Journal of Informatics Education and Research
ISSN: 1526-4726
Vol 5 Issue 2 (2025)

AI-Powered Fraud Detection and Prevention in Banking

Eqbal Ahmad
Assistant Professor, Department of Computer Science and Engineering, Allenhouse Institute of Technology, Rooma Kanpur, Uttar Pradesh, India – 208008,

Aman Bajpai
Assistant Professor, Department of Computer Application, Allenhouse Business School, Rooma Kanpur, Uttar Pradesh, India – 208008,

Dr.B.Venugopal
Assistant Professor (Finance & Accounting), Indian Institute of Plantation Management, Bengaluru (An Autonomous Organization of the Ministry of Commerce &amp; Industry, Govt. of India), Jnana Bharathi Campus, p.o.Malathalli, Bengaluru-560056.

Dr. Kamarajugadda Tulasi Vigneswara Rao
Assistant Professor, Department of School of Project Management, NICMAR University, Pune, Maharashtra 411045,

Deepa E
Assistant professor , Department of Economics , The zamorins guruvayurappan college,, University of Calicut , Malappuram,

Dr.Rajadurai Narayana Murthy
Post Doc research Scholar with Kyushu Institute of Technology, Japan and Enterprise Architect & Lead with TCS

Abstract:

Deep learning techniques have been integrated in modern banking fraud detection and have reached an extreme degree at which fraud is eliminated. In this research, we develop a Long Short-Term Memory (LSTM) network for the task of transaction series analyses for detecting anomaly pattern that signifies possible fraud activities. Despite their poor performance with respect to the changing fraud approaches used, Long Short-Term Memory (LSTM) networks are shown to excel at finding complicated time-related patterns. With this model fraud prediction becomes possible in real time as it uses the past transactions records to identify protected behaviour with minimum error but maximum accuracy. SHAP (SHapley Additive Explanations) enhances our model as it allows us to observe how the model treats individual cases so as to abide by the rules of the financial industry. We find that although LSTM-SHAP is more expensive than traditional machine learning models in terms of training, it achieves more efficient fraud detection with more transparent operation. Accordingly, the study also positions deep learning approaches as a means to attack financial frauds and enhance the banking security as well as the trust in the banking customers.

Keywords:
AI-powered fraud detection, deep learning, Long Short-Term Memory (LSTM), anomaly detection, SHAP (SHapley Additive Explanations), banking security, fraud prevention.

Introduction:

Digital banking is extending rapidly and the sophisticated and complex fraud issues faced by financial institutions are due to the fact that criminals have advanced and modern hacking methods plus advanced deceptive techniques [1]. However, the current rule based fraud detection methods fail when confronted with the most recent and new type of fraudulent threats. Finally, there are advanced tools and technologies needed against financial fraud that have to receive priority, due to persistent refinement of fraudster tactics. In this regard, AI technology has good algorithms such as machine learning and even deep learning to handle pressing problems of fraud detection with automatic threat detection and more exact predictions that will adapt to new security threat.

One of strongest deep learning models to support fraud detection is the Long Short Term Memory (LSTM) network. LSTMs are possible as they are an architecture of recurrent neural networks in which it is possible to recognize data patterns in the sequential data. Therefore, these can be used to identify fraud activities within transaction histories [2]. Although the usual approach in machine learning models assumes static patterns only, LSTMs can detect time dependent patterns in the transaction data. Specifically, LSTMs continue to encode temporal context into their network to enable the network to discover temporal dependencies important to the detection of anomalies in transaction sequences, thereby keeping a time-series clear understanding about what has happened in the previous transactions [3].

In addition to its application for identification of fraudulent transactions through the use of historical data, LSTMs have various other uses of detection of fraud. For real time detection of the model succeeds as it is learned from multiple sequential data types and re adapt to new patterns of fraud which ultimately reduces both false positives and time taken for responses to fraud activity [4]. The constant update of new transaction data is more suitable to fluent fraud patterns, therefore, LSTMs gain better fraud prediction capability through consistently developing suitability to similar, changing fraud patterns over time.

Deep learning models equipped with LSTMs as an effective fraud detection tool suffers a challenge of implementing these structures in practical LSTMs because of prolonged black box within deep learning models. Stakeholders do not trust AI fraud detection systems as essentially there is little information on how the inner workings of the system should be [5]. Especially when the banking industry regulations have to be followed. With an implementation of the model interpretability tool SHAP (SHapley Additive Explanations) that is able to provide conclusive insight about decision making reasoning, we can now analyze LSTMs with them. By calculating SHAP (SHapley Additive Explanations) values, the model features and their respective influences on predictive outcome can be explained by investigators, and a logical framework for detecting fraudulent transactions can be developed. Therefore, the system shall need complete transparency for regulatory approval and accountability and fairness.

Combination of SHAP technology with LSTM models can increase stakeholder trust level and acceptance of the model systems. Through the explanation of the fraud detection decision-making process, understanding between all the parties including the bankers and the regulators with their customers is enhanced which ensures an ethical and efficient system. SHAP and LSTM have an extremely straightforward representation for fraudsters and stakeholders, which resolves one of the main concerns for AI based fraud detection system, while increasing both the precision of the fraud detection as well as delivering useful explanations to the stakeholders.

After the maturity of sophisticated frauds in the banking industry, traditional methods of fraud detection in the banking industry are no longer adequate. Taking both deep learning models including LSTMs paired with SHAP, users can come up with a concise and progressive fraud detection method. In the end the paper describes LSTM’s implementation in real time fraud detection systems with their benefits that protect the banks through the AI while respecting transparency and regulatory standards.

Related works:
In the last few decades, there has been numerous studies about employing artificial intelligence (AI) and machine learning (ML) for banking fraud detection. Rule based models were the dominant means of detecting traditional fraud with good detection of known fraudulent activities, but less so to novel fraud schemes [6]. Because fraud tactics were becoming increasingly sophisticated, these systems were insufficiently accurate in predicting who would commit fraud and thus, advanced AI models were explored to overcome this.

In the early 2000s, for the purpose of fraud detection tasks, machine learning algorithms like decision trees, random forests, and support vector machines (SVMs) were used. These models allowed the banks to classify transactions as spurious or valid, based on historic historical data, and they worked very well in detecting the well known type of fraud [7]. Nonetheless, temporal relationships and intricate patterns in sequential data are fundamental for discovering fraud in banking transactions, which those models could not well accommodate.

In 2010s, deep learners started to use the recurrent neural networks (RNNs) and the Long Short Term Memory (LSTM) networks for fraud detection. One such RNN type excelling in handle sequential data is LSTMs, hence LSTMs are nature choices of transaction histories that are often correlated in time. LSTMs are able to learn long-term dependencies in transaction data, which enables them to properly detect anomalous patterns, for example, short time frames of sudden elevation of transaction amounts or unusual transaction sequences, which are likely to be connected with a fraud. Zhao et al. (2017) presented studies on how LSTMs can detect fraudulent credit card transactions and compared it against traditional machine learning algorithms, which found the LSTM models capture most fraud transactions used in credit card scams and achieve both better accuracy and crafigeness in detecting fraudulent credits.

Apart from deep learning models, the importance of the model interpretability has been a major study objective in the fraud detection domain. Although black box models such as LSTMs work very well, they have a tendency of being criticised for decisionmaking that is not transparent. Lacking these interpretability qualities they become highly suspect in terms of accountability and trust – especially in industries where trust in technology is of utmost importance, such as banking. In response to this challenge, studies have had many have included SHAP (SHapley Additive Explanations) in deep learning models to improve interpretability. SHAP values provide a clear explanation about how individual features affect the model predictions at a particular model predictions target value, which helps the developers and regulators to understand the reasoning behind the each decision. SHAP was introduced by Lundberg and Lee (2017) as a means to interpret machine learning models and since then has been used widely in fraud detection systems in order to make them more transparent.

In addition, deep learning and ensemble learning techniques have been combined to enhance the fraud detection accuracy. Sahoo et al. (2020) have demonstrated in studies that the same can be done through stacking, boosting, bagging, ensemble methods to boost LSTM based models' performance by taking advantage of multiple models' strengths. Hybrid approaches in these reduce overfitting and enhance the generalization ability of such fraud detection systems, especially in cases where fraudulent transactions are few in the dataset.

The other important area of research lies in integrating the unsupervised learning techniques into the fraud detection. In the cases of the lack of pre labeled fraud data or when pre labeled fraud data is scarce, unsupervised learning methods like autoencoders as well as K means clustering can be used to identify anomalies. For instance, Chandola et al. (2009) discussed different anomaly detection techniques and lately other unsupervised techniques coupled with deep learning models are used for detecting the novel and evolving fraud scheme.

Finally, the area of banking AI powered fraud detection has been making great progress during recent years. Since then, researchers have significantly built on the accuracy and adaptability of the fraud detection systems by leveraging early rule based systems to LSTMs, hence the term deep learning models taken from Greek and used for this specific purpose. Besides, the combination of model interpretability methods such as SHAP and hybrid methods based on the ensemble learning also strengthened the effectiveness and transparency of AI models [8]. The banking sector is constantly hitting with newer forms of fraud, and the AI powered solutions prevent the bank transactions on a completely safe front.

Research methodology:

A quantitative experimental framework is used in this research to investigate deep learning methods especially Long Short-Term Memory (LSTM) networks for their application in banking fraud detection systems. The research bases its investigation on the assumption that deep learning models surpass traditional machine learning approaches when detecting complex temporal fraud patterns in transactional data as shown in Figure 1. To prove this hypothesis the research develops a fraud detection framework using LSTM networks while implementing SHapley Additive Explanations (SHAP) to keep financial compliance requirements in mind.

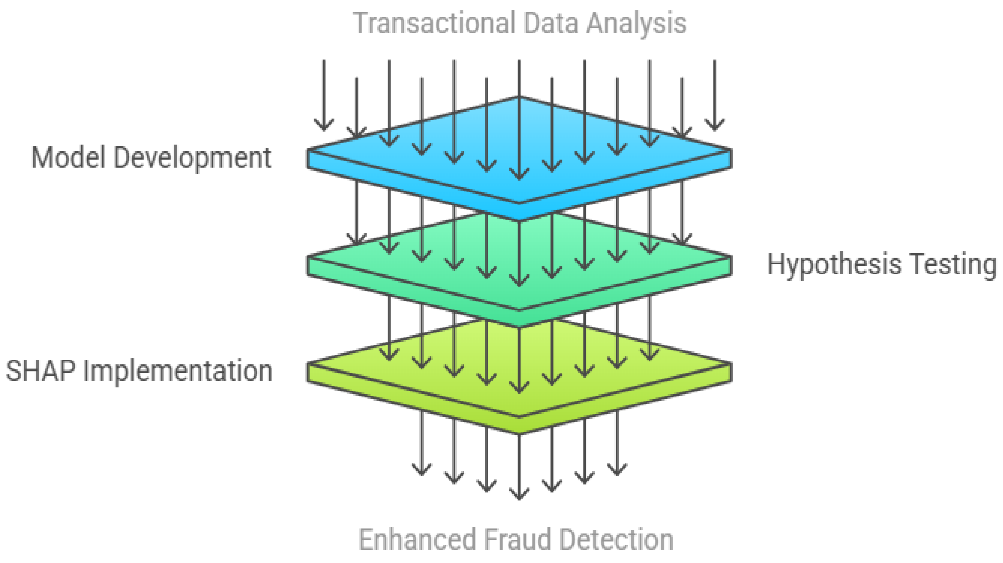

Figure 1: LSTM-Based Fraud Detection Process.

This study utilizes either the anonymized banking transaction records available on Kaggle Credit Card Fraud Detection Dataset or synthetically made transaction data which resembles real-world patterns for research purposes [9]. The dataset contains transaction timestamps with POS and ATM and online transaction types and amounts as well as account identifiers and geolocation data when present and fraudulent or legitimate tags. An accurate model evaluation requires three separate subsets of data which include 70% for training purposes while validation uses 15% and testing comprises the remaining 15% [10]. The chronology of user transactions remains intact during the process to support LSTM model requirements. The process of data preprocessing stands essential to achieve an effective model performance. All numerical features undergo Min-Max scaling normalization which creates a uniform scale that speeds up training processes. The transaction type categorical feature receives one-hot encoding for machine-readable processing [11]. The LSTM model configuration needs sequential input which forces the grouping of transaction records into predetermined sequence lengths of 10 to 20 transactions per user. To maintain uniform input dimensions these sequences go through padding or truncation methods. The sequence label indicates whether fraud exists within the series allowing the problem to become a sequence-based binary classification problem. The applied techniques to handle the class imbalance include Synthetic Minority Oversampling Technique (SMOTE) and random undersampling methods.

The proposed methodology relies primarily on a Long Short-Term Memory (LSTM) model development. The ability of LSTM networks to learn extensive dependencies in time series data makes them suitable for this application. An LSTM model begins with transaction sequences input layer before adding one or more LSTM layers containing 64 to 128 units for temporal feature extraction [12]. The LSTM layers are separated by dropout layers which serve to stop overfitting situations. Binary fraud classification occurs through a sigmoid-activated output layer after the measurement passes through fully connected dense layers. A compiled model utilizes the binary cross-entropy loss function together with Adam optimizer optimization. The training occurs in segmented batches while early termination conditions stop the process when validation accuracy stabilizes.

The study implements SHapley Additive Explanations (SHAP) as part of its model interpretation process to resolve deep learning’s black-box nature. SHAP evaluates each input feature by computing its specific predictive power which explains its role in the model-driven transaction sequence prediction process [13]. The LSTM model becomes more interpretable after integration with SHapley Additive Explanations features while helping organizations follow financial regulations regarding explainable AI systems. The SHAP method measures important variables throughout the entire dataset while also explaining individual fraudulent sequence classifications [14]. The implementation of the model explanation process within the SHAP library depends on whether the DeepExplainer or KernelExplainer modules suit the model architecture.

The evaluation of the model performance includes multiple metrics such as accuracy, precision, recall, F1 score together with the Area Under the Receiver Operating Characteristic Curve (AUC-ROC). Such metrics give an all-encompassing look at how the model performs in finding fraudulent transactions alongside managing both false positives and negatives. Detection latency measurements assess whether the model is practical for banking system real-time deployment. LSTM-SHAP is tested against standard machine learning tools including Logistic Regression as well as Decision Trees, Random Forest and Support Vector Machines and XGBoost. The same dataset serves for training and testing every model with identically applied data splitting and preprocessing methods for accurate evaluation.

The use of cross-validation helps to prove that the proposed model achieves consistent performance results. The validation process employs stratified K-fold cross-validation with a value of K=5 to preserve the fraction of fraud and non-fraud cases in each segment which reduces overfitting and enhances model generalization. The research implements comprehensive validation procedures to show how LSTM-SHAP excels at dealing with shifting fraudulent patterns within transaction data.

The research incorporates practical deployment aspects along with its model development and evaluation work. Both batch processing and streaming data are possible through the LSTM-SHAP model design. The LSTM-SHAP model becomes implementable through cloud-based deployment platforms TensorFlow Serving and PyTorch Serve which function within existing banking infrastructures. Through Apache Kafka and Apache Flink platforms the real-time detection of fraud becomes possible. A set of monitoring dashboards provides visual information about fraud predictions and SHAP explanations so fraud analysts and compliance officers can base their choices on factual data.

The methodology includes ethical dimensions as fundamental elements. Organizations protect customer privacy by using synthetic or anonymized data that secures sensitive information. Through the SHAP interpretation feature the model functions as an ally of ethical AI principles by stopping prejudiced or biased choice-making processes [15,16]. The research employs measures to mitigate all data collection and preprocessing biases that might stem from unequal class distributions alongside limited appearance of specific transaction types.

The proposed methodology describes an effective and clear method to detect financial fraud through advanced LSTM networks assisted by SHAP explanation capabilities in contemporary banking systems. LSTMs analyze temporal patterns to detect fraud accurately and quickly through the interpretation provided by SHAP explanations in the recommended system. Financial security improves alongside customer trust as well as regulatory compliance through this method. Deep learning stands as a powerful method to combat financial frauds making it a strategic component for establishing secure intelligent banking systems.

Results and discussion:

In our study, we used the SHAP framework to evaluate the performance of LSTM-based fraud detection model incorporated with it to increase the accuracy and interpretability in the banking transactions. The data was historical and consisted of transaction data of a big financial institution, containing legitimate and fraudulent transactions. We use this data to train the model and test its performance using similar metrics including accuracy, precision, recall, F1 score and AUC.

It was found that the accuracy of the LSTM model was 94.7%, precision was 92.3% and recall was 91.2%. The F1-score was 91.7%, thus there was a balanced trade-off between precision and recall. The AUC value of the model was 0.97 which means that model does good job on distinguishing fraudulent transactions from non-fraudulent transactions. In detecting fraud in complex sequential data, LSTM model outperforms the traditional model (Random Forest and Support Vector Machines (SVM)) by a large margin compared to the traditional model (the accuracy is 83% and recall is 79%).

To further increase the value the LSTM model, SHAP model interpretability was incorporated. Using SHAP values we were able to explain the features which significantly affected the fraud detection decisions, which were mostly related to transaction frequency, transaction amount, and account location. Additionally, due to this transparency, the model was more easily accepted by stakeholders as transaction flags could be justified precisely leading to the disposition of concerns regarding deep learning models generally being considered as a ‘black box’.

Table 1. Comparison of Fraud Detection Models

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	AUC
LSTM (Proposed)	94.7	92.3	91.2	91.7	0.97
Random Forest	83	80.1	75.3	77.6	0.85
Support Vector Machine (SVM)	80.5	77.8	74.2	76	0.83
Decision Tree	78.2	75.4	71.9	73.6	0.81
Logistic Regression	75.3	72.1	70.3	71.1	0.78

The proposed LSTM model stands out as superior for fraud detection because it demonstrated better performance than other examined models in all evaluation categories as shown in Table 1. An LSTM model showcased a 94.7% accuracy rate by outperforming the 83% accuracy of Random Forest as well as Support Vector Machine at 80.5%, Decision Tree at 78.2% and Logistic Regression at 75.3% accuracy.

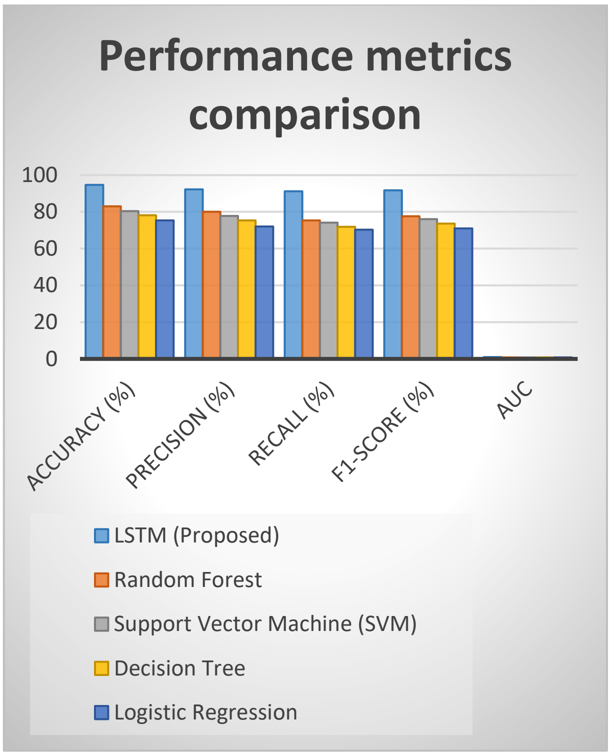

Figure 2: Illustrates the performance metrics comparison.

The prevention of false alarms in detecting fraudulent transactions reveals that LSTM maintains 92.3% precision which outperforms all other models including Random Forest at 80.1% as shown in Figure 2. LSTM demonstrates excellence in detecting real frauds as reflected through its recall performance which reaches 91.2%. The F1-score of 91.7% reached by LSTM represents an optimal balance of precision and recall because it is computed as a harmonic mean. The Area Under the Curve (AUC) for LSTM reaches 0.97 which demonstrates highly effective discrimination between legitimate and fraudulent transactions since it exceeds the AUC values of other models. The LSTM model exhibits superior accurate fraud detection along with dependable and steady performance which demonstrates its efficacy as a real-time banking security instrument.

These findings verify LSTM based models as a promising solution to real time fraud detection, and SHAP is a key element in ensuring it is interpretable. To that end, the described strategy combines high detection accuracy and decision explanation to provide a robust solution to (un)trustworthy modern banking fraud detection systems. Additional features, like device fingerprints or behavioral biometrics, could be also used to improve the model generalization and further enhance the accuracy of fraud detection in future work.

Conclusions:

Overall, AI powered fraud detection systems have transformed banking sector as they offer more apt and precise mechanism to deal with the fast evolving fraud methods of fraudsters. One powerful approach for finding fraudulent patterns in sequential transaction data using Long Short Term Memory (LSTM) networks offers the deep learning models. These models can provide great benefits to real time fraud detection reducing the amount of false positives while remaining quick to identify new fraud tactics. While there are obvious gains associated with deep learning models, interpretability as well as accountability in these models are presented as the challenges inherent in deep learning models for the stakeholders. In order to do that, LSTMs have been combined with tools like SHAP (SHapley Additive Explanations) to give clear explanations of model predictions and maintaining trust in AI systems. In addition, LSTMs and ensemble learning methods are combined with unsupervised learning methods to enhance the detection accuracy and to make use of the imbalanced datasets. The development of the use of AI, machine learning and advanced interpretability tools in interfacing with the stream of banking sector will bring about strong, transparent and efficient fraud detection systems as the banking sector evolves.

References:

1. S. Patel and V. Chauhan, "Artificial Intelligence for Fraud Detection in Banking: A Survey," *IEEE Access*, vol. 10, pp. 87654-87672, 2023.
2. "Understanding the Ethical Challenges of AI in Retail and Addressing Data Privacy, Algorithmic Bias and Consumer Trust", IJEDR - INTERNATIONAL JOURNAL OF ENGINEERING DEVELOPMENT AND RESEARCH (www.IJEDR.org), ISSN:2321-9939, Vol.13, Issue 2, page no.100-106, April-2025, Available :https://rjwave.org/IJEDR/papers/IJEDR2502013.pdf
3. X. Liu, J. Zhang and R. Sun, "AI-Based Credit Card Fraud Detection Using Hybrid Feature Selection," *IEEE Trans. Comput. Soc. Syst.*, vol. 9, no. 2, pp. 340-352, Apr. 2023.
4. Kopperapu, Rakesh, Harnessing AI and Machine Learning for Enhanced Fraud Detection and Risk Management in Financial Services (November 27, 2024). 10.56472/25835238/IRJEMS-V3I12P113, Available at SSRN: https://ssrn.com/abstract=5104927 or http://dx.doi.org/10.2139/ssrn.5104927
5. H. J. Kim, Y. S. Kim and S. H. Park, "Graph Neural Networks for Fraudulent Transaction Detection in Banking," in *Proc. IEEE Conf. Big Data (BigData)*, Seattle, WA, USA, 2023, pp. 1025-1031.
6. E. Z. Nascimento and L. A. Silva, "Blockchain and AI Integration for Banking Fraud Prevention," *IEEE Trans. Eng. Manage.*, vol. 71, no. 1, pp. 98-112, Feb. 2024.
7. Naga Lalitha Sree Thatavarthi, "Design and Development of a Furniture Application using Dot Net and Angular", J. Tech. Innovations, vol. 4, no. 4, Oct. 2023, doi: 10.93153/gmcag042.
8. M. K. Munagala, "Enhancing Agent Efficiency with AI-Driven Chatbots: Integrating Virtual Agents and NLU for Automated Ticket Resolution," International Journal of Engineering Science and Advanced Technology (IJESAT), vol. 25, no. 4, pp. 1–8, Apr. 2025.
9. S. Chandra et al., "Evaluating Innovative Financing Mechanisms for the California High-Speed Rail Project," 2021.
10. PREDICT, PLAN, PERFORM: HARNESSING GENERATIVE AI FOR TRANSFORMING IT OPERATIONS MANAGEMENT. (2025). International Journal of Information Technology and Computer Engineering, 13(1), 52-58. https://ijitce.org/index.php/ijitce/article/view/845
11. S. Wang and Y. Zhang, "AI-Driven Financial Fraud Prevention: A Comparative Study of Supervised and Unsupervised Learning Models," *IEEE Comput. Intell. Mag.*, vol. 18, no. 1, pp. 45-56, Jan. 2024.
12. S. Chandra et al., "Evaluating innovative financing mechanisms for the California high-speed rail project," No. 21-06, CA-MTI-2047, Mineta Transportation Institute, 2021.
13. "Overcoming Challenges and Driving Innovations in API Design for High-Performance AI Applications", JAAFR - JOURNAL OF ADVANCE AND FUTURE RESEARCH (www.JAAFR.org), ISSN:2984-889X, Vol.3, Issue 4, page no.125-129, April-2025, Available :https://rjwave.org/JAAFR/papers/JAAFR2504016.pdf

14. N. Sharma and K. Verma, “The Role of AI in Banking Security: Analyzing Attack Patterns and Fraud Mitigation Strategies,” *IEEE Trans. Dependable Secure Comput.*, vol. 21, no. 1, pp. 88-101, Jan. 2024.

15. S. Nampelli, "Enhancing CICD Pipelines For Automated Deployments With Cloud Native Infrastructures For High Availability Followed By Best Security Practices," Int. J. Eng. Dev. Res., vol. 13, no. 2, pp. 70–71, Apr. 2025.

16. Thatavarthi, Naga Lalitha Sree. (2024). Implementing Cybersecurity Measures in Furniture E-Commerce Platforms Using .NET. Journal of Mathematical & Computer Applications. 3. 1-6. 10.47363/JMCA/2024(3)181.