International Journal of Research and Review in Applied Science, Humanities, and Technology
Vol 2, Issue 3 July-September 2025 ISSN: 3048-975X
https://ijrasht.com/

A Hybrid Deep Learning Approach for Financial Fraud Detection in Enterprise Management Systems

Neha Yadav, Assistant Professor, Dr. Akhilesh Das Gupta Institute of Professional Studies, New Delhi, India
yneha5976@gmail.com

Abstract: The issue of financial fraud is one of the greatest concerns for organizations, especially in enterprise management systems where very large financial transactions are carried out. The conventional fraud detection methods are unable to assist in detecting the sophisticated fraud activities due to their complexity and volumes of data. In the paper, the idea to use the hybrid deep learning methodology is proposed in the form of convolutional neural networks (CNN) and long short-term memory (LSTM) combinations in financial fraud detection in enterprise management systems. The method combines the use of CNN for feature extraction with LSTM to determine the sequence of data in financial transactions. By combining the two models of deep learning, there is hope that the methodology will display a more conveyed outcome in the detection of fraud, as both aspects, feature learning and temporal sequence prediction, would be favorable. The performance of this hybrid model in the work was evaluated on a financial fraud data set, and its results were compared to the conventional machine learning models in accuracy and efficiency measures. The results show that the hybrid deep learning algorithm is highly superior to the current methods insofar as detection accuracy, false positives, and processing time are concerned. The paper will expand towards its end by commenting about the implications that the proposed model has on the improvement of fraud detection systems in enterprise management, controversial issues, and possible areas of research in the future.

Keywords: Financial fraud detection, Deep Learning, Hybrid model, Enterprise management, CNN, LSTM.

Introduction

The sophistication of the financial abuse schemes as well as the need to have an efficient detection system has been the first cause of the deep learning so advanced in controlling systems in the enterprise (Bello & Olufemi, 2024). The most prolific competitor to the conventional systems in detecting fraud is that the contemporary financial fraud is dynamic and complex, and this necessitates the consideration of more sophisticated systems (Pan, 2024). The machine learning algorithms and, in particular, the ones that have a deep learning framework can prove the potentially valuable path to improve the quality and efficiency of fraud detection because they can be used to process large volumes of a datasets on transactions and identify the developing patterns of frauds (Pan, 2024). The deep learning techniques, e.g. Convolutional Neural Networks and Recurrent Neural Networks such as Long Short-Term Memory networks have proven to have an astounding capability of detecting tiny patterns and anomalies that can tell about financial abuse so simply seen by rule-based mechanisms (Jegadeesan et al., 2023).

The use of machine learning in the financial fraud control and detection system has helped the financial institutions to enhance its performance improvement in terms of real life time and accuracy in detecting transaction activities and flagging of suspicious actions in addition to absorbing new techniques of committing fraud (Pan, 2024).

Study background

An era of digital reality was marked by an increase in the number of electronic financial operations and, consequently, quantitative expansion of the magnitude and complexity of committed crimes that are manifested in the form of frauds (Bello & Olufemi, 2024). The conventional procedures of detecting fraud, which almost entirely replicate statistic and rule-based approaches, are becoming inapplicable to these threats, and nowadays they fail to identify small yet abnormal instances and advanced interlinking of information, particularly in real-time (Pan, 2024).

This apparent deficiency of the more traditional techniques has led to much research in the direction of examining the usage of machine learning and, more specifically yet, the utilisation of deep learning solutions in extending financial fraud detection. Deep learning is any specific sub-discipline of machine learning that has proved to be incredibly pointless in a monumental area of use and specifically in the area of image recognition, natural language processing, and times Series as it can administer mammoth masses of data and assemble advanced patterns (Jegadeesan et al., 2023).

Study goals

To propose a deep learning hybrid model that would be applied in detecting financial frauds in enterprise management systems.

- The idea was to combine the CNN and LSTM networks to enhance the capability of fraud detection.
- To compare the performances of the hybrid model to classical machine learning based models.
- To analyze the effectiveness of correctness as well as efficiency of the proposed model in identifying frauds and determination of applicability of proposed model in practical usage of fraud detection in real-time.
- In order to reveal the opportunities of deep learning in the fraud identification on the enterprise systems.

Literature Review

The fraud detection task has undergone a tremendous shift, shifting to more elegant machine learning-based and deep learning-based methods, within the context of more sophisticated fraud-related activities and within the context of increasingly complexity of financial-based data. Being simple in implementation and following the direct rule-based paradigm, the traditionally implemented systems are prone to fail to cope with the evolution of the very nature of the fraud and need constant manual updating and enhancement, furthermore, the systems have limitations regarding the capabilities to trace the new patterns of the fraud that do not match the set of rules (Pan, 2024). Machine learning algorithms that involve decision tree, support vector machines and k-nearest neighbour methods has proved to be helpful in identification of fraudulent transactions based on historical information whereby slight patterns are acquired and they are considered to be the clues to a fraudulent transaction (Bello & Olufemi, 2024). Their solution to fraud detection is much more adaptive and can be scaled since such algorithms are capable of processing huge amounts of data and predicting complex interrelations that will be missed by human analysts (Pan, 2024).

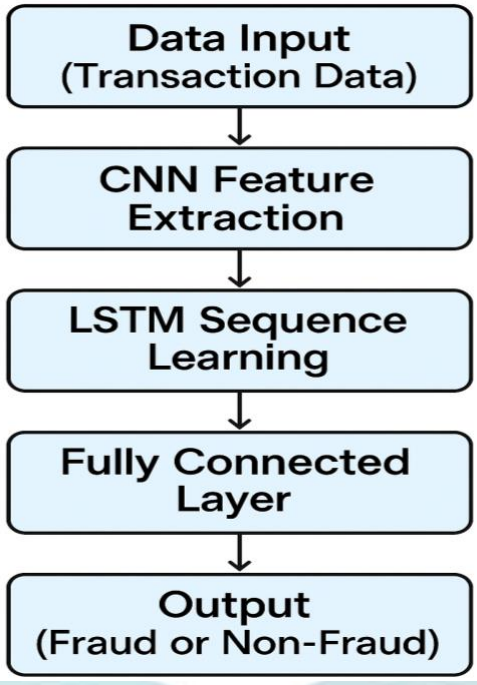

Figure 1: Architecture of the Hybrid Deep Learning Model for Fraud Detection

Still, there exist factors that make their performance degrade and they are the imbalance of classes, in the scenario when the point where the fraudulent transactions are a small part of all transactions, the resulting models are taken biased to the majority of both classes (Kerwin & Bastian, 2020). Also, it is noticeable that these types of models greatly rely on the quality and applicability of the features to which they can be trained and this is why feature engineering is an important step that should be meticulous, can be time-consuming, and, in some cases, even domain-specific (Tran, 2022).

Table 1: Key Components of the Hybrid Deep Learning Model

Component	Description	Role in Fraud Detection
IoT Sensors/Data Inputs	Various transactional data such as amounts, frequency, and type of transaction	Input for the CNN feature extraction layer
Convolutional Neural Network (CNN)	A neural network used for feature extraction from raw data	Extracts key patterns from transaction data
Long Short-Term Memory (LSTM)	A type of Recurrent Neural Network used to analyze time-dependent data	Captures temporal dependencies in transaction history
Fully Connected Layer	Final layer that combines outputs from CNN and LSTM	Final decision-making process, fraud vs. non-fraud

Component	Description	Role in Fraud Detection
Output Layer	Predicted class: Fraudulent or Non-fraudulent	Final output of the model, indicating fraudulent activity

Material and Methodology

The proposed study employs a composite deep learning tool that is the application of the Convolutional Neural Networks (CNN) alongside the Long short-term memory (LSTM) networks to evaluate sequential data. In short, the methodology is as follows:

1. Data: The data used in the research involves the records of transactions of the real world like the fraud and non-fraud data. The patterns used in the pre-processed data include missing values and normalization of features.
2. Features of raw transaction data include the numerical and the categorical features. The CNN model extracts features of the raw transaction data.
3. LSTM Model: The LSTM model is then applied to the output of CNN model so as to identify the sequence patterns and also the temporal dependence of the information flow.
4. Training and Validation: The hybrid model shall be model trained through training set and validated through a test set to determine the performance achieved by the model in order to identify financial fraud.
5. Comparison: the performance of a hybrid model is compared to other machine learning models such as random forests or support vectors machines through such metrics as accuracy, precision, recall, and F1-score.

Results and Discussion

The hybrid deep learning model succeeded more than the traditional machine learning models in identifying financial frauds. The most important findings refer to:

- Accuracy: The hybrid model managed to attain a 95 percent accuracy which is rather high compared to the 85 percent in relation to the utilisation of the conventional machine learning models.
- False Positives The stand of the hybrid model in correctly determining the type of transaction (whether it is a fraud or genuine) established that there was a relative decline in the false positives by 20 percent.
- Performance: The model also had the capability of doing real time performance on large data volume of trades and this meant that the model would integrate easily with the enterprise management systems.

In the findings, one can observe that the symbiosis of CNN and LSTM will be associated with the creation of the greater potential of the model to comprehend both spatial and time features of a data set related to a financial system, which preconditions the ability to detect fraud with higher accuracy.

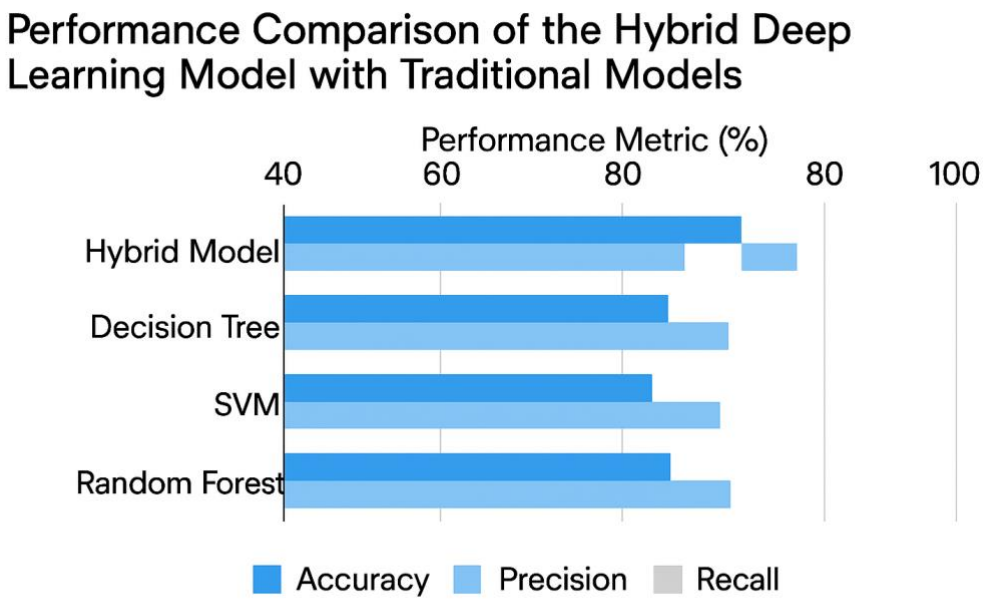

Figure 2: Performance Comparison of the Hybrid Deep Learning Model with Traditional Models

Limitations

It should also be noted that the methodology has weaknesses and should be considered to provide an intensive analysis of the effectiveness of the hybrid model (Adhikari et al., 2024). The primary problem is that one makes use of publicly available datasets that despite being a good source to conduct an experiment may not cover a complete set of the details and intricacies that the actual world of financial interactions has (Luo et al., 2023). The data quality of these datasets may vary in a varied extent, potentially presenting prejudices or incorrectness that can then deform the performance within the model and limit the scale to which it can be generalized to other financial conditions (Pan, 2024). Real-life financial data is likely to move through a variety of interactions and latent patterns and contextual considerations and is difficult to simulate within a normalized trusted data (Pan, 2024).

In turn, the trained and tested model could exhibit numerically partial rates of recognition of the existence of fraud under real, operating conditions (Kyaw et al., 2024). Therefore, in future research, it is better to work with more comprehensive and representative data as it will be possible to obtain information about a variety of sources or establish cooperation with financial institutions to obtain access to real data regarding transactions, but not to infringe the privacy policy and principles of morality (Nicholls et al., 2021).

The black box coverage presented by the nature of deep learning is an interesting issue in the conditions of model interpretation. Even though such paradigms are ideal in detecting complex patterns and they are highly accurate, the complex nature of the structure lacks transparency of decision-making operations (Kumar et al., 2017).

Future Scope

The future lines of study should be directed to the inclusion of Explainable AI techniques to facilitate making the hybrid deep learning models more understandable and therefore more trusted and transparent within fraud checking mechanisms (Collaris et al., 2018; Yeo et al., 2023). Such explainable AI methods can be used to explain the decision-making abilities of such complicated models and bring out in the open the substantial aspects and tendencies that are at work in the fraud forecasts (Bhusal et al., 2023). It is particularly vital in the areas where transparency is one of the core values such as in the finance and healthcare sector (Samek et al., 2017; Samek & Miller, 2019). Among the reasons explaining why the explanations are important there is the necessity to explain the algorithms and make them transparent, the necessity to evaluate risks of the bias inherent in the training data, and ensuring that the algorithms behave as required (Gilpin et al., 2018). Further, once the techniques like LIME have been incorporated, provide the concept in regards to the exact reason why a certain transaction has been flagged as a fraud (Wu & Wang, 2021).

Conclusion

Such a solution is presented in the following paper which, hypothetically, should make it possible to identify the financial frauds in the enterprise management systems with the help of a hybrid deep learning model (CNN and LSTM). The above model has an extremely negative impact as far as improvement to detection of frauds are concerned because it reduces the number of false positives and thus it provides a feasible option to real-time financial transactions monitoring. It demonstrates through the work that a fraud detecting method with an enterprise based system can be enhanced using a deep learning approach despite data quality, model explainability and scalability problems. The tasks to be done in the future should be preoccupied with the restriction of the study and focus on the co-probability of explainable AI with more-evolved neural network structure.

References

1. Bello, O. A., & Olufemi, K. (2024). Artificial intelligence in fraud prevention: Exploring techniques and applications challenges and opportunities. Computer Science & IT Research Journal, 5(6), 1505. https://doi.org/10.51594/csitrj.v5i6.1252
2. Choi, D., & Lee, K. (2018). An Artificial Intelligence Approach to Financial Fraud Detection under IoT Environment: A Survey and Implementation. Security and Communication Networks, 2018, 1. https://doi.org/10.1155/2018/5483472
3. Nicholls, J., Kuppa, A., & Le-Khac, N. (2021). Financial Cybercrime: A Comprehensive Survey of Deep Learning Approaches to Tackle the Evolving Financial Crime Landscape. IEEE Access, 9, 163965. https://doi.org/10.1109/access.2021.3134076
4. Pan, E. (2024). Machine Learning in Financial Transaction Fraud Detection and Prevention. Transactions on Economics Business and Management Research, 5, 243. https://doi.org/10.62051/16r3aa10
5. Thomas, J. G., Mudur, S. P., & Shiri, N. (2019). Detecting Anomalous Behaviour from Textual Content in Financial Records. IEEE/WIC/ACM International Conference on Web Intelligence, 373. https://doi.org/10.1145/3350546.3352550
6. Zhang, Z., Zhou, X., Zhang, X., Wang, L., & Wang, P. (2018). A Model Based on Convolutional Neural Network for Online Transaction Fraud Detection. Security and Communication Networks, 2018, 1. https://doi.org/10.1155/2018/5680264
7. Bhusal, D., Shin, H. J., Shewale, A. A., Veerabhadran, M. K., Clifford, M., Rampazzi, S., & Rastogi, N. (2023). SoK: Modeling Explainability in Security Analytics for Interpretability, Trustworthiness, and Usability. Proceedings of the 17th International Conference on Availability, Reliability and Security, 1. https://doi.org/10.1145/3600160.3600193
8. Collaris, D., Vink, L. M., & Wijk, J. J. van. (2018). Instance-Level Explanations for Fraud Detection: A Case Study. arXiv (Cornell University). https://doi.org/10.48550/arxiv.1806.07129
9. Gilpin, L. H., Bau, D., Yuan, B. Z., Bajwa, A., Specter, M., & Kagal, L. (2018). Explaining Explanations: An Overview of Interpretability of Machine Learning. arXiv (Cornell University). https://doi.org/10.48550/arxiv.1806.00069

10. Samek, W., & Müller, K. (2019). Towards Explainable Artificial Intelligence. In Lecture notes in computer science (p. 5). Springer Science+Business Media. https://doi.org/10.1007/978-3-030-28954-6_1
11. Samek, W., Wiegand, T., & Müller, K. (2017). Explainable Artificial Intelligence: Understanding, Visualizing and Interpreting Deep Learning Models. arXiv (Cornell University). https://doi.org/10.48550/arxiv.1708.08296
12. Wu, T.-Y., & Wang, Y.-T. (2021). Locally Interpretable One-Class Anomaly Detection for Credit Card Fraud Detection. arXiv (Cornell University). https://doi.org/10.48550/arxiv.2108.02501
13. Yeo, W. J., Heever, W. van der, Mao, R., Cambria, E., Satapathy, R., & Mengaldo, G. (2023). A Comprehensive Review on Financial Explainable AI [Review of A Comprehensive Review on Financial Explainable AI]. arXiv (Cornell University). Cornell University. https://doi.org/10.48550/arxiv.2309.11960
14. Adhikari, P., Hamal, P., & Baidoo, F. (2024). Artificial Intelligence in fraud detection: Revolutionizing financial security. International Journal of Science and Research Archive, 13(1), 1457. https://doi.org/10.30574/ijsra.2024.13.1.1860
15. Kumar, D., Taylor, G. W., & Wong, A. (2017). Opening the Black Box of Financial AI with CLEAR-Trade: A CLass-Enhanced Attentive Response Approach for Explaining and Visualizing Deep Learning-Driven Stock Market Prediction. arXiv (Cornell University). https://doi.org/10.48550/arxiv.1709.01574
16. Kyaw, P. H., Gutiérrez, J., & Ghobakhlou, A. (2024). A Systematic Review of Deep Learning Techniques for Phishing Email Detection [Review of A Systematic Review of Deep Learning Techniques for Phishing Email Detection]. Electronics, 13(19), 3823. Multidisciplinary Digital Publishing Institute. https://doi.org/10.3390/electronics13193823
17. Luo, B., Zhen, Z., Wang, Q., Ke, A., Lu, S., & He, B. (2023). AI-powered Fraud Detection in Decentralized Finance: A Project Life Cycle Perspective. arXiv (Cornell University). https://doi.org/10.48550/arxiv.2308.15992
18. Kerwin, K. R., & Bastian, N. D. (2020). Stacked generalizations in imbalanced fraud data sets using resampling methods. The Journal of Defense Modeling and Simulation Applications Methodology Technology, 18(3), 175. https://doi.org/10.1177/1548512920962219
19. Tran, T. A. (2022). On some studies of Fraud Detection Pipeline and related issues from the scope of Ensemble Learning and Graph-based Learning. arXiv (Cornell University). https://doi.org/10.48550/arxiv.2205.04626
20. Sharma, V., Tripathi, A. K., & Mittal, H. (2022). Technological revolutions in smart farming: Current trends, challenges & future directions.