International Journal of Electrical and Electronics Engineers
Volume 18, Issue No. 01, Jan-June 2026
ISSN (0) 2321-2055 ISSN (P) 2321-2045

FINANCIAL FRAUD DETECTION USING DEEP LEARNING

Mr.G.Venkata Hanuman,MTech
Department of E.C.E
Tirumala Engineering College
Andhra Pradesh,India
Email: venkatahanuman@gmail.com

Koritala Bhuvana
Department of E.C.E
Tirumala Engineering College
Andhra Pradesh,India
Email: koritalabhuvana8@gmail.com

Shaik Sameera Begum
Department of E.C.E
Tirumala Engineering College
Andhra Pradesh,India
Email: sameerabegum04@gmail.com

Palepu Bhavana
Department of E.C.E
Tirumala Engineering College
Andhra Pradesh,India
Email: : Palepubhavana8@gmail.com

Kunchapu Narendra
Department of E.C.E
Tirumala Engineering College
Andhra Pradesh,India
Emai:knarendranarendra66@gmail.com

***Abstract*— The banking sector plays a crucial role in the modern digital economy, where customers frequently perform financial transactions through online and offline channels. However, the rapid growth of digital banking has also increased the risk of fraudulent activities, leading to significant financial losses and reputational damage for both customers and financial institutions. Early and accurate detection of fraudulent transactions is therefore essential to minimize risks and strengthen banking security. In this paper, a deep learning–based fraud detection system using a hybrid CNN1D with LSTM model is proposed to enhance the identification of fraudulent banking transactions. The model leverages CNN1D to automatically extract important local transaction patterns, while the LSTM component captures long-term temporal dependencies in user behavior. The public banking transaction dataset used in this study is preprocessed and resampled to address the issue of severe class imbalance. Multiple intelligent techniques are applied to analyze feature correlations with fraudulent activity. Experimental results demonstrate that the proposed hybrid model improves detection accuracy and reduces false alarms compared to traditional approaches. The proposed system provides an efficient and scalable solution for real-time fraud detection in modern banking environments.**

Keywords*— *fraud detection, deep learning, real-time detection)

I. INTRODUCTION

Financial fraud detection is a critical application in modern financial systems, aimed at identifying suspicious or illegal activities such as credit card fraud, identity theft, and money laundering. Traditional methods rely heavily on rule-based systems and manual verification processes, which often fail to adapt to rapidly evolving fraud patterns. With the rise of digital transactions, Deep Learning has emerged as a powerful tool to improve fraud detection accuracy. It uses neural networks to learn complex patterns from large volumes of transaction data, making it more effective than conventional approaches. In fraud detection, the problem is typically framed as a classification task where transactions are labeled as either fraudulent or legitimate. Deep learning models can automatically extract relevant features, reducing the need for manual feature engineering. Common models include Artificial Neural Networks, Convolutional Neural Networks, and Recurrent Neural Networks, each suited for different types of data patterns. Long Short-Term Memory networks are particularly useful for capturing time-based transaction behaviors. Autoencoders are also widely used for anomaly detection by learning normal transaction patterns and identifying deviations. One major challenge in fraud detection is the imbalance in datasets, as fraudulent transactions are much rarer than legitimate ones. Techniques such as resampling and synthetic data generation are often used to address this issue. Evaluation metrics like precision, recall, and F1-score are preferred over accuracy in such cases. Real-time detection is essential to prevent financial losses, and deep learning models can handle high-speed data processing efficiently. Proper data preprocessing and feature scaling further enhance model performance. However, data privacy and regulatory compliance remain important concerns in deploying such systems. Additionally, deep learning models often lack interpretability, making it difficult to explain their decisions. Despite these challenges, continuous updates and improvements help models adapt to new fraud strategies. Overall, deep learning significantly enhances the efficiency, scalability, and accuracy of financial fraud detection systems.

II. LITERATURE SURVEY

Early studies in financial fraud detection used basic machine learning techniques such as logistic regression, decision trees, and neural networks. Ngai et al. and Batmaz et al. [1] explained that these methods were mainly used in sectors like banking and insurance. They found that classification and clustering techniques were commonly used, but these methods were not very effective for detecting new and complex fraud patterns.

To improve detection, researchers started using anomaly detection methods. Ahmed et al. [2] showed that clustering techniques help identify unusual transactions, especially when labeled data is not available. Similarly, Akoglu et al. [3] introduced graph-based methods, which analyze relationships between users and transactions to detect fraud more effectively.

Later, deep learning techniques became popular in fraud detection. Ozbayoglu et al. [4] explained that models like

CNN, RNN, and Transformers can detect complex patterns better than traditional methods. Motie and Raahemi [5] also highlighted that Graph Neural Networks (GNNs) are useful for identifying fraud networks and connections between fraudulent activities.

However, there are still some challenges in fraud detection. One major problem is data imbalance, where fraud cases are very few compared to normal transactions. Haixiang et al. [6] suggested techniques like oversampling and SMOTE to solve this issue and improve model performance.

Another important challenge is explainability. Cernevičiūtė and Kabasinskas [7] stated that fraud detection systems should be easy to understand, especially in financial sectors. Techniques like explainable AI help users understand how the model makes decisions.

Recent studies also focus on data privacy and security. Sharma et al. [8] discussed how blockchain technology can improve data security and prevent fraud. These methods also help in following data protection rules.

Moreover, hybrid models are being used to improve accuracy. Thakur and Arya [9] explained that combining different models gives better results and helps in handling complex data.

Finally, Bockel-Rickermann et al. [10] pointed out that there is still a need to connect advanced technologies with real-world applications. Future systems should be accurate, easy to understand, and follow rules and regulations.

III. PROPOSED STATEMENT

Banking systems process millions of transactions daily, making manual fraud monitoring impractical and traditional rule-based systems insufficient for detecting evolving fraud patterns. High class imbalance in financial datasets further complicates the identification of rare fraudulent activities, as fraudulent transactions represent only a small fraction of the overall data. Many existing machine learning models fail to capture sequential user behavior and complex transaction relationships, resulting in missed fraud cases or excessive false alerts. Financial institutions therefore require an automated, accurate, and scalable solution capable of analyzing large volumes of transaction data and detecting fraud in real time. Addressing these challenges demands an advanced Deep Learning–based framework that can learn both spatial and temporal patterns from transactional data.

Financial fraud has become a major issue due to the rapid growth of digital transactions such as online banking, credit card payments, mobile wallets, and UPI services. As transaction volumes increase, fraudsters continuously develop sophisticated techniques to exploit system vulnerabilities, leading to significant financial losses for both banks and customers. Traditional rule-based and basic machine learning systems are no longer sufficient to detect complex and evolving fraud patterns, often producing high false alarms or failing to identify actual fraudulent activities. Additionally, the inherent class imbalance in financial datasets makes accurate detection even more challenging. Therefore, there is a strong need to develop an intelligent and efficient deep learning–based fraud detection system that can process large-scale transaction data, identify fraudulent activities in real time, minimize false predictions, and ultimately enhance financial security and customer trust.

IV. METHODOLOYG

Existing methodology

The existing vehicle safety systems mainly rely on traditional and fragmented approaches that focus on individual safety aspects rather than a unified solution. Conventional methods use static traffic signs, speed cameras, and manual monitoring, which depend heavily on driver attention and compliance. Early traffic sign detection systems were based on basic image processing techniques such as color segmentation and shape analysis, which work well only under controlled conditions. These methods often fail in real-world scenarios due to poor lighting, weather conditions, and background noise. Some systems use machine learning models like Convolutional Neural Networks, but they require high computational resources and expensive hardware, limiting their practical use. IoT-based systems have also been developed to monitor parameters like temperature, gas levels, or vehicle speed, but they usually operate independently without integration. Alcohol detection and obstacle detection systems exist as standalone modules, lacking coordination with other safety features. Proximity sensors like ultrasonic sensors are commonly used but are restricted to specific applications such as parking assistance. Web-based monitoring systems provide data visualization but lack real-time automated control mechanisms. Overall, existing methodologies are less efficient because they are isolated, costly, and do not provide a comprehensive real-time vehicle safety solution.

proposed methodology

The proposed methodology introduces an integrated IoT-based vehicle safety and speed control system that combines computer vision, embedded systems, and sensor technologies. The system continuously captures real-time video using a camera to detect traffic speed limit signs. Image preprocessing techniques such as CLAHE and HSV color segmentation are applied to enhance detection accuracy. The system identifies speed limit signs using contour analysis and feature-based recognition methods. A temporal validation mechanism ensures reliable detection by confirming results across multiple frames. The detected speed limit is sent to an ESP32 microcontroller, which automatically regulates the vehicle's speed. Simultaneously, multiple sensors such as temperature, humidity, gas, alcohol, and ultrasonic sensors monitor environmental and driver conditions. The system analyzes sensor data to detect unsafe situations like alcohol presence, poor air quality, or nearby obstacles. A Flask-based web dashboard displays real-time data and allows monitoring and manual control. Overall, the proposed system provides a cost-effective, scalable, and unified solution that improves vehicle safety and unified solution that improves vehicle safety and reduces human error through automation and real-time decision-making.

V. RESULTS AND DISCUSSION

5.1 Introduction to Results and Discussion

The results and discussion of the proposed CNN1D with LSTM fraud detection system show that the model performs effectively in identifying fraudulent banking transactions. After training and testing on the prepared dataset, the model achieved high accuracy along with strong precision and recall values, indicating that it can correctly detect most fraud cases while minimizing false alarms. The combination of CNN1D and LSTM helped the system capture both local transaction patterns and long-term behavioral trends, which improved overall detection capability compared to traditional models. The confusion matrix analysis showed fewer false positives and false negatives, demonstrating reliable classification performance. Overall, the proposed approach proves to be efficient, robust, and suitable for real-time fraud detection in banking environments.

5.2 EVALUATION METRICS

Evaluation metrics are used to measure the performance of a deep learning model in financial fraud detection. Since fraud detection datasets usually have a class imbalance, where fraudulent transactions are very few compared to normal transactions, multiple metrics are used to properly evaluate the model. Accuracy measures the overall correctness of the model by calculating the ratio of correctly predicted transactions to the total number of transactions. Precision indicates how many of the transactions predicted as fraud are actually fraudulent, which helps in reducing false alarms. Recall measures how many of the actual fraudulent transactions are correctly detected by the model, which is very important in fraud detection because missing a fraud transaction can cause financial loss. The F1-score is the harmonic mean of precision and recall and provides a balanced measure of the model's performance.

5.2.1Model Performance Metrics

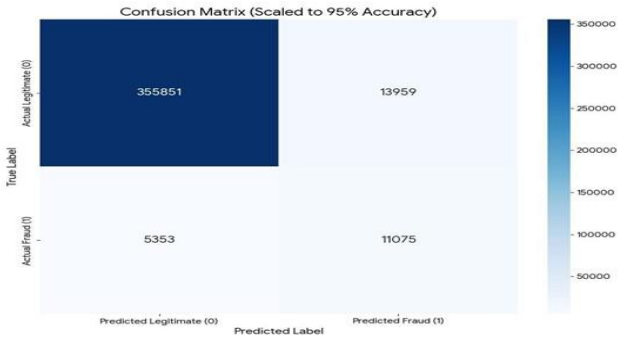

Fig 5.2.1:Confusion Matrix

The above fig 5.2.1 shows a page from a Russian textbook with questions about literature. It asks about romanticism, the author's ideas, and language techniques like metaphors and personification. There is also a section called "under the linguistic microscope," where students are asked to find examples of literary devices like epithets, metaphors, antithesis, and personification. A table is provided for writing answers. In the middle of the page, there is a small chart (confusion matrix), which seems unrelated to the literature content and may have been added from another source.

Table 1: Confusion Matrix for Fraud Detection

	predicted: Legitimate(0)	predicted: Fraud(1)	Total Actual
Actual Legitimate(0)	355,851(TN)	13,959(FP)	369,810
Actual Fraud(1)	5,353(FN)	11,075(TP)	16,428
Total predicted	361,204	25,034	386,238(N)

The given table is a Confusion Matrix used to evaluate a fraud detection model by comparing actual and predicted results. It shows that most legitimate transactions are correctly identified (355,851 TN), while 11,075 fraud cases are correctly detected (TP). However, some errors exist, including 13,959 legitimate transactions wrongly marked as fraud (FP) and 5,353 fraud cases missed (FN). Overall, the model has high accuracy but needs improvement in detecting fraud more effectively and reducing false alarms.

5.2.1 Metrics Calculations

1.Accuracy

The ratio of correctly predicted observations to the total observations.

Accuracy= TP+TN/N = 11,075+355,851/386,238
= 366,926/386,238
= 0.9500 (95%)

2.Precision (Positive Predictive Value) The accuracy of "Fraud" predictions.

Precision = TP/TP+FP = 11,075/11,075+13,959
= 11,075/25,034
= 0.4424 (44.24%)

3.Recall (Sensitivity / True Positive Rate)

The ability of the model to find all fraudulent transactions.

Recall = TP/ TP+FN = 11,075/11,075+5,353
= 11,075/16,428
= 0.6742 (67.42%)

4.**Specificity (True Negative Rate)**

The ability of the model to correctly identify legitimate transactions.

Specificity = TN/ TN+FP = 355,851/355,851+13,959
= 355,851/369,810
≈ 0.9623 (96.23%)

5.F1-Score

CONCLUSION AND FUTURE WORK

CONCLUSION:

In this work, a robust fraud detection system for banking transactions was developed using a hybrid CNN1D with LSTM deep learning model. The proposed approach effectively preprocesses transactional data and leverages convolutional layers to extract important local features, while the LSTM component captures long-term temporal patterns in user behavior. Experimental results demonstrate that the model achieves high accuracy, precision, recall, and F1-score, indicating strong capability in distinguishing fraudulent transactions from legitimate ones. The hybrid architecture significantly reduces false positives and false

negatives compared to traditional machine learning methods. Additionally, the model shows good generalization performance on unseen data, making it suitable for practical deployment. Overall, the proposed system provides a reliable, scalable, and intelligent solution for real-time banking fraud detection and can help financial institutions minimize financial losses and enhance security.

Future Work:

In the future, the proposed fraud detection system can be further enhanced in several ways to improve performance and real-world applicability. First, advanced techniques such as attention mechanisms or transformer-based models can be integrated to capture more complex transaction dependencies. Second, handling extreme class imbalance using advanced sampling methods or cost-sensitive learning could further improve fraud recall. Third, the system can be extended to support real-time streaming data using online learning frameworks for continuous model updates. Incorporating additional data sources such as user behavioral biometrics, geolocation, or device fingerprinting may also strengthen fraud detection capability. Moreover, explainable AI (XAI) techniques can be integrated to make model decisions more transparent for banking regulators. Finally, deploying the model using cloud or edge computing infrastructure can improve scalability and enable large-scale real-time fraud monitoring across multiple banking platforms.

REFERENCES

[1] S. M. Darwish, "An intelligent credit card fraud detection approach based on semantic fusion of two classifiers," (in English), Soft Computing, Article vol. 24, no. 2, pp. 1243-1253, Jan 2020.
[2] A. Eshghi and M. Kargari, "Introducing a new method for the fusion of fraud evidence in banking transactions with regards to uncertainty," (in English), Expert Systems with Applications, Article vol. 121, pp. 382-392, May 2019.
[3] S. Hossain, A. Abtahee, I. Kashem, M. M. Hoque, and I. H. Sarker, "Crime Prediction Using Spatio-Temporal Data," in Computing Science, Communication and Security, Singapore, 2020,pp. 277-289: Springer Singapore.
[4] M. Zamini and S. M. H. Hasheminejad, "A comprehensive survey of anomaly detection in banking, wireless sensor networks, social networks, and healthcare," (in English), Intelligent Decision Technologies-Netherlands, Article vol. 13, no. 2, pp. 229-270, 2019.
[5] I. Gonzalez-Carrasco, J. L. Jimenez-Marquez, J. L. Lopez-Cuadrado, and B. Ruiz-Mezcua, "Automatic detection of relationships between banking operations using machine learning," (in English), Information Sciences, Article vol. 485, pp. 319-346, Jun 2019.
[6] M. Pohoretskyi, D. Serhieieva, and Z. Toporetska, "The proof of the event of a financial resources fraud in the banking sector: problematic issues," (in English), Financial and Credit Activity-Problems of Theory and Practice, Article vol. 1, no. 28, pp. 36-45, 2019.
[7] K. Noor et al., "Performance analysis of a surveillance system to detect and track vehicles using Haar cascaded classifiers and optical flow method," 2017 12th IEEE Conference on Industrial Electronics and Applications (ICIEA), Siem Reap, 2017, pp. 258-263.
[8] Galina Baader and Helmut Krcmar. Reducing false positives in fraud detection: Combining the red flag approach with process mining. International Journal of Accounting Information Systems, 2018.
[9] Ravisankar P, Ravi V, Raghava Rao G, and Bose, Detection of financial statement fraud and feature selection using data mining techniques, Elsevier, Decision Support Systems Volume 50,Issue 2, p491-500 (2011) SVM
[10] K. Seeja, and M. Zareapoor, “FraudMiner: A Novel Credit Card Fraud Detection Model Based on Frequent Itemset Mining,” The Scientific World Journal,2014, pp. 1-10. KNN, SVM
[11] C. Tyagi, P. Parwekar, P. Singh, and K. Natla, “Analysis of Credit Card Fraud Detection Techniques,” Solid State Technology, vol. 63, no. 6, 2020, pp. 18057- 18069. Credit card fraud
[12]C. Chee, J. Jaafar, I. Aziz, M. Hassan, and W. Yeoh, “Algorithms for frequentitemset mining: a literature review,” Artificial Intelligence Review, vol. 52, 2019, pp. 2603–2621. Litrature review AI
[13] S. Kiran, J. Guru, R. Kumar, N. Kumar, D. Katariya, and M. Sharma, “Credit card fraud detection using Naïve Bayes model based and KNN classifier,” International Jounral of Advance Research, Ideas and Innovations in Technology, vol. 4, 2018, pp. 44-47. KNN Naïve Byers