IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.155177

AI-Based Cyber Fraud Detection System

Mr. Harikrishna[1], M Shreya Reddy[2], Manasa V[3], Kirti M Maracharaddi[4]

CSE Department, Ballari Institute of Technology & Management[1-4]

Abstract: The need for this project is to develop an AI-based system that is capable of identifying cyber fraud, credit card fraud, UPI fraud, and online payment fraud, among others. The proposed system would utilize machine learning techniques that analyze user behavior and transaction patterns with a view to identifying any anomaly and something that is suspect. Indeed, this system is expected to keep track of all fraud activities that occur instantly, hence all activity that contradicts the usual activity of a particular user might be identified by this system instantly. The system proposed involves monitoring all digital transaction aspects related to credit card payments, UPI, and all online transaction activity, among others. Moreover, this system has the capability of learning from data, hence its accuracy improves with time due to its behavioral and pattern recognition feature. The end result of this project is expected to be a quick, reliable, and accurate system that offers instant notifications that cut down losses and restrict all unauthorized transactions instantly, hence making digital money much more secure, and users can trust financial institutions more.

Keywords: Cyber Fraud, Real-Time Transaction Monitoring, Machine Learning, Anomaly Detection, Digital Payments.

1. INTRODUCTION

Although the pace of digital transformations is accelerating the ease of financial transactions, it has also created opportunities for cyber fraudsters. The next-generation fraudsters use sophisticated phishing links, account hacks, device impersonation, and UPI fraud. The conventional fraud protection technologies are rule-based and are incapable of recognizing novel or unseen fraud actions. As the fraud actions are becoming more sophisticated day by day, the developing field is already creating the requirement for the adaptive AI fraud protection technology for the intelligent recognition of user behaviors and the real-time detection of suspicious transactions. This paper aims to design an effective AI-based fraud protection technology for securing financial hazards and building trust among the users for the electronic payments environment.

1.1. OBJECTIVES

[1] To keep track of the online transaction process in real time, like the transaction involving a credit card, UPI, online payment, etc.
[2] To use machine learning algorithms for identifying unusual or suspicious activities based on transaction patterns.
[3] For user behavior analysis and anomaly identification through AI-based methods.
[4] To provide instant notifications and restrict any unauthorized and fraudulent activities.

1.2. EXISTING SYSTEM

The current fraud analysis techniques are primarily based on rule-centric approaches, which identify whether a transaction is legit or a potential fraud based on a set of predetermined rules. These systems have the capability to identify known patterns related to fraud but have limitations in detecting the evolving approaches adopted by fraudsters. These systems also have flaws related to high rates of false positives, wherein legit transactions are also identified as potential frauds. Furthermore, the current systems have no behavioral analysis capabilities and are unable to identify the evolving trends related to user behavior.

1.3. PROPOSED SYSTEM

The newly proposed AI system for fraud detection incorporates an intelligent framework that has the capability of learning from user behavior and detecting abnormalities indicative of fraud. Unlike conventional models that follow a rules-based mechanism for fraud detection, the new model utilizes machine learning algorithms that analyze past behaviors of financial transactions and categorize new transactions as being either legitimate or fraudulent. The model takes into consideration various factors like the amount, time, rate, location, device used, and type of merchant. When the model recognizes a potential threat, it triggers an instant notification on the user's end and has the ability to take preventive measures. The proposed system ensures improved accuracy of fraud detection with each new pattern identified.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.155177

1.4. SYSTEM FEATURES

[1] This system helps by constantly tracking digital payments made through UPI, credit cards, or web platforms.
[2] It detects aberrant or suspicious behaviors through the use of artificial intelligence and machine learning algorithms.
[3] It is able to automatically identify fraud patterns and high-risk behavior.
[4] It sends alerts on possible fraud transactions to avoid financial loss.

2. LITERATURE SURVEY

Recently, some studies carried out in India have helped to promote technological developments related to law, AI-assisted models, and case management mechanisms. A paper by Sharma and Kumar [1] reported a study related to credit card fraud detection employing machine learning models, where models consisting of Random Forest and XGBoost were analyzed. The paper reported that XGBoost outperformed others due to its ability to tackle imbalance datasets correctly, resulting in improved precision and identification of irregular spending patterns.Singh and Verma [2] analyzed deep learning techniques to detect fraud online payment services in real-time situations. In their paper, they analyzed the performance of LSTM networks; they found that these networks were capable of detecting irregular patterns in a series of online transactions to give instant notifications to avoid fraud situations.Nair and Mehta [3] analyzed UPI-based anomaly pattern recognition using unsupervised models such as One-Class SVM and K-Means. The authors found that these models were capable of identifying irregular patterns associated with user behavior, including improved fraud detection at early stages, especially when limited data related to fraud exists.Das and Banerjee [4] discussed a combined approach comprising statistical models as well as AI techniques to improvise fraud detection precision. In their paper, they showed that a combination of logistic regression and Random Forest algorithms ensured a significant reduction in false alarms along with improved irregular patterns of fraudulent cases.Patel and Ghosh [5] analyzed a fraud detection model using a federated learning technique, whereby banking institutions were found to be able to cooperate with each other without accessing others' private data and ideas. The authors mentioned that these models ensured data privacy at levels equivalent to models analyzed using centralized fraud detection mechanisms.Chen and Zhao [6] analyzed a study related to a fraud detection mechanism using an autoencoder technique, which was successful for irregular transaction patterns, particularly when working with large data sets. In this paper, they clarified that irregularities revealed with data from techniques related to autoencoders could perform better when a small amount of data related to fraud exists, which includes irregular transaction patterns associated with fraud cases.Kumar and Banerjee [7] analyzed a study using a GNN technique to identify fraud networks with a common relationship between accounts to detect mule accounts associated with fraud.In a paper, Iyer and Reddy [8] discussed various methods related to biometrics and devices with fraud prevention related to account takeover mechanisms. Their work demonstrated that incorporating behavioral characteristics like typing rhythm and device behaviors significantly improved resistance to imitation attacks.Additionally, Nair and Joshi [9] investigated handy explanations in AI like SHAP values and LIME. The objective was to improve interpretability in fraud models. The results demonstrated that using interpretative machine learning improved analysts' comprehension, promoting increased trust and decreased investigation time.Roy and Menon [10] offered a discussion on existing methods for protecting confidentiality in fraud models using differential and secure aggregation. It has been recognized through this development that a significant consideration in learning efficient fraud models is protecting users' confidentiality.

3. METHODOLOGY

The system adopts a structured way of end-to-end development involving the integration of data processing, machine learning, and real-time fraud analysis modules. This involves data acquisition, which involves transaction data from different sources, with each set of data consisting of various parameters for the transaction, including the amount transferred, time of the transaction, location, device ID, type of transaction, and user behavior. These raw data can have duplicates, some data may be missing, and some data may have inconsistencies. Hence, each data set undergoes intense processing for data cleaning. This involves data pre-processing steps, which include data normalization, elimination of outliers, data encoding for categorical variables, and derivation of Behavioral Features to make data in the best possible form to train machine learning models.The data sets, after being prepared, are split into training and testing data, so the system can learn the pattern from the data and test its performance on other data. Various machine learning models, including Logistic Regression, Random Forest, Support Vector Machines, and XGBoost, have also been applied in the system. Each of these models learns to identify transactions marked as fraud and normal in terms of their pattern and behavior. Feature importance analysis has also been applied to identify what parameters, such as unusual transfer amount, login time, and foreign device, influence fraud accuracy.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.155177

The trained model is then applied to a real-time detection scenario. During this process, the model is constantly observing incoming transactions and testing them using the ML model. When there is abnormal behavior, it identifies a particular transaction as high risk and sends an alarm. However, to ensure that it adapts to changes over time, there is continuous learning, whereby there is constant addition of fraud examples to be applied to retrain or update the model from time to time. In this way, it adapts to different approaches that cyber attackers may form over time. The whole process is facilitated by a backend engine developed using Python and ML libraries, while a simple GUI is utilized to provide visual representation for viewing alerts and flags of transactions in a real-time scenario.

The complete working model / Flowchart is shown in figure 1 and its use-case diagram is presented in figure 2.

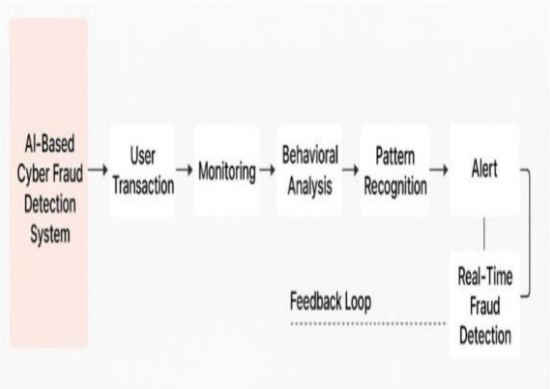

Fig 1. Working model of AI-Based Cyber Fraud Detection System

The process begins with making a digital, online transaction by the user, which could be UPI money transfer, online credit card payments, or other online transactions made by the user. Details of transactions done by the user are taken online, in real-time.

This data will be subjected to certain data handling processes, such as data cleansing, data normalization, encoding of categorical attributes, extraction of features, among others, to make it optimal for processing by machine learning algorithms. On analysis of the data processed using the machine learning models, anomalies in deviating user behavior may be identified.

On the basis of the prediction, the transaction is classified as an actual or fraud transaction. The actual transactions are processed, while the fraud transactions are flagged or blocked. In case of fraud prediction, the alert notification is sent instantly to the user and also to the system admin. The fraud instances are also stored and are used for self-training of the system on the basis of the newly identified fraud patterns.

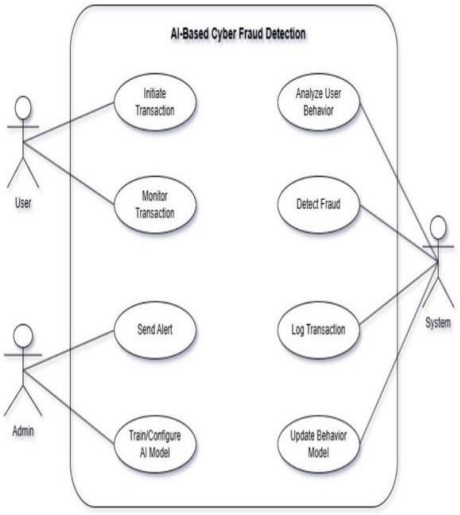

Fig 2. Use case Diagram

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.155177

Fig 2 above shows the use case diagram describing the relationship between various actors and the fraud detection system. The main actors who take part in this scenario are User and System Administrator.
The User is able to register, login into the system, perform online transactions, and receive fraud alerts. The system is always monitoring transactions, analyzing user behaviors using artificial intelligence, and automatically identifying any attempt of fraud.

Functions of the Administrator include the monitoring of fraud alerts, examining cases where fraud has been detected by the system or by users/modifications made to the machine learning model. The above diagram shows the automated process and how AI can be used as a means for little or even no human interference for accurate and safe fraud results.

4. RESULTS AND DISCUSSIONS

The various machine learning algorithms indicate that the developed system is highly efficient when compared to the precision and speed of the generated results for fraud detection. The Random Forest and XGBoost classifiers were very important for the precise detection of the small deformities existing in the transactional patterns. During the validation process, this system identified abnormalities such as: ‘sudden large money transfers,’ ‘login attempts from nfamiliar devices,’ and the start of the transactions during very unusual times. The entire process took only milliseconds to identify the abnormalities and thereby proved to be a real-time fraud prevention mechanism.Another important point to make is that the developed system has less False Positive results when compared to the traditional mechanisms that were initially used and were rule-driven. Unlike the previous mechanisms, where the legitimate transactions were identified as deformities by the system, the developed AI-driven model was highly stable and thereby made the precise identification of the deformities by analyzing the usage patterns and thereby hinted at the required deformities. This ensures that the users' trust levels are not affected and that there would not be any interruptions to the users' transaction processes. This proved to be highly efficient for the identification of new deformities for the fraud behaviors and hence clarified the benefits of the ‘Anomaly Detection and Adaptive Learning.’ The usability of the developed system related to the warning mechanism and the ‘Transaction Monitoring Interface' developed for the users provided a simple and straightforward view to the users regarding the fraudulent activities. The users could clearly understand the reason for the warnings and thereby make use of the backend analysis also for further clarification. Since the developed system continuously learns and updates the new information for the algorithm retraining and thereby the system's efficiencies were improved when the entire transaction history was made to pass through the system. This retraining mechanism enables the system to be up to date and not vulnerable to new ‘cyber threats.’ The results clearly indicate the capabilities and practicability of the proposed ‘AI-driven Fraud Detection System' that significantly decreased financial risks in the ‘Digital Payment World’.

4.1. OUTPUTS

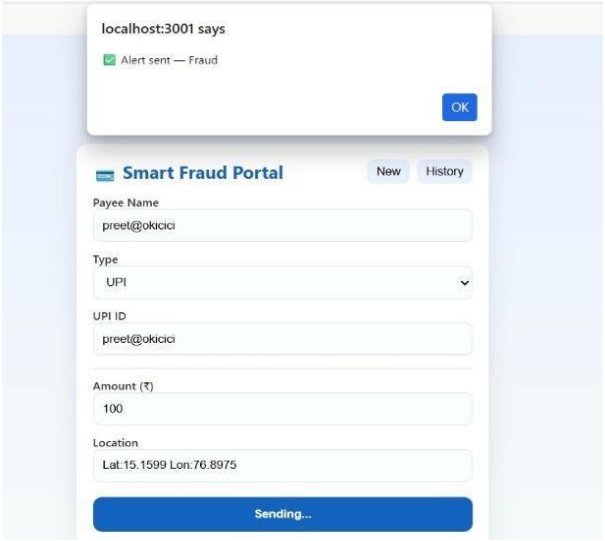

Fig 3. UPI fraud alert generation

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.155177

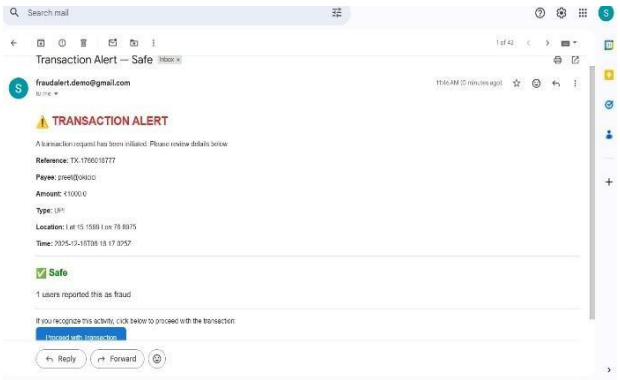

Fig 4. Email alert for safe transaction verification

Fig 5. Payment completion confirmation screen

Fig 6. Successful payment after user confirmation

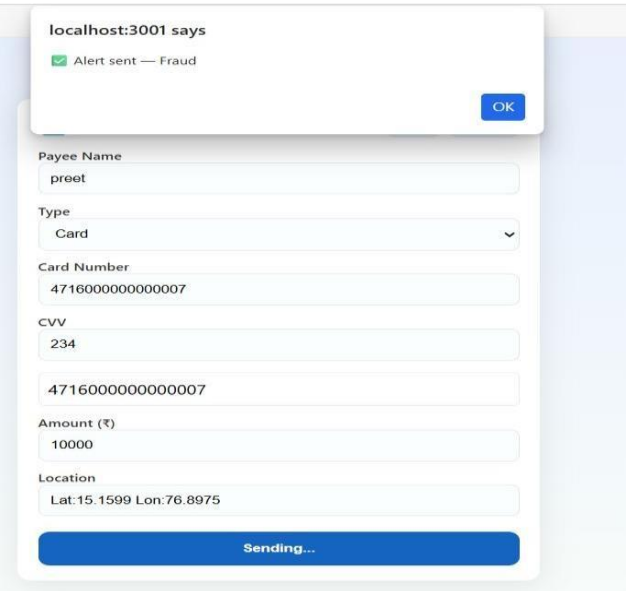

Fig 7. Card transaction fraud alert generation

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.155177

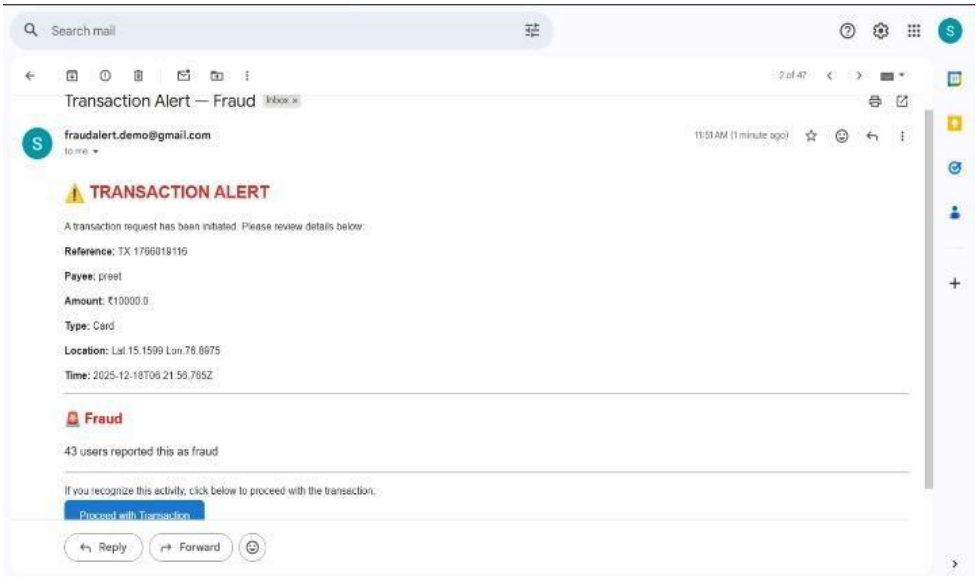

Fig 8. Email alert for fraudulent card transaction

Fig 9. Transaction confirmation page showing fraud risk

Fig 10. Successful payment after user confirmation

5. CONCLUSION

The AI-designed system for the detection of cyber fraud is a state-of-the-art intelligent system that is highly effective for the detection of fraudulent online transactions. By incorporating the concepts of machine learning, behavioral analysis, and online monitoring, the unauthorized actions can be accurately identified and blocked. In the current solution, the system learns from the new data, and therefore, the system can adapt to the ever-changing nature of cyber threats. The system minimizes the risks associated with finances and maximizes the trust for the processes involved in online payments. Future developments may emphasize more on the advanced concepts of the neural network, multi-bank fraud sharing, or the graph displays.

REFERENCES

[1]. A. Dal Pozzolo, O. Caelen, Y. Le Borgne, S. Waterschoot, and G. Bontempi, "Learned lessons in credit card fraud detection from a practitioner perspective," *Expert Systems with Applications*, vol. 41, no. 10, pp. 4915–4928, 2014.

[2]. P. K. Singh and R. Jain, "A survey on credit card fraud detection using machine learning," *International Journal of Engineering Research & Technology*, vol. 6, no. 7, pp. 1–6, 2017.

[3]. A. Bahnsen, D. Aouada, B. Ottersten, "Example-dependent cost-sensitive decision trees for fraud detection," *Expert Systems with Applications*, vol. 42, no. 19, pp. 6609–6619, 2015.

[4]. P. Ravisankar, V. Ravi, G. Raghava Rao, and I. Bose, "Detection of financial statement fraud and feature selection using data mining techniques," *Decision Support Systems*, vol. 50, no. 2, pp. 491–500, 2011.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026
DOI: 10.17148/IJARCCE.2026.155177

[5]. R. J. Bolton and D. J. Hand, "Statistical fraud detection: A review," *Statistical Science*, vol. 17, no. 3, pp. 235–255, 2002.
[6]. S. Jurgovsky et al., "Sequence classification for credit-card fraud detection," *Expert Systems with Applications*, vol. 100, pp. 234–245, 2018.
[7]. A. Srivastava, A. Kundu, S. Sural, and A. K. Majumdar, "Credit card fraud detection using Hidden Markov Model," *IEEE Transactions on Dependable and Secure Computing*, vol. 5, no. 1,pp. 37–48, 2008.
[8]. S. Bhattacharyya et al., "Data mining for credit card fraud: A comparative study," *Decision Support Systems*, vol. 50, no. 3, pp. 602–613, 2011.
[9]. Q. Chen, H. Jiang, Q. Guo, and J. Chen, "Fraud detection for fintech transactions using machine learning," in *Proc. IEEE International Conference on Big Data*, 2018, pp. 4187–4196.
[10]. G. Kou, Y. Lu, Y. Peng, and M. Shi, "Evaluation of classification algorithms using MCDM and rank correlation," *International Journal of Information Technology & Decision Making*, vol. 11, no. 1, pp. 197–225, 2012.
[11]. S. Whitrow, D. Hand, P. Juszczak, D. Weston, and N. Adams, "Transaction aggregation as a strategy for credit card fraud detection," *Data Mining and Knowledge Discovery*, vol. 18, no. 1,pp. 30–55, 2009.
[12]. D. Castillo, G. Kogan, and D. Tomar, "Real-time fraud analytics using machine learning," *IEEE Access*, vol. 8, pp. 160926–160936, 2020.
[13]. M. Zareapoor & P. Shamsolmoali, "Application of credit card fraud detection: Based on machine learning techniques," in Proc. IEEE International Conference on Computational Intelligence and Communication Technology, 2015, pp. 1-6.
[14]. X. Li, W. Huang, and J. Luo, "Dynamic financial fraud detection using adaptive algorithms," *Journal of Financial Crime*, vol. 27, no. 4, pp. 1135–1150, 2020.

