3] Prof . Nanda S. Kulkarni[4]
Department of Computer Engineering [1,2,3,4]
Siddhant College of Engineering, Pune, Maharashtra, India
sujata.sanap2323@gmail.com

Abstract: *The Fraud Payment Detection App is an intelligent digsital transaction security system developed to detect suspicious and fraudulent payment activities during online transactions. The application is built using Java/XML for the Android front-end, Firebase for real-time backend storage and synchronization, and Razorpay for secure payment gateway integration. Unlike traditional payment applications that only record whether a transaction succeeds or fails, this system adds an advanced fraud monitoring layer that evaluates each payment in real time before final approval.*

The app supports product-based checkout functionality, where users can select from available online products and complete payments through Razorpay. During each transaction, the system captures and stores important payment metadata such as order ID, payment ID, transaction amount, payment mode, timestamp, retry attempts, and payment status. In addition to this, several fraud-related indicators are monitored, including repeated failed payment attempts, abnormal transaction amounts, IP address mismatch, device fingerprint mismatch, unusual login timing, frequency of payments, and sudden location drift.

The core strength of the proposed system lies in its hybrid fraud detection engine, which combines rule-based analysis, machine learning prediction, and behavioral analytics. The rule engine checks predefined suspicious conditions, the machine learning model estimates fraud probability based on historical transaction patterns, and behavioral analytics compares current activity with the normal usage pattern of the user. Based on the calculated fraud risk score, the transaction is classified as safe, suspicious, or fraudulent. The admin dashboard provides real-time monitoring of total transactions, success and failure rates, suspicious payments, fraud alerts, and trend analytics through graphs and reports. This system offers a smart, scalable, and secure solution for preventing online payment fraud and improving trust in digital payment platforms.

Keywords: Smart city, Fraud Payment Detection, Online Transaction Security, Java/XML, Firebase, Razorpay, Machine Learning, Rule-Based Detection, Behavioral Analytics, Fraud Risk Score, Android Application, Suspicious Transaction Monitoring, Payment Security System

INTRODUCTION

With the rapid growth of digital payments, online shopping, mobile wallets, and UPI-based transactions, the risk of payment fraud has also increased significantly. People now perform financial transactions through mobile applications and online platforms every day, making digital payment systems a critical part of modern life. Although payment gateways such as Razorpay provide secure transaction processing, many applications still depend only on basic payment confirmation mechanisms and do not include intelligent fraud analysis before or during the payment process. As a result, suspicious payment attempts, repeated failed transactions, unusual user behavior, and unauthorized access patterns may go unnoticed until financial damage has already occurred.

The Fraud Payment Detection App is designed to solve this problem by introducing an intelligent fraud monitoring and analysis layer into the digital payment workflow. This project is developed using Java/XML for the Android

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 1, May 2026
Impact Factor: 8.2

application interface, Firebase for backend data storage and real-time synchronization, and Razorpay for payment gateway integration. The system is not limited to simply recording transaction status such as success or failure, but goes further by analyzing multiple transaction-related parameters in real time to identify whether a payment is safe, suspicious, or potentially fraudulent.

In this application, users can browse available online products, add them for checkout, and complete payment through Razorpay. During the payment process, the system captures important metadata such as transaction amount, payment mode, timestamp, payment retries, order ID, payment ID, and status. Along with this, the application also observes advanced fraud indicators such as IP address mismatch, device fingerprint mismatch, unusual login timing, repeated failed payment attempts, abnormal payment frequency, amount deviation from previous history, and sudden location changes. These parameters are stored in Firebase and become part of the fraud analysis process.

The most important feature of this project is its hybrid fraud detection engine. This engine combines three different approaches to improve fraud detection accuracy. The first is rule-based detection, where predefined fraud conditions are checked, such as too many failed attempts in a short period, unusually high transaction amounts, or inconsistent device and location details. The second is machine learning-based detection, where a model studies historical transaction patterns and generates a fraud risk score for the current payment. The third is behavioral analytics, where the system compares the present user activity with the normal behavior profile of that user to identify anomalies. By combining these approaches, the system becomes much more powerful than a traditional payment monitoring system.

The application also includes an admin dashboard that displays transaction records and fraud-related insights in a user-friendly format. Through the dashboard, the administrator can monitor total transactions, successful and failed payments, suspicious cases, fraud score trends, and alert notifications. Based on the risk score generated by the fraud engine, the system can automatically approve a safe payment, flag a suspicious payment for review, or block a highly risky transaction instantly. This makes the proposed system useful not only for payment processing but also for fraud prevention, transaction transparency, and digital trust building.

In today's environment, where online fraud techniques are becoming more advanced and dynamic, there is a strong need for smart systems that can analyze payment behavior in real time and respond quickly. The Fraud Payment Detection App is a practical attempt to build such a system using modern Android development tools, cloud backend support, payment gateway integration, and intelligent fraud detection techniques. The project aims to contribute toward safer digital payment ecosystems by reducing fraudulent transactions, improving security m.

II. LITERATURE REVIEW

• Almazroi and Ayub (2023) in their paper "Online Payment Fraud Detection Model Using Machine Learning Techniques" (published in IEEE Access) found that a hybrid model combining supervised learning with unsupervised anomaly detection improved online payment fraud detection accuracy while also reducing false positives compared with more conventional ML and deep learning baselines.

• Wang et al. (2023) in their paper "CAeSaR: An Online Payment Anti-Fraud Integration System With Decision Explainability" (published in IEEE Transactions on Engineering Management / IEEE Computer Society Digital Library) found that a modular anti-fraud integration framework with decision explainability can improve the practicality of data-driven anti-fraud engineering for online payment services, and the framework was validated in practice.

• Aurna et al. (2023) in their paper "Federated Learning-Based Credit Card Fraud Detection: Performance Analysis with Sampling Methods and Deep Learning Algorithms" (published in the 2023 IEEE International Conference on Cyber Security and Resilience) found that federated learning is a viable privacy-preserving approach for fraud detection, and that combining it with sampling methods and deep learning models can strengthen performance on highly imbalanced credit card datasets.

• Xie et al. (2023) in their paper "Time-Aware Attention-Based Gated Network for Credit Card Fraud Detection by Extracting Transactional Behaviors" (published in IEEE Transactions on Computational Social Systems) found that

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 1, May 2026 Impact Factor: 8.2

incorporating time-aware attention and gated modeling of transactional behavior improves fraud detection by capturing the temporal patterns hidden in users' payment histories.

• Zhu et al. (2024) in their paper "NUS: Noisy-Sample-Removed Undersampling Scheme for Imbalanced Classification and Application to Credit Card Fraud Detection" (published in IEEE Transactions on Computational Social Systems) found that handling fraud data imbalance by removing noisy samples before undersampling can improve classification robustness and make fraud detection models more reliable on skewed transaction data.

• Aurna et al. (2024) in their paper "FedFusion: Adaptive Model Fusion for Addressing Feature Discrepancies in Federated Credit Card Fraud Detection" (published in IEEE Access) found that adaptive model fusion helps federated fraud detection systems cope with feature discrepancies across institutions or clients, making collaborative fraud detection more practical in real-world distributed settings.

• Tang and Liu (2024) in their paper "A Credit Card Fraud Detection Algorithm Based on SDT and Federated Learning" (published in IEEE Access) found that combining a Structured Data Transformer (SDT) with federated learning helps address both distributed deployment challenges and complex transaction patterns, making the model better suited for modern digital payment environments.

III.PROBLEM DEFINITION AND SCOPE

1) Problem Statement:

Despite advancements in encryption, current digital payment infrastructures suffer from three critical "Structural Blind Spots":

- **Static Validation Flaw:** Traditional systems rely on "what the user knows" (CVV/OTP). If these are stolen via phishing, the gateway accepts the transaction as legitimate.
- **Contextual Blindness:** Gateways often ignore the "where" and "how" of a transaction. A payment initiated from a known fraudulent IP range or a "rooted" device is often treated the same as a secure one.
- **The Velocity Gap:** Humans cannot manually monitor the speed of bot-driven attacks. Automated "carding" attacks can attempt thousands of transactions in seconds, overwhelming standard merchant dashboards.
- **Verification Friction:** Excessive security often creates a "bad user experience" (false positives), leading to cart abandonment. There is a dire need for a system that is "Invisible yet Omnipresent."

2) Objectives:

The primary objective of this dissertation is to architect and deploy a multi-layered security application. Specifically:

- **To Develop a Hybrid Fraud Engine:** Integrate a Rule-Based Engine with Behavioral Analytics to assign a dynamic "Risk Score" to every transaction.
- **To Implement Device Fingerprinting:** Create a system to capture hardware-level metadata (Android ID, IMEI hashes, and Build Specs) to identify hardware-based fraud patterns.
- **To Synchronize Real-Time Backend Operations:** Utilize Firebase Cloud Functions and Firestore to ensure that data collection and analysis happen in <200ms, ensuring zero lag in the payment flow.
- **To Provide an Integrated Admin Analytics Dashboard:** Build a Java/XML interface that visualizes fraud trends, allowing merchants to "see" the invisible threats through heatmaps and trend lines.
- **To Ensure Gateway Integrity:** Seamlessly bridge the Fraud Engine with the Razorpay API to allow for "Conditional Checkout"—blocking the payment UI if the risk score exceeds a defined threshold.

3) Scope

The scope of this project is defined by its application in the Android and iOS ecosystems (via cross-platform backend logic):

- **In-Scope:** * Development of the Android Dashboard (Java/XML).
  - Creation of a "Product Checkout" simulation for testing.
  - Logic for IP-based geolocation and velocity checking.
  - Firebase backend orchestration.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 1, May 2026
Impact Factor: 8.2

- Out-of-Scope: * This project does not replace the bank's internal fraud systems but acts as a

Merchant-Side Shield.

Physical hardware security (e.g., NFC skimming at POS terminals) is not addressed; the focus is strictly on Online E-commerce Fraud

IV. RESEARCH METHODOLOGY

The methodology of the Fraud Payment Detection App is designed to monitor, analyze, and classify digital payment transactions in real time by combining payment gateway integration, cloud data storage, rule-based checking, behavioral monitoring, and machine learning-based fraud scoring. The complete system is organized into multiple phases so that every payment made through the application can be observed and evaluated before final action is taken. The proposed methodology ensures that suspicious transactions are not treated like normal successful payments and instead pass through an intelligent fraud analysis pipeline.

The first step in the methodology is the user transaction process. In this phase, the user opens the Android application developed using Java/XML, browses the available products, and selects an item for purchase. Once the user proceeds to checkout, the application sends the product and order details to the backend. The system then prepares the payment request and connects with the Razorpay payment gateway to initiate the transaction. Razorpay generates important transaction identifiers such as order ID, payment ID, payment status, timestamp, and payment mode, which are used for further monitoring.

The second step is the transaction data collection phase. During payment execution, the system captures not only basic payment information but also additional fraud-sensitive parameters. These include transaction amount, retry count, payment frequency, login timing, IP-related details, device identity, location variation, and previous transaction behavior. This information is stored in Firebase in real time. Firebase acts as the central backend database where all transaction logs, user payment history, suspicious activity indicators, and fraud analysis results are maintained for future comparison and live dashboard display.

The third step is the preprocessing and feature preparation phase. In this phase, the raw transaction data is converted into meaningful fraud analysis inputs. For example, the system compares the current transaction amount with the user's normal payment history, checks whether the current device matches the previously used device, verifies whether multiple failed attempts occurred in a short duration, and identifies whether a sudden change in payment behavior is present. These processed values are transformed into fraud indicators that are passed into the fraud detection engine.

The fourth step is the rule-based fraud analysis phase. This is the first level of fraud checking. In this stage, the system applies predefined logical rules to quickly detect obvious fraud situations. For instance, if a user attempts payment many times within a short period, if the transaction amount is much higher than normal, if the device fingerprint suddenly changes, or if the payment location is very different from past behavior, the system raises a suspicion level. Rule-based detection is useful because it gives immediate and explainable fraud alerts based on fixed conditions.

The fifth step is the machine learning fraud prediction phase. After rule-based evaluation, the transaction is passed to an ML model trained on historical payment patterns. The model studies combinations of different transaction features and generates a fraud risk score. This score indicates the likelihood that the payment may be genuine, suspicious, or fraudulent. Machine learning helps detect hidden fraud patterns that cannot always be captured through manually written rules. It strengthens the intelligence of the system by learning from previous transaction behavior and improving decision quality.

The sixth step is the behavioral analytics phase. In this step, the system compares the current transaction with the normal behavioral profile of the user. The profile may include usual transaction range, preferred payment method, common login time, device consistency, and location habits. If the current transaction strongly differs from this normal behavior, the system increases the fraud risk level. Behavioral analytics is important because even if a transaction technically looks valid, unusual user behavior can still indicate unauthorized access or malicious activity.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 1, May 2026 Impact Factor: 8.2

The seventh step is the fraud classification and decision phase. In this stage, the results from rule-based detection, machine learning prediction, and behavioral analytics are combined to produce a final fraud classification. Based on the calculated fraud score, the system marks the payment as one of three categories: safe, suspicious, or fraudulent. If the score is low, the transaction is approved. If the score is moderate, the payment is flagged for admin review. If the score is very high, the transaction is blocked instantly to prevent possible loss. This layered decision-making approach improves security and reduces false approvals.

The eighth step is the dashboard monitoring and alert generation phase. All transaction details and fraud results are displayed on the admin dashboard built with XML-based Android UI components. The dashboard shows total transactions, successful payments, failed payments, suspicious transactions, fraud trends, and alerts. Graphs and summary cards help the admin quickly understand payment patterns and identify risky activities. Real-time synchronization through Firebase ensures that any new suspicious payment is immediately reflected on the dashboard.

BLOCK DIAGRAM

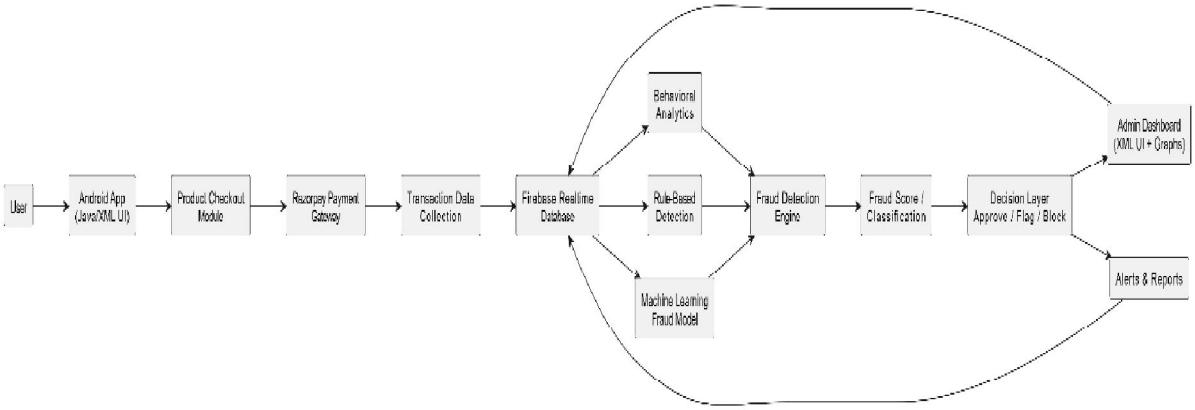

Fig. 4.1 Block Diagram of Proposed System.

This block diagram shows the working flow of the Fraud Payment Detection App. The user starts payment through the Android app, the transaction is processed by Razorpay, and all payment-related data is collected and stored in Firebase. Then, rule-based detection, machine learning, and behavioral analytics analyze the transaction. After that, the system generates a fraud score and classifies the payment. Finally, the decision layer approves, flags, or blocks the transaction, and the results are shown on the admin dashboard with alerts and reports.

V. RESULTS AND DISCUSSION

The Fraud Payment Detection App was developed and evaluated as an intelligent payment monitoring system capable of identifying normal, suspicious, and fraudulent transactions during online payment processing. The system successfully integrated Java/XML-based Android interfaces, Firebase real-time backend support, and Razorpay payment gateway functionality to create a complete digital payment environment with fraud analysis capability. The main objective of the project was to move beyond simple payment status tracking and introduce real-time fraud detection using transaction rules, user behaviour patterns, and risk-based analysis.

During testing, the application was able to perform product checkout, generate payment transaction records, store transaction metadata in Firebase, and display the details through the admin dashboard. The system effectively collected major fraud-related parameters such as payment amount, repeated payment attempts, timestamp variation, unusual location behaviour, device mismatch, and abnormal user activity. These inputs were then analyzed by the fraud

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 1, May 2026
Impact Factor: 8.2

detection engine, which classified transactions into safe, suspicious, or fraudulent categories based on the generated fraud score.

The results showed that the proposed system can successfully identify risky payment behaviour in a structured and understandable way. Transactions with normal behaviour patterns were approved, while unusual or abnormal transactions were either flagged for review or marked as potentially fraudulent. This proves that the combination of rule-based logic and behavioural monitoring can significantly improve payment security. The dashboard also helped in visualizing overall transaction trends, success and failure ratio, suspicious payment counts, and fraud alerts, which made the system more useful from an administrative and monitoring perspective.

From the discussion, it is clear that the project provides a practical and scalable approach for fraud prevention in digital payment applications. One of the biggest strengths of the system is that it does not wait for fraud to happen and then report it later. Instead, it attempts to identify fraud signals during the transaction process itself. This proactive approach can reduce financial loss, improve trust in online payments, and support better decision-making for administrators. The use of Firebase also made it easy to manage transaction history and synchronize data in real time.

Parameter	Observation
Product Checkout	Successfully completed through app
Razorpay Integration	Payment flow executed properly
Firebase Storage	Transaction records stored in real time
Rule-Based Detection	Suspicious conditions identified correctly
Behavioural Analysis	Unusual activity patterns detected
Fraud Classification	Payments marked as safe, suspicious, or fraudulent
Dashboard Monitoring	Alerts, graphs, and transaction logs displayed
Overall System Performance	Stable and effective for fraud monitoring

Table 1: Results Table

However, the effectiveness of the system depends on the quality of the fraud rules and the historical behaviour data available for comparison. In a real-world large-scale system, the machine learning model would require a properly trained fraud dataset to improve prediction accuracy. Similarly, behavioural analytics becomes stronger only after enough transaction history has been collected for each user. Even with these limitations, the project demonstrates that integrating fraud intelligence with a payment application can greatly improve the security and reliability of online transaction systems.

VI. CONCLUSION

This The Fraud Payment Detection App successfully demonstrates how a modern digital payment system can be enhanced with intelligent fraud monitoring and risk analysis features. The project was developed using Java/XML for the Android application interface, Firebase for real-time backend storage and synchronization, and Razorpay for secure payment processing. The system not only supports product checkout and transaction recording, but also adds an advanced fraud detection layer that monitors suspicious payment behaviour during the transaction process.

The proposed application proved effective in collecting important transaction details such as payment amount, order information, payment status, repeated attempts, device variation, location change, and other behavioural indicators. By combining rule-based checking, machine learning-based fraud scoring, and behavioural analytics, the system was able

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 1, May 2026 Impact Factor: 8.2

to classify transactions as safe, suspicious, or fraudulent. This makes the application more powerful than a regular payment app that only verifies whether a payment is completed or failed.

The project also provides an admin dashboard that helps in monitoring transaction records, suspicious payment alerts, fraud patterns, and system activity in real time. This improves transparency, supports faster decision-making, and helps reduce the chances of financial loss caused by unauthorized or risky transactions. The integration of Firebase further strengthens the system by enabling real-time data updates and structured transaction history management.

VII. FUTURE SCOPE

The Fraud Payment Detection App has strong potential for further enhancement and real-world deployment in advanced digital payment systems. In the future, the project can be improved by integrating a more powerful and fully trained machine learning or deep learning model using large-scale real transaction datasets. This would increase fraud prediction accuracy and help detect more complex fraud patterns that cannot be captured through simple rules alone.

The system can also be extended by adding stronger device fingerprinting, browser fingerprint analysis, and network-level verification for better identification of unauthorized users. Integration of geolocation intelligence, IP reputation services, and blacklist or whitelist mechanisms can further strengthen fraud risk assessment. Multi-factor authentication can also be introduced for high-risk transactions, where suspicious payments require OTP, biometric verification, or admin approval before completion.

Another important future enhancement is the use of adaptive and self-learning fraud engines. Such systems can continuously learn from new transaction history and update risk patterns automatically over time. This would make the fraud detection process smarter, faster, and more suitable for real-time commercial payment platforms.

The project can further be expanded into a complete web and mobile fraud analytics platform for banks, e-commerce systems, fintech applications, and online subscription services. Advanced dashboards with live charts, predictive trends, user-level fraud profiling, and automated alert notifications through email or SMS can also be added. Integration with cloud functions and secure backend APIs would make the system more scalable and production-ready.

REFERENCES

1] I. D. Mienye and N. Jere, “Deep Learning for Credit Card Fraud Detection: A Review of Algorithms, Challenges, and Solutions,” IEEE Access, vol. 12, pp. 96893–96910, 2024, doi: 10.1109/ACCESS.2024.3426955.

[2] A. A. Almazroi and N. Ayub, “Online Payment Fraud Detection Model Using Machine Learning Techniques,” IEEE Access, vol. 11, pp. 137188–137203, 2023, doi: 10.1109/ACCESS.2023.3339226.

[3] C. Wang, S. Chai, H. Zhu, and C. Jiang, “CAeSaR: An Online Payment Anti-Fraud Integration System With Decision Explainability,” IEEE Transactions on Dependable and Secure Computing, vol. 20, no. 3, pp. 2565–2577, 2023, doi: 10.1109/TDSC.2022.3186733.

[4] S. K. Hashemi, S. L. Mirtaheri, and S. Greco, “Fraud Detection in Banking Data by Machine Learning Techniques,” IEEE Access, vol. 11, pp. 3034–3043, 2023, doi: 10.1109/ACCESS.2022.3232287.

[5] I. D. Mienye and Y. Sun, “A Deep Learning Ensemble With Data Resampling for Credit Card Fraud Detection,” IEEE Access, vol. 11, pp. 30628–30638, 2023, doi: 10.1109/ACCESS.2023.3262020.

[6] E. Esenogho, I. D. Mienye, T. G. Swart, K. Aruleba, and G. Obaido, “A Neural Network Ensemble With Feature Engineering for Improved Credit Card Fraud Detection,” IEEE Access, vol. 10, pp. 16400–16407, 2022, doi: 10.1109/ACCESS.2022.3148298.

[7] F. K. Alarfaj, I. Malik, H. U. Khan, N. Almusallam, M. Ramzan, and M. Ahmed, “Credit Card Fraud Detection Using State-of-the-Art Machine Learning and Deep Learning Algorithms,” IEEE Access, vol. 10, pp. 39700–39715, 2022, doi: 10.1109/ACCESS.2022.3166891.

[8] Y. Xie, G. Liu, C. Yan, C. Jiang, and M. C. Zhou, “Time-Aware Attention-Based Gated Network for Credit Card Fraud Detection by Extracting Transactional Behaviors,” IEEE Transactions on Computational Social Systems, vol. 10, no. 3, pp. 1004–1016, 2023, doi: 10.1109/TCSS.2022.3158318.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 1, May 2026
Impact Factor: 8.2

[9] N. F. Aurna, M. D. Hossain, Y. Taenaka, and Y. Kadobayashi, "Federated Learning-Based Credit Card Fraud Detection: Performance Analysis with Sampling Methods and Deep Learning Algorithms," in Proc. 2023 IEEE International Conference on Cyber Security and Resilience (CSR), 2023, pp. 180–186, doi: 10.1109/CSR57506.2023.10224978.
[10] N. F. Aurna, M. D. Hossain, L. Khan, Y. Taenaka, and Y. Kadobayashi, "FedFusion: Adaptive Model Fusion for Addressing Feature Discrepancies in Federated Credit Card Fraud Detection," IEEE Access, vol. 12, pp. 136962–136978, 2024, doi: 10.1109/ACCESS.2024.3464333.
[11] Y. Tang and Z. Liu, "A Credit Card Fraud Detection Algorithm Based on SDT and Federated Learning," IEEE Access, vol. 12, pp. 182547–182560, 2024, doi: 10.1109/ACCESS.2024.3491175.
[12] H. Zhu, M. Zhou, Y. Xie, and A. Albeshri, "A Self-Adapting and Efficient Dandelion Algorithm and Its Application to Feature Selection for Credit Card Fraud Detection," IEEE/CAA Journal of Automatica Sinica, vol. 11, no. 2, pp. 377–390, 2024, doi: 10.1109/JAS.2023.124008.
[13] Y. Xie, M. C. Zhou, G. Liu, L. Wei, H. Zhu, and P. De Meo, "A Transactional-Behavior-Based Hierarchical Gated Network for Credit Card Fraud Detection," IEEE/CAA Journal of Automatica Sinica, vol. 12, no. 7, pp. 1489–1503, 2025, doi: 10.1109/JAS.2025.125243.
[14] E. Ileberi and Y. Sun, "A Hybrid Deep Learning Ensemble Model for Credit Card Fraud Detection," IEEE Access, vol. 12, pp. 175829–175838, 2024, doi: 10.1109/ACCESS.2024.3502542.
[15] T.-T.-H. Le, Y. Hwang, H. Kang, and H. Kim, "Robust Credit Card Fraud Detection Based on Efficient Kolmogorov-Arnold Network Models," IEEE Access, vol. 12, pp. 157006–157020, 2024, doi: 10.1109/ACCESS.2024.3485200.
[16] J. G. Almaraz-Rivera, J. A. Cantoral-Ceballos, J. F. Botero, F. J. Muñoz, and B. D. Martinez, "Hyphatia: A Card-Not-Present Fraud Detection System Based on Self-Supervised Tabular Learning," IEEE Open Journal of the Computer Society, vol. 6, pp. 812–821, 2025, doi: 10.1109/OJCS.2025.3570600.