



International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 9.935

Volume 15, Issue 5, May 2026

UPI Fraud Detection using Hybrid Deep Learning

Dr. R.Muthuvenkatakrishnan, Ramani Teja Kiran, Reddaboina Gokul, Rayala Dhanush,

Assistant Professor, Dept. of Computer Science and Engineering, Bharath Institute of Higher Education and Research,
Tamil Nadu, India

Dept. of Computer Science and Engineering, Bharath Institute of Higher Education and Research, Tamil Nadu, India

Dept. of Computer Science and Engineering, Bharath Institute of Higher Education and Research, Tamil Nadu, India

Dept. of Computer Science and Engineering, Bharath Institute of Higher Education and Research, Tamil Nadu, India

ABSTRACT: The Unified Payments Interface (UPI) has transformed the digital financial transactions in India with the ability to make professional and merchant payments instantly and seamlessly on a peer to peer basis. Nonetheless, the quick rise in digital transactions has greatly extended the danger of committing financial frauds including phishing attacks, identity theft, intruders and fraudulent payment demands. The traditional fraud detection systems mainly consist of rule-based and simple machine learning algorithms that are not known to detect advanced and emerging fraud trends in real time. The paper suggests a Hybrid Deep Learning-based UPI Fraud Detection Framework incorporating various techniques of deep learning, such as Long Short-Term Memory (LSTM), Convolutional Neural Networks (CNN), and Artificial Neural Networks (ANN) to enhance the accuracy and reliability of the fraud detections. The suggested system will examine transaction history, behavioral pattern, device details, location characteristics, and frequency of transactions to detect suspicious activities. The use of LSTM captures the sequential behavior patterns in transactional sequences, CNN is used to extract the hidden patterns in the complex transactional data, and ANN is used to carry out the final fraud classification. The hybrid model allows real time tracking of UPI transactions which greatly minimizes false positive and false negatives as opposed to the traditional systems of fraud detection. The offered framework will increase the security of financial transactions and offer a scalable solution that can address the volume of digital payment data due to the combination of feature engineering, anomaly detection mechanisms, and predictive modeling with deep learning.

KEYWORDS: Upi Fraud Detection, Deep Learning, LSTM, CNN, Artificial Neural Network, Financial Fraud Detection, Analysis of Behaviors, Digital Payment Security.

I. INTRODUCTION

The active development of the digital payment technologies has changed the global financial ecosystem greatly. With the introduction of the Unified Payments Interface (UPI) in India, the manner in which people and companies make financial transactions has been transformed. UPI allows immediate transfer of money between bank accounts using mobile applications and is convenient, fast, and can be used in a variety of banking systems. Its simplicity and efficiency have seen UPI grow exponentially in adoption to be one of the most commonly used real-time payment systems in the world. UPI-enabled application processes millions of transactions each day, therefore, it is an important part of the Indian digital economy.

Although UPI has had many positive aspects, this trend has also been met with cybercriminals who are using their weak spots to perpetrate fraud against the digital payment system. Fraudulent activities that are commonly related to the UPI are phishing, counterfeit payment requests, social engineering, identity theft, and unauthorized account access. Fraudsters are also known to employ advanced methods in order to manipulate the users or capitalize on the vulnerability of the transaction authentication systems. This has rendered financial institutions and payment platforms with a big challenge to identify and stop fraudulent transactions.

Fraud detection systems of the traditional kind are mainly based upon rule-based systems and simple machine learning methods. Such systems normally identify fraud on the basis of preset limits like transactional abnormality volumes or volume. But these methods do not usually manage to capture tricky patterns of behavior related to current cyber fraud methods. Fraudsters keep evolving their schemes and hence rules-based systems cannot be considered to be effective in

curbing new threats. Also, conventional models often produce high false positive rates that have the effect of blocking valid user transactions that would decrease user trust and satisfaction.

The recent developments in the field of artificial intelligence and deep learning have provided new opportunities in the enhancement of the system of fraud detection. Deep learning models can process large amounts of transactional data and extract concealed patterns which are hard to discover in traditional statistical techniques. These models have the capability to get to know complicated associations among numerous features like transaction time, location, device details, and user behavior patterns. With such capabilities, various fraud detection systems can be developed with deep learning to achieve enhanced prediction and adapt to the changing fraud methods.

In that regard, the current study offers a Hybrid Deep Learning Framework of UPI Fraud Detection, which can combine several deep learning frameworks to improve the performance of detecting fraud. The proposed system consists of Long Short-Term Memory (LSTM) networks, Convolutional Neural Networks (CNN), and Artificial Neural Networks (ANN) that are used to analyze the sequences of transactions, isolate hidden patterns of behavior, and classify frauds correctly. The system considers various parameters such as the transaction history, the device features, the location data as well as the frequency of the transactions with the aim of detecting suspicious activities in real time.

This hybrid method enhances the overall detection power of using the advantages of various deep models of learning. The LSTM networks are also very efficient in the extraction of sequential dependencies in the transaction data whereas the CNN models can extract high-level patterns of complex feature representations. The last layer of classification used with the help of ANN is an additional layer of classification that increases the accuracy of predicting and minimizes the rate of false detection results. With the combination of the above methods, the intended system is proposed to offer a scalable and dependable fraud detection system that can offer security to high-scale digital payment transactions.

II. LITERATURE SURVEY

The detection of financial fraud in online payment systems has emerged as a significant field of study because of the high rate of online transactions and online banking portals development. A number of employees have suggested the use of machine learning and deep learning systems, which can be used to track fraudulent activities within financial systems, especially when using Unified Payments Interface (UPI).

Nazmoddin et al. [1] suggested a machine learning-based method of fraudulent UPI transactions identification by using supervised learning algorithms. The research was aimed at the investigation of transaction characteristics (amount, time, and user behavioral patterns). These findings confirmed that machine learning frameworks are capable of enhancing the accuracy of fraud detection by a large margin than those of traditional rule-based systems.

Rupa Rani et al. [2] proposed a safe UPI fraud detection model that combines a machine learning approach with feature engineering approaches. Dimensionality reduction and class balancing were the preprocessing methods used in the system to enhance the performance of detection. The significance of dealing with a skewed dataset in the detection of financial fraud problems was emphasized in their work.

A comparative analysis of various machine learning algorithms to detect UPI fraud was given in the work of Sindhu and Vijaya Sree Swarupa [3]. Some of the algorithms that they studied include decision trees, support vector machines, and clustering-based anomaly detection techniques. The research came up with the conclusion that the application of the two other strategies together, i.e., supervised and unsupervised learning, can enhance the ability to identify the patterns of fraud that are unknown.

A fraud detection model that analyzes the pattern of transactions within digital payment systems was proposed by Nagaraj et al. [4] and is founded on Convolutional Neural Networks (CNN). Hidden relationships among the transactional features were captured using the CNN architecture, which allowed it to detect more complex fraud patterns than the traditional machine learning models.

Priya et al. [5] explored the anomaly detecting algorithms of UPI transactions through machine learning models. The focus of their work was on the importance of behavioural analysis, monitoring of transaction patterns in suspicious

activity detection. The paper has shown that anomaly detection algorithms have the capacity of identifying abnormal transaction patterns in financial data.

An example of deep learning models that included Bidirectional Long Short-Term Memory (BiLSTM) networks with an attention-based autoencoder was suggested by Sudharson et al. [6] to implement a financial fraud detection model. The model represented sequential behavior of the transactions and enhanced the feature representation by attention, which results in enhanced performance of detecting multifaceted fraudulent behavior.

Pillai and Ponmary Pushpa Latha [7] proposed a hybrid deep learning algorithm combining LSTM and CNN systems to detect fraud in a banking system automatically. The model used sequential transaction trends and spatial features extraction to enhance the accuracy of fraud detection and the false positive rates were minimized.

The machine learning-based UPI fraud detection system presented by Sushma et al. [8] is based on the analysis of metadata of transactions, device data, and behavioral features of users. The system had a better efficiency to detect ingredients by incorporating machine learning techniques of classification.

Tyagi [9] discussed the use of artificial intelligence in the detection of financial fraud and emphasized the ability of deep learning algorithms to process a large amount of transaction data and discover the concealed fraudulent patterns. The paper has highlighted the increased significance of AI-powered strategies in protecting current digital payment systems.

Wei Min et al. [10] suggested a deep behavioral sequence clustering method of detecting fraud based on explainable deep learning methods. The model studied sequence of transactions and used mechanisms of clustering in order to detect patterns of abnormal behavior in financial transactions.

In a comprehensive research, Bhattacharyya et al. [11] have developed credit card fraud detection that involves machine learning algorithms like random forest, logistic regression, and support vectors machines. The study revealed that ensemble models are a highly effective way of optimizing fraud detection with highly skewed datasets.

Carcillo et al. [12] suggested an adaptive fraud detection system based on streaming data analysis and real-time machine learning. They are addressing the problem of fraud by processes that deal with large volumes of financial transaction streams and dynamically update models to detect new trends in fraud.

In the article by Fiore et al. [13], the authors proposed a deep learning model of detecting financial fraud through autoencoders and neural networks. The paper has shown that deep architectures have the ability to acquire more intricate feature embeddings and enhance detection of anomalies within transaction data.

Pozzolo et al. [14] examined the problem of class imbalance in the fraud detection systems and suggested cost-sensitive techniques in learning to solve the problem. Their work emphasized the necessity of a balance between the detection accuracy and reducing the false positive.

Randhawa et al. [15] suggested application of deep neural network plus random forest classifier in order to identify fraudulent financial transactions. Their hybrid framework was able to gain better detection accuracy through a way that deep feature extraction was employed together with ensemble learning methods.

Though such studies show that there are tremendous improvements in fraud detection methods, most of the current systems use single-model structures which are not capable of appropriately depicting behavioral patterns which are complex and exist during UPI transactions. Hence, the proposed study presents a hybrid deep learning model with LSTM, CNN, and ANN to enhance the accuracy of fraud detection, minimization of the false detection, and efficient provision of real-time monitoring of UPI transactions.

III. PROPOSED METHODOLOGY

The high rate of online payment systems has contributed to the greater demand of smart systems of fraud detection that can be used to spot suspicious activity in real time. The conventional methods of fraud detection are primarily based on rule-based systems and simplistic machine learning methods and they are not effective to identify sophisticated and changing patterns of fraud. To overcome these shortcomings, the proposed system presents Hybrid Deep Learning-based UPI Fraud Detection Framework, which has been proposed to utilize a combination of various deep learning models in order to enhance accuracy and reliability of detection. The suggested system studies different properties of transactions such as the amount of transactions, time, user behavior pattern, information regarding devices and the geographical location. Through a combination of various deep learning methods that include the Long Short-Term Memory (LSTM), Convolutional Neural Networks (CNN) and Artificial Neural Networks (ANN), the system can both learn sequential transaction patterns and uncover hidden relationships among features in large amounts of financial data. The hybrid system allows the system to identify fraudulent transactions more efficiently with a reduced amount of false positive and false negative.

A. SYSTEM ARCHITECTURE

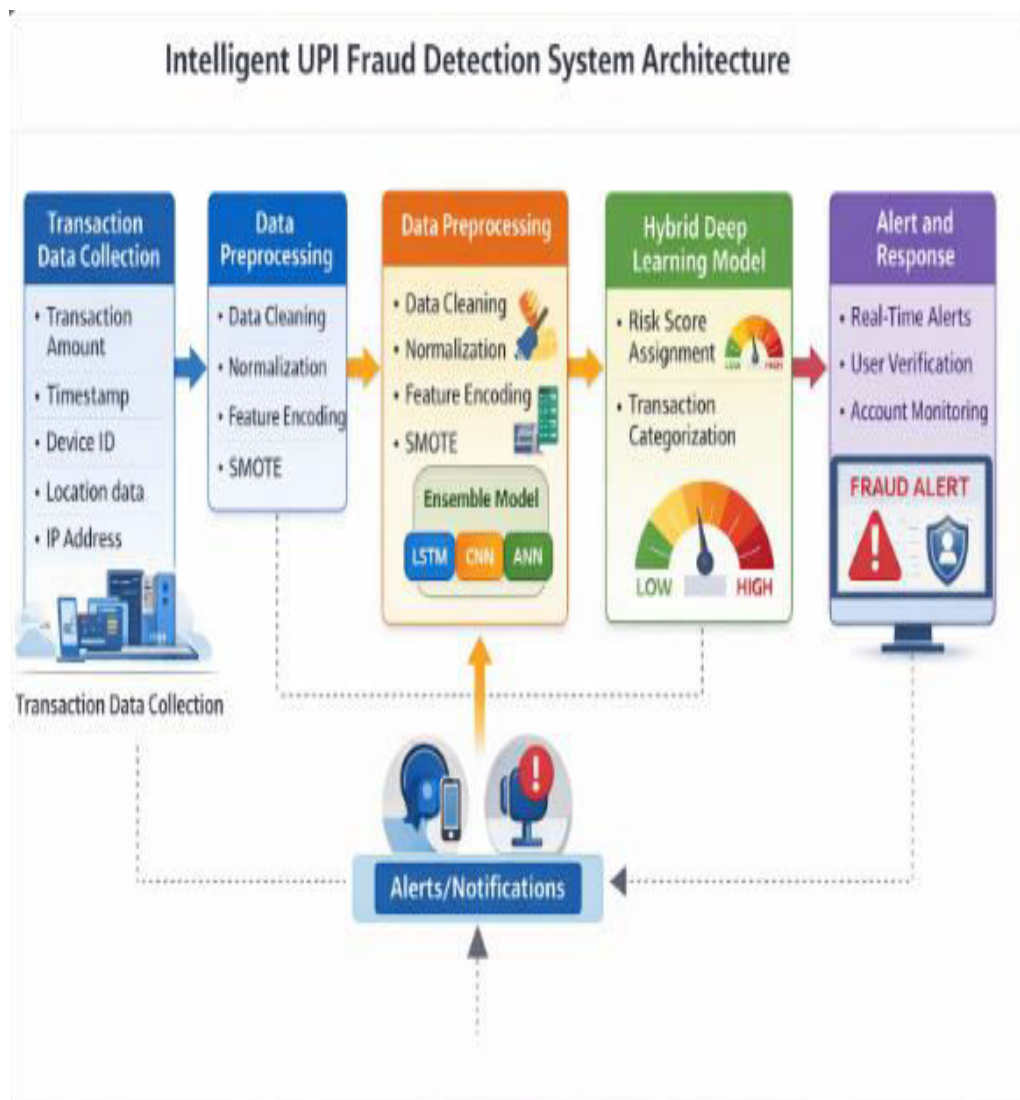


Figure 1: System Architecture

The architecture of the proposed fraud detection system has several layers of processing transaction data and detecting possible fraud patterns. Data concerning the transactions that are made on UPI platforms are initially collected and stored to be analyzed. This information consists of several unique attributes, including; transaction amount, date, device details, IP address, and position of the user. The data on transactions obtained is then sent to the preprocessing layer where data cleaning, normalization and feature encoding is done. SMOTE (Synthetic Minority Oversampling Technique) is among the techniques used to resolve the class imbalance issue that is common in datasets of fraud detection. We preprocessed the raw data and then put the processed data into the Hybrid Deep Learning Model. The LSTM network is a sequential analysis network of transactional patterns and user behavioral sequence. The CNN element obtains concealed relationships and sophisticated feature associations on the transaction dataset. The results of these models are then put together and fed into an Artificial Neural Network (ANN) classifier that does the actual fraud prediction. The results of the prediction are sent to a risk assessment module which provides a score to the transaction of risk of fraud. Depending on the risk level assigned, the system activates the right security measures like verification of transactions, generation of alerts or monitoring of accounts.

B. SYSTEM MODULES

Transaction Data Collection Module:

Such a module gathers the information about the transactions made on UPI platforms. The data collected is the amount of transaction, date, device number, IP address, merchant number and location. The gathered data is the main dataset that is used in detecting frauds.

Data Preprocessing Module:

The preprocessing module processes the raw transaction data to be used in machine learning. It does data cleaning, missing data, feature encoding, and normalization. Moreover, the module uses SMOTE method in managing the imbalance in the number of classes between genuine and fraudulent transactions.

Multi-purpose Deep Learning Detection Module:

This is the main component of the proposed system. It incorporates the models of LSTM, CNN, and ANN to examine the patterns of transactions. LSTM will extract sequential behavioral patterns of the transaction history, whereas CNN will extract hidden connections among the transaction features. The ANN classifier takes into consideration the combined output to decide whether the transaction is fraudulent.

Risk Scoring Module and Ensemble :

The ensemble techniques combine the predictions of the deep learning models to enhance the accuracy of the decisions. According to the model prediction, the system will allocate risk score which classifies the transactions into low risk, medium risk, or high risk.

Explainable AI Module :

In order to enhance transparency when deciding on fraud detection, the system will use explainability methods, including SHAP-based feature importance analysis. This module gives us an insight as to what factors are contributing towards what causes a transaction to be classified as a fraud.

Alert and Response Module :

The alert module sends notification when some suspicious transaction is detected. To avoid possible losses of funds, the system can activate other protocols of verification like OTP authentication, blockage of transaction, or account tracking.

C. FLOWCHART

The flowchart shows how the proposed Hybrid Deep Learning-based UPI Fraud Detection System will work. The first step is the UPI transaction data collection that is parameterized with the values of transaction amount, time, device identification, and location. These attributes give crucial details that would be needed in the analysis of the behavior of transactions

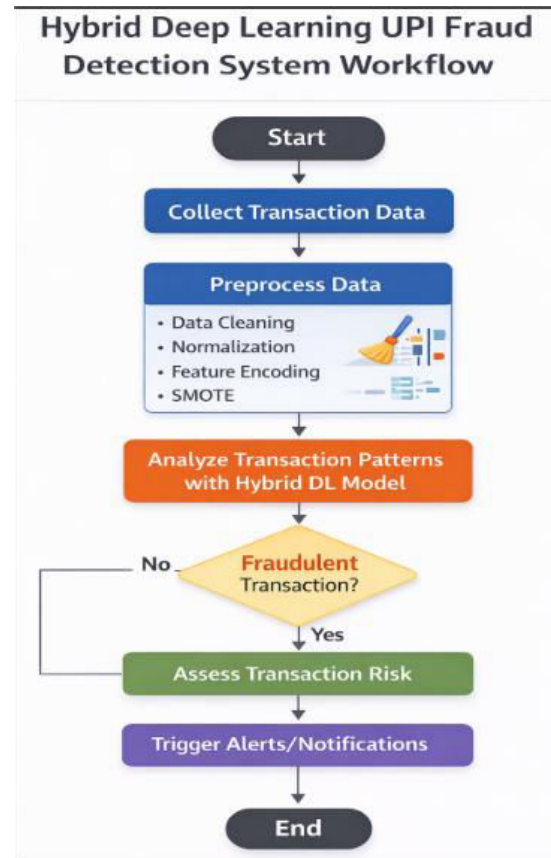


Figure 2: Workflow

ven to the preprocessing phase where the data is cleaned The data is then gi, normalized and feature coded giving the dataset to be analyzed by models. Moreover, the SMOTE method is used to deal with the issue of class imbalance between genuine and fraud transactions.

Following the preprocessing, the processed data are chewed through the hybrid deep learning framework that integrates LSTM, CNN and ANN structures. In this model, the transactions patterns and behavioral sequences are assessed to determine uncovered fraud patterns.

The system then analyzes that the transaction under analysis is fraudulent. In case the anomaly is not detected, the system keeps on monitoring the new incoming transactions. In case a fraud has been detected, the system will then determine the level of risk in the transaction based on the results of prediction.

The last stage is the system creates an alert and notification to take security measures including user verification, blocking transactions or monitoring accounts. The given workflow will allow detecting fraud rather efficiently in real-time and contribute to increasing the level of security of digital payment systems.

Advantages of the Proposed System:

The suggested hybrid deep learning model has a number of benefits compared to the conventional fraud detection systems. To begin with, with the combination of several deep learning models, the system will be able to both learn sequential behavior of transactions and concealed patterns of features, thus increasing the detection accuracy. Second, the system does real-time tracking of UPI transactions, and thus fraudulent transactions can be detected before the transaction is made. Third, advanced preprocessing and class balancing methods are used, which minimize false positive and false negative. Lastly, the scalable architecture enables the system to carry out high numbers of digital payment transactions in an efficient manner, which makes it fit contemporary financial platforms.

IV. RESULTS AND DISCUSSION

The Hybrid Deep Learning-based UPI Fraud Detection system proposed was tested on the basis of the transaction data which included the following attributes: transaction amount, timestamp, device information, IP address, and geographical location. The behavior of transactions was studied using these features and patterns were identified when it comes to legitimate and fraudulent transactions.

Following the data cleaning and normalization and coding of the data, the hybrid deep learning model comprising of LSTM- CNN and ANN were trained to process transaction sequences and derive a relationship between hidden features. Sequential behavioral patterns in user transactions were learnt by the LSTM model and complex feature interactions by the CNN model. The ANN classifier carried out the last classification of the fraud basing on the taught feature representation.

The outcomes of the experiments show that the hybrid model yields better performance than the traditional machine learning models in terms of fraud detection. The system was also more accurate in the predictive process because the system effectively learned both the sequential transaction patterns of entities and complicated relationships between features. Also, SMOTE was used to even the data set and mitigate the influence of legitimate transactions.

The proposed system proved to identify suspicious transactions in real time and minimized false positives and false negatives. The framework will present an effective and scalable approach to risk monitoring of vast amounts of UPI transactions and improve digital payments security by combining the methods of deep learning with risk scoring and alert systems.

V. CONCLUSION

The blistering development of online payment systems like the Unified Payments Interface (UPI) has caused a large number of financial fraud threats to grow. The rule-based mechanisms and simple machine learning models of traditional fraud detection are frequently not able to identify complex and emerging patterns of fraud. In order to overcome these drawbacks, the current study presented Hybrid Deep Learning-based UPI Fraud Detection System that combines LSTM, CNN and ANN model in order to examine transaction patterns and identify fraud.

The suggested system will examine various attributes of transactions like user interaction, device details, transaction history, and geographic positions to detect suspicious transactions. The system enhances the accuracy of fraud detection by detecting sequential patterns with the LSTM trained mechanism and features with the CNN trained mechanism, and classifying with the ANN trained mechanism, creating less false positives, false negatives.

The analysis of the experiment proves that the hybrid model could be used more effectively in detecting fraudulent transactions than when conventional methods are used. Moreover, the system will help in monitoring transactions in real time and processing large amounts of digital payment information on-demand. Consequently, the suggested framework is a good and effective way of ensuring that the security of UPI-based digital transactions is improved.

VI. FUTURE SCOPE

Further studies can be conducted to enhance the performance of fraud detectors, including the incorporation of more sophisticated deep learning models like Transformer models and Graph Neural Networks that would be able to learn intricate user-user, user-device, and user-transactions relationships.

It is also possible to scale the system to enable real-time streaming transaction analysis using big data processing piping solutions like Apache Kafka or Spark to process large financial data more effectively. Transparency and trust in decisions to detect fraud can also be enhanced by incorporating sophisticated explainable AI methods.

Besides, the proposed system can be integrated with banking infrastructures and digital payments platforms to introduce automated controls over fraud and rapid reaction to suspicious actions, thus enhancing the security of digital financial ecosystems on the whole.

REFERENCES

- [1] Dr. M. D. Nazmoddin, M. Swetha, G. Yashwanthi and Y. Divyasree, UPI Fraud Detection with the help of machine learning, Eudoxus Press, 2024. [Online]. Available: <https://eudoxuspress.com/index.php/pub/article/view/2503>
- [2] R. Rani, A. Alam, and A. Javed, "Secure UPI: Fraud Detection System based on Machine Learning and UPI transactions," in Proc. 2nd Int. Conf. Disruptive Technologies (ICDT), IEEE, 2024. [Online]. Available: <https://ouci.dntb.gov.ua/en/works/9Jkwmaq7/>
- [3] J. Sindhu and V. S. Swarupa, UPI Fraud Detection with the help of machine learning algorithms, the International Journal of Engineering Research Science and Technology, 2024.[Online].Available:<https://ijerst.org/index.php/ijerst/article/view/446>
- [4] M. Nagaraju, P. Nagendra Babu, et al., "Fraud Detection by using Convolutional Neural Networks (CNN) in UPI," 2024.[Online].Available:<https://society.org/articles/activity/10.21203/rs.3.rs-4088962/v1>
- [5] N. Priya, R. Sridhar and R. Rajesh, Anomaly Detection in the UPI Transactions with the help of machine learning techniques, in the Proc. IEEE Conf., 2022. doi: 10.1109/UPI2022.9831123.
- [6] K. Sudharson, S. Varsha and S. Rajalakshmi, 2025, Financial Transactional Fraud Detection Across a Hybrid BiLSTM with Attention-Based Autoencoder, International Research Journal of Modernization in Engineering Technology and Science. [Online]. Available: <https://asianrepo.org/index.php/irjmt/article/view/128>
- [7] R. P. Pillai and D. P. Pushpa Latha, A Deep Learning Based Hybrid Model of the Automated Detection of Internal Fraud in a bank system using the LSTM and CNN Techniques, Journal of Information Systems Engineering and Management, 2025. [Online].Available:<https://jisemjournal.com/index.php/journal/article/view/7468>
- [8] S. Madhu Bala et al, A. A. H. Sushma, [8] "ML-powered UPI Fraud Detection" JournalStar Research Journal, 2025. [Online]. Available: <https://journalstar.in/ml-powered-upi-fraud-detection/>
- [9] N. Tyagi, Artificial Intelligence in Financial Fraud Detection: A Deep learning approach to it, International Journal of Computer Technology and Engineering, 2024. [Online].Available:<https://ijctece.com/index.php/IJCTEC/article/view/180>
- [10] W. Min, W. Liang, et al., "Explainable Deep Behavioral Sequence Clustering to detect transaction frauds," arXiv preprint arXiv:2101.04285, 2021. [Online]. Available: <https://arxiv.org/abs/2101.04285>
- [11] A. Bhattacharyya, V. Jha, K. Tharakunnel and J. Westland, Data Mining in Credit Card Fraud: A Comparative Study, Decision Support Systems, vol 50, no 3, pp. 602-613, 2011.
- [12] F. Carcillo, Y. A. Le Borgne, O. Caelen, G. Bontempi, Streaming Active Learning Strategies for Real-Life Credit Card Fraud Detection Data Mining and Knowledge Discovery, vol. 33, no. 6, pp. 1499-1529, 2019.
- [13] R. Fiore, F. Palmieri, A. Castiglione and A. De Santis, Generative Adversarial Networks to advance the effectiveness of classification in credit card fraud detection, Information Sciences, vol. 479, pp.448-455, 2019.
- [14] A. Dal Pozzolo, O. Caelen, R. A. Johnson, and G. Bontempi, Calibrating Probability with Undersampling with Unbalanced Classification in Proc. IEEE Symposium on Computational Intelligence and Data Mining, 2015.
- [15] K. Randhawa, C. K. Loo, M. Seera, C. P. Lim and A. K. Nandi found that AdaBoost and majority voting systems are significant in detecting credit card fraud (p. 14277-14284).



INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

 9940 572 462  6381 907 438  ijirset@gmail.com



www.ijirset.com

Scan to save the contact details