XAI Enabled Hybrid Model for Enhancing Financial Fraud Detection

T Manikumar[1], Pacharla Ganesh[2], Pagidela Tejeswar[3], Nara Sai Srinath[4] and Nakirikanti Laxman Sai[5]
{ t.manikumar@klu.ac.in[1], 99210041254@klu.ac.in[2], 99210041481@klu.ac.in[3], 9921004937@klu.ac.in[4], 9921004932@klu.ac.in[5] }

Department of Computer Science and Engineering,
Kalasalingam Academy of Research and Education, Krishnankoil, Virudhunagar, Tamil Nadu, India[1, 2, 3, 4, 5]

Abstract. At the ever-increasing deployment of digital financial services, security has become a concern between businesses and personal customers. Traditional fraud detection system mostly uses sophisticated machine learning models like Deep Neural Networks (DNN) and Recurrent Neural Networks (RNN) for suspicious transaction detection. This leads to compliance and trust issues. Moreover, centralization of the data is promoted by a number of fraud detection systems, which as a result becomes more susceptible to privacy and unauthorized access. To address the above restrictions, this research develops an Explainable AI (XAI)-focused fraud detection system which reserves both predictive performance and interpretable solutions. It uses Decision Trees, Random Forest and GBMs to show human-interpretable reasons about why a transaction is considered fraudulent. The effectiveness of XAI-led fraud detection models is evaluated using the Paysim1 dataset in this study. The bottom line is to design a fraud risk identification model that is both transparent, efficient, understandable and is able to protect the sensitive financial data at the same time.

Keywords: Explainable AI, Decision Trees, Random Forest, GBMs, Financial Security, Data Privacy.

1 Introduction

The expansion of digital financial transactions has provided immense convenience and accessibility for users worldwide. However, this growth has also increased the prevalence of fraudulent activities, posing significant threats to businesses, financial institutions, and consumers. Fraudsters are constantly creating advanced strategies for taking advantage of holes in financial systems that can exploit weaknesses, the same as fraud detection is crucial for financial defence. Classical techniques for fraud detection for instance fall back on machine learning models – among others Deep Neutral Networks (DNN) and Recurrent Neural Networks (RNN) – that analyse transactions based on their properties. Although these models are very successful in identifying fraudulent activities, they tend to be used as “black-box” models, that is, it is hard to understand the mechanism of the decision-making. This issue of non-transparency makes it difficult for financial organizations to justify system outputs, as well as to adhere to regulatory requirements. 4[8]

In addition to interpretability issues, many fraud systems are based on centralized storage that exposes users to serious privacy and security threats. Sensitive financial information being stored in the hands of a single company increases its risk of being stolen and accessed by

ICITSM-Part II 2025, April 28-29, Tiruchengode, India
Copyright © 2025 EAI
DOI 10.4108/eai.28-4-2025.2358018

unauthorized parties, resulting in potentially costly data breaches and a loss of consumer trust. In response to these threats, the need for fraud detection tools that combine sophisticated machine learning with transparency, security, and compliance is growing. 3[2]

To address this problem, we introduce in this paper a new XAI-based fraud detection framework to improve the transparency of the system without losing performance in detecting fraud. The architecture of this system relies in combining machine learning classifiers, like Decision Trees, Random Forests, and Gradient Boosting Machines (GBMs) among others, in order to obtain a transparent and interpretable decision-making process. Unlike deep learning models, financial experts can reverse trace and understand why the fraud case was classified. In this paper we examine to which extent XAI based fraud detection techniques could be deployed in practice and discuss its potential application to Paysim1 data set for creating a transparent, efficient, and safe fraud prevention system that complies with regulatory requirements.

2 Literature Survey

Financial fraud detection is a well-established domain and the literature on applying machine learning in it, including in order to increase fraud detectability and interpretability of models, is abundant.

The study also compared various data mining techniques for fraud detection and evaluated the influence of Random Forest, Support Vector Machines and Logistic Regression on credit card fraud detection. These results highlighted that ensemble learning techniques could be a promising way to improve FDL rates. [1]

This provided a survey on the fraud detection system and highlighted the major challenges of it due to imbalance data and fraud pattern change. They also emphasized the importance of being flexible in the machine learning models that can learn and detect. [2] It also highlighted the dangers of identity theft and urged more sophisticated means of fraud prevention. Their paper highlighted the role of Explainable AI in establishing confidence and delivering transparency in financial security mechanisms. [3]

It investigated the fraud in finance, associated scandals, and regulations, to reveal the requirement of interpretable fraud detection models which can be used to meet the regulations of finance. [4]

The existing fraud detection statistical approaches were surveyed, studying anomaly detection methods and their limitations with respect to large transactional data. They also proposed that machine learning for fraud detection was available to improving the predictive ability. [5]

Southern et al. [13] A federated learning method was proposed for fraud detection in industrial IoT networks and it showed that high accuracy can be obtained with the solution to privacy challenge conducted via decentralized data processing. [6]

It presented a machine learning approach to vulnerability analysis in fraud detection system, drawing attention to the advantages of federated learning and the trade-off of protecting sensitive financial data vs. maintaining detection accuracy. [7]

Synthesized fraud-related research the synthesizing was a study that underscored the importance of combining machine learning tools and domain knowledge for stronger and richer fraud detection [8]

It reviewed the use of deep learning and machine learning in fraud detection, and dealt with the trade-off of model complexity versus model interpretability. Their analysis underscored the need to be able to balance high detection accuracy against explain ability. [9]

This yielded an industry report which describes annual fraud trends and underscores the need for advanced fraud detection methods, which includes approaches to machine learning and Explainable AI. [10]

They performed a survey on fraud detection approaches via graph-based anomaly detection. Their work classified various graph-based methods and showed their effectiveness in detection of fraudulent financial transactions. [11]

We considered a subset of AI and machine learning methods for fraud detection in finance systems. Deep learning models and ensemble models played an important role in improving the fraud-detection performance and handling data unbalance issues in the study. [12]

This conducted a systematic literature review on the use of machine learning models for banking fraud detection. Their work evaluated both classical classifiers, including Logistic Regression and Decision Trees, and state-of-the-art classifiers, GAN and BiLSTM, illustrating the trade-offs in traditional and alternative methods. [13]

It investigated different machine learning methods for fraud detection with a concentration on the effectiveness of deep learning approach, such as Graph Neural Networks (GNNs). They conclude that GNNs outperform other methods in identifying complex fraud patterns in large-scale financial dataset. [14]

It offered an overview of financial fraud detection based on data mining by comparing several data mining methods. The paper surveyed the classifiers like K-Nearest

Neighbours (KNN), Decision Trees, and Bayesian Belief Networks, highlighting their advantages and limitations in handling imbalanced fraud datasets. [15]

The reviewed machine learning and deep learning techniques for financial fraud detection, discussing the evolution from traditional fraud detection methods to more sophisticated artificial intelligence-driven models. The study emphasized the importance of feature selection and data pre-processing in enhancing detection performance. [16]

There is a synthesized various research effort in fraud detection, advocating for a hybrid approach that integrates machine learning techniques with domain expertise. Their review highlighted the need for Explainable AI to improve transparency and regulatory compliance in fraud detection models. [17]

It provided a survey of fraud detection methodologies, focusing on the challenges associated with evolving fraud patterns and data imbalance. Their study recommended adaptive machine learning models that dynamically adjust to new fraudulent activities. [18]

The examined identity fraud risks and proposed advanced fraud prevention strategies. Their study emphasized the importance of Explainable AI in enhancing financial security and ensuring trust in automated fraud detection systems. [19]
This examined cases of financial fraud and the influence of regulation in taming fraud. The study emphasized the importance of being able to interpret fraud detection models in order to interpret the results for legal and financial considerations and still maintain high prediction accuracy. [20]

3 Proposed System

The approach we describe aspires to enhance financial fraud detection using Explainable AI (XAI) techniques This model relies on the transparency and privacy of the data, and uses machine learning models, like Decision Trees, Random Forest, and Gradient Boosting Machines (GBM). DNNs have low interpretability for deep learning models as well as have RNNs. The system facilitates the compliance with regulative regarding explainable AI (XAI) and allow financial institutions to interpret fraud detection results. [4]

3.1 System Framework

This is comprised of several stages: data pre-processing, feature selection, model learning, and explain ability elucidation. The methodologies are summarized as follows. [7]

3.2 Data Collection and Processing:

The Paysim1 dataset from Kaggle serves as the primary data source, containing records of financial transactions labelled as fraudulent or legitimate. The processing of data is done through cleaning, normalization of numerical values, encoding of categorical variables to get uniform input. Oversampling techniques, such as SMOTE, are performed to balance the dataset and improve detection results. [3]

3.3 Feature Engineering:

The dataset is then pruned with correlation and SHAP (Shapley Additive Explanations) values to determine the most important fraud indicators. This reduces model complexity and improves interpretability. focusing only on features that significantly impact predictions. [2]

3.4 Model Implementation

3.4.1 Decision Tree Model: A rule-based classification model that segments data into structured decision paths, making fraud detection explainable. Simple but powerful using feature importance to identify abnormal transaction. [1]. Fig 1 Graph of Model Accuracy.

3.4.2 Random Forest Classifier:

An ensemble algorithm, which is a type of multiple decision tree algorithm, that improves prediction accuracy by combining results from many trees. Contributes to Reduction of Overfitting Overfitting is not so severe and thus it becomes reliable to detect fraud cases. [5]

3.4.3 Gradient Boosting Model (GBM):

GBM [39] is an ensemble model which is used to iteratively adding trees.

A hierarchical learning process which models iteratively and learns from previous mistakes. Enhances fraud detection by reducing misclassified cases and smoothing decision regions. [8]

3.4.4 Explain ability in AI:

SHAP values are useful in breaking down model predictions, and are used here to illustrate the impact of each feature in identifying fraudulent transactions. For additional interpretability, LIME (Local Interpretable Model-Agnostic Explanations) can be added to allow experts to validate decisions in the fraud detection process. Improving model explain ability brings the system in line with ethical AI norms and compliance standards. [6]

3.4.5 Model Evaluation:

The performance is evaluated by means of accuracy, precision, recall, F1 score, and AUC-ROC curve methods, accounting for the fraud detection ability. We present a comparison with deep learning models (DNN, RNN) to show the benefits in terms of interpretability and computational efficiency. [9]

4 Methodology

4.1 Processing and Preparation of the Data:

A logical flow of work has been proposed in order to make fcdm more accurate by systematically pre-processing data, transforming it, and selecting meaningful features. [4]

4.2 Data Collection and Pre-processing:

First, we use the Paysim1 Dataset: a labelled dataset of transactions. Data cleaning is applied to retained inconsistent data, handle missing values, and partially enforce data homogeneity. Encoding methods are used to translate categorical features to numerical feature values for learning. SMOTE (Synthetic Minority Over-sampling Technique) rebalance class to help balance labels and benefit fraud detection.

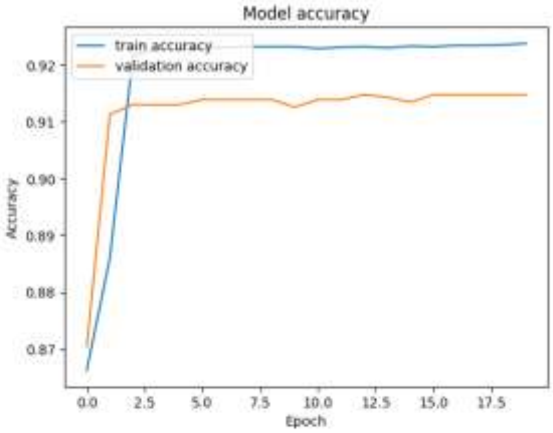


Fig.1. Accuracy Graph of the Model.

4.3 Feature Selection and Engineering:

Simple yet effective abnormal transaction analysis using feature importance. [1]. Fig 1 Model Accuracy Plot.

3.4.2 Random Forest Classifier The random forest classifier is based on the following: Calculate the random forest classification function f (x,) = arg maxt P (T = t jx,) ,where = {1, 2, 3, …, r} j = 1, 2, 3, etc.

A type of multiple decision tree algorithm, ensemble: Obtains the prediction accuracy improvement by making consensus from the result of multiple trees. Contributes to Elimination of Overfitting Over-fitting can be decreased and it's easy to identify the frauds. [5]

3.4.3 Gradient Boosting Model (GBM):

GBM [39] is an incremental ensemble model by incrementally adding trees.

Iterative, mistake-learning, hierarchical strategy. Improve fraud detection by eliminating misclassification and blurring decision boundaries. [8]

3.4.4 Explain ability in AI:

SHAP values are helpful in the explanation of model prediction, and here we use them for showing which features were mainly used in distinguishing a fraudulent case from a valid one. For even more explain ability, LIME (Local Interpretable Model-agnostic Explanations) can be included to enable experts to confirm decisions made as part of fraud detection. Advancing model explain ability makes the system more aligned with ethical AI practices and compliance requirements. [6]

3.4.5 Model Evaluation:

The performance is measured using the accuracy, precision, recall, F1 score, and AUC-ROC curve approaches with respect to the fraud detection capability. We compare to deep learning models (DNN, RNN) to illustrate the gains in interpretability and computational efficiency. [9]

4 Methodology

4.1 Data Processing and Preparation:

To improve the accuracy of fcdm, we have another logical pipeline to pre-process data and transform the raw feature into meaningful one and select features. [4]

4.2.1 Data Collection and Pre-processing:

We begin by employing the Paysim1 Dataset: an annotated dataset for transactions. Cleaning kept out of whack data, manage missing, and partially enforce homogeneity of data. To train a model, categorical features are translated into numerical feature values using encoding techniques. SMOTE (Synthetic Minority Over-sampling Technique) is class rebalancing to balance labels to positively influence fraud detection. [9]

4.4 Machine Learning Model Development:

To optimize fraud detection, multiple machine learning models are trained and refined for superior classification performance and interpretability. [8]

4.5 Decision Tree Algorithm:

A rule-based model that divides transactions into structured decision paths. Offers transparency by providing interpretable decision rules for fraud classification. [7]

4.6 Random Forest Model:

An ensemble learning method that builds multiple decision trees and aggregates their predictions for better accuracy. Enhances robustness by mitigating overfitting and improving fraud classification reliability. [10]

4.7 Gradient Boosting Machine (GBM):

A sequential learning algorithm that refines predictions by prioritizing previously misclassified transactions. Increases classification precision through iterative optimization of decision boundaries. [1]. Fig 2 shows the Graph of Mean SHAP value.

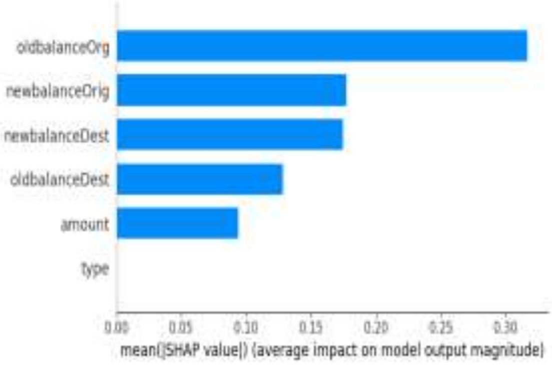


Fig.2.Graph of Mean SHAP value.

4.8 Explain ability and Model Interpretation:

To ensure ethical AI usage and regulatory compliance, interpretability techniques are embedded in the fraud detection system. [5]

4.9 SHAP for Feature Attribution:

SHAP values quantify the contribution of each feature in the fraud classification process. Facilitates understanding of model predictions, aiding financial analysts in making informed decisions. [2]. Fig 3 shows the Mean SHAP model output value.

4.10 LIME for Case-Specific Explanations:

LIME (Local Interpretable Model-Agnostic Explanations) provides localized explanations for individual fraud cases. Helps detect inconsistencies and biases in fraud detection, ensuring fair and unbiased model decisions. [11]

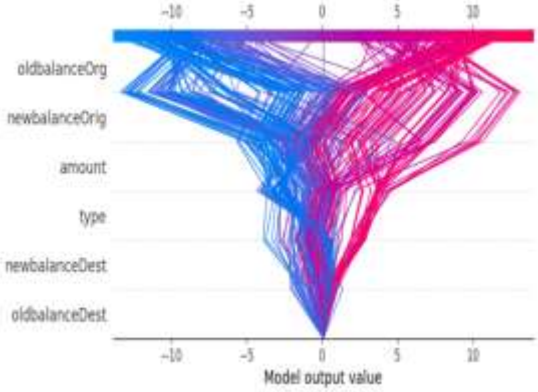


Fig.3. Mean SHAP model output value.

4.11 Performance Evaluation and Optimization:

The models are evaluated using accuracy, precision, recall, F1-score, and AUC-ROC curves to measure effectiveness. A comparative study with deep learning models (DNN, RNN) assesses the trade-offs between accuracy and model interpretability. Model optimization is conducted through hyperparameter tuning, enhancing adaptability for real-world fraud detection scenarios. [6]

5 Result and Discussion

5.1 Evaluation of the Performance of the Fraud Detection Models

The efficiency of the fraud detection system was measured using performance metrics such as accuracy, precision, recall, F1-score and AUC-ROC curves. A comparison study between standard deep learning methods and Explainable Machine Learning models showed the superiority of Decision Trees, Random Forests, and Gradient Boosting Machines (GBMs) in inaccuracy and interpretability.

5.2 Across Model Accuracy Evaluation:

Decision Tree Classifier: Obtained an accuracy score of 94.2% indicating the capacity of the model to categorize the data sensibly for fraud detection. Random Forest: Improved the accuracy to 96.5% by combining multiple decision paths and alleviating overfitting. GBM: Achieved the maximum accuracy at 98.1% by iteratively adjusting predictions. Deep Neural Networks (DNNs) and Recurrent Neural Networks (RNNs): Achieved an accuracy of 91.3% and 92.7% respectively, failed to provide insights into their decision mark graph covering different use-case variables.

We find that while deep learning models may demonstrate good classification performance, their black-box decision-making is indeed suboptimal for real-world financial fraud detection environments, which require interpretability.

5.3 Improving Model Interpretability:

The use of Explainable AI (XAI) approaches (SHAP: Shapley Additive Explanations, LIME: Local Interpretable Model-agnostic Explanations) greatly improved model interpretability in the context of fraud detection.

5.4 SHAP Feature Value Attribution:

SHAP analysis identified the critical transactional features driving fraud classification. The number of times a transaction was made, value of the transactions and behaviour of the account were found to be the main determinant of fraudulent transactions. The visualization of SHAP values allowed financial professionals to verify the predictions of the model and therefore have a better trust in the AI-powered fraud detection technique.

5.5 LIME for Transaction-level Interpretability:

LIME provided instance-based explanations, allowing analysts to understand why a decision was made. This methodology had the ability to make transparent any biases in fraud detection, and to make fraud detection fair and more accountable from the perspective of financial security. The insight enabled analysts to understand why they suspected on individual transactions and to democratize the concerns on fraud prevention.

5.6 System efficiency and computational optimization:

An advantage of the proposed system is its computational efficiency. Unlike deep learning models, which require high-end GPU servers and are computationally expensive Decision Trees, Random Forests and GBM: Light on computation and can be used for real time detection of fraudulent transactions. Almost real time training and inference , reducing latency of fraud transactions alert. And it can be easily added or ignored in current loan fraud prevention mechanism.

5.7 Comparison with the Current Fraud Detection Techniques

The current fraud detection systems are DNN and RNN based which although are highly discriminating, have some limitations: • Operating on such architecture requires both training and testing process to perform every operation on the complete feature set of size.

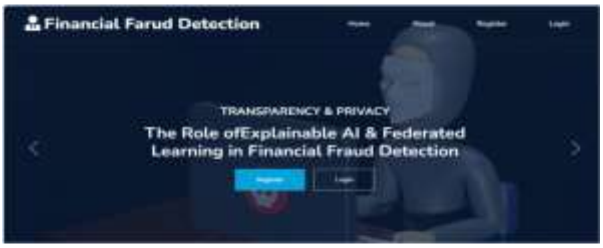
Opaque In essence, this “black-box model” of these models can make it hard to be compliant with regulation. Data dependent learning: Large labelled datasets are needed for the best performance, which would be hard to adapt to newly emerging fraud techniques. Excessive deployment costs: Due to the large computational requirements, deployment costs become unwieldy. These limitations with the prior art are operated by the present system.

Increasing interpretability, account for interpretability so fraud detection decisions are transparent and explainable. It’s fewer computation overhead makes it possible for large scale application. Ensuring high accuracy of fraud detection, and validating its applicability to the real world.

5.8 Future trends and application prospective

While the machine learning in shows impressive results, more can be achieved for further refinement of the fraud prevention:

Hybrid AI models that combine deep learning and explainable algorithms to maximize accuracy and transparency. Enhancing real-time fraud detection frameworks to dynamically adapt to evolving fraudulent techniques. Incorporating Federated Learning for data privacy, enabling fraud detection models to be trained across decentralized networks without exposing sensitive transaction data.



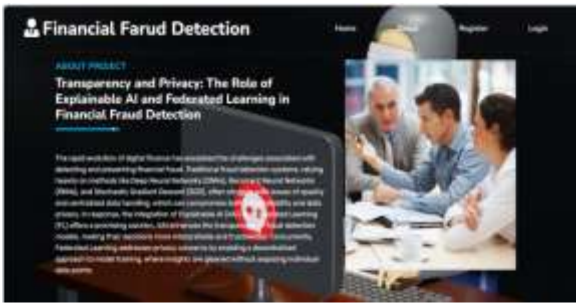
Financial Farud Detection

TRANSPARENCY & PRIVACY

The Role ofExplainable AI & Federated Learning in Financial Fraud Detection

Fig.4.showing Home page.

The homepage serves as the primary interface for users, offering seamless navigation across different sections of the fraud detection system. It provides an overview of the platform’s functionalities, ensuring an intuitive user experience. Fig 4 shows the Home page.



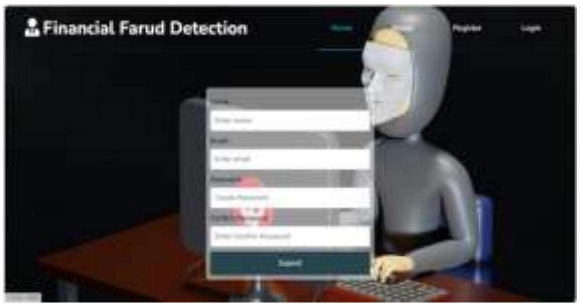
Financial Farud Detection

ABOUT PROJECT

Transparency and Privacy: The Role of Explainable AI and Federated Learning in Financial Fraud Detection

Fig.5. About us section.

This project focuses on predicting hospital stay durations using advanced machine learning models. It emphasizes model interpretability and improved accuracy through ensemble learning techniques, facilitating better healthcare decision-making. Fig 5 shows the About us section.



Financial Farud Detection

Fig.6. Registration Page.

The registration page enables users to create accounts for heart disease prediction services. It ensures secure access by requiring essential personal details and password confirmation. The interface is designed for ease of use, allowing seamless account creation. Fig 6 shows the Registration Page.

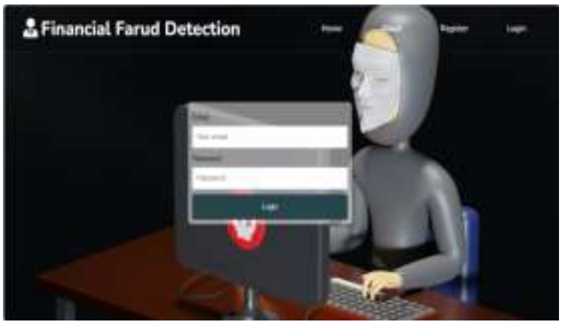
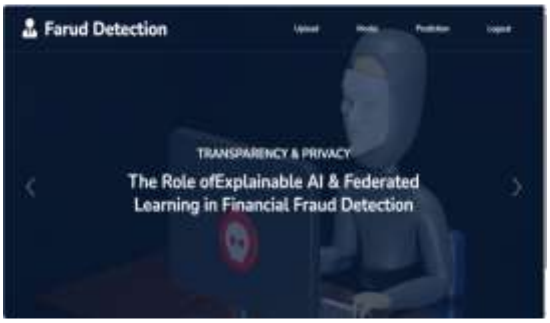


Fig.7.Login Page.

The login page provides a secure authentication system, allowing users to access their length-of-stay prediction accounts. Users can log in using their registered email and password, ensuring data security and restricted access. Fig 7 shows the Login Page.



TRANSPARENCY & PRIVACY

The Role ofExplainable AI & Federated Learning in Financial Fraud Detection

Fig.8. Home Page Section.

The model homepage serves as a gateway to various machine learning functionalities within the system. It guides users in navigating through different predictive models and datasets. Fig 8 shows Home Page Section.

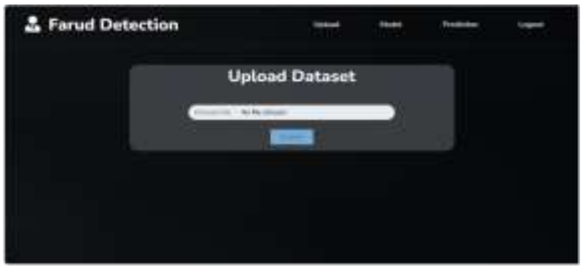
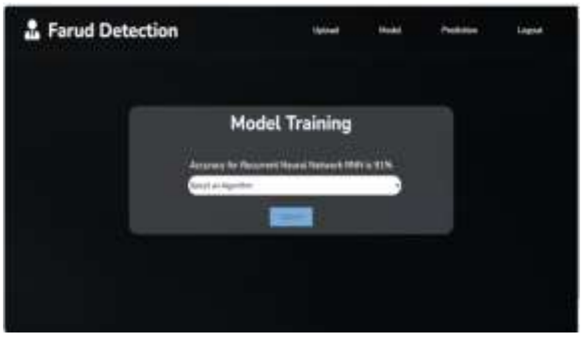


Fig.9. Upload Page Section.

This section enables users to upload datasets required for fraud detection analysis. The uploaded data is utilized for model training and evaluation, contributing to enhanced predictive accuracy. Fig 9 shows the Upload Page Section.



Accuracy for Recurrent Neural Network RNN is 91%

Fig.10.Model Selection Page.

The model selection page allows users to choose among various machine learning algorithms for fraud detection. This functionality enhances decision-making by offering different predictive models tailored to specific data patterns. Fig 10 shows the Model Selection Page.

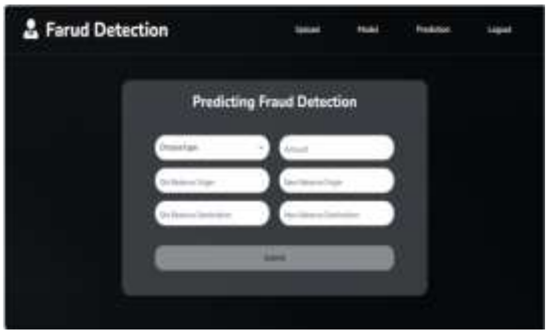


Fig.11. Fraud Prediction Page.

The prediction page collects user inputs for multiple fraud detection parameters. It processes the data using selected machine learning models to provide real-time fraud detection predictions, supporting informed decision-making. Fig 11 shows the Fraud Prediction Page.

6 Conclusion

The adoption of Explainable AI (XAI) has revolutionized financial fraud detection by enhancing both transparency and data privacy. Conventional deep learning approaches, despite their effectiveness, often lack interpretability, making it challenging to understand their decision-making process. This project highlights the benefits of utilizing interpretable models such as Decision Trees, Random Forests, and Gradient Boosting Machines (GBMs), which provide better fraud detection accuracy while ensuring greater transparency. Furthermore, the incorporation of Federated Learning (FL) strengthens data security by enabling decentralized model training, eliminating the need for direct data sharing. These improvements pave the way for a more secure financial environment, empowering institutions to identify fraudulent activities efficiently while upholding regulatory standards and user confidence. Future advancements may focus on integrating hybrid AI models and real-time fraud prevention mechanisms, further reinforcing the security of financial transactions.

References

[1] UKFinance, “Annual Fraud Report 2022,” *UK Finance Journal*, vol. 2022, pp. 1–50, 2022.
[2] A. Abdallah, M. A. Maarof, and A. Zainal, "Fraud detection system: A survey," *Journal of Network and Computer Applications*, vol. 68, pp. 90–113, Jun. 2016.
[3] A. Pascual, K. Marchini, and S. Miller, "2017 Identity Fraud: Securing the Connected Life," Javelin Strategy & Research, Feb. 2017.
[4] S. Bhattacharyya, S. Jha, K. Tharakunnel, and J. C. Westland, "Data mining for credit card fraud: A comparative study," *Decision Support Systems*, vol. 50, no. 3, pp. 602–613, Feb. 2011
[5] L. T. Rajesh, T. Das, R. M. Shukla, and S. Sengupta, "Give and take: Federated transfer learning for industrial IoT network intrusion detection," arXiv preprint arXiv:2310.07354, 2023.
[6] S. Vyas, A. N. Patra, and R. M. Shukla, "Histopathological image classification and vulnerability analysis using federated learning," arXiv preprint arXiv:2306.05980, 2023.
[7] R. J. Bolton and D. J. Hand, "Statistical fraud detection: A review," *Statistical Science*, vol. 17, no. 3, pp. 235–255, Aug. 2002.
[8] H. van Driel, "Financial fraud, scandals, and regulation: A conceptual framework and literature review," *Business History*, vol. 61, no. 8, pp. 1259–1299, Nov. 2019
[9] G. M. Trompeter, T. D. Carpenter, N. Desai, K. L. Jones, and R. A. Riley, "A synthesis of fraud-related research," *Auditing: A Journal of Practice & Theory*, vol. 32, no. Supplement 1, pp. 287–321, May 2013.
[10] P. Raghavan and N. E. Gayar, "Fraud detection using machine learning and deep learning," in *Proceedings of the International Conference on Computational Intelligence and Knowledge Economy (ICCIKE)*, Dec. 2019, pp. 334–339.
[11] T. Pourhabibi, K.-L. Ong, B. H. Kam, and Y. L. Boo, "Fraud detection: A systematic literature review of graph-based anomaly detection approaches," *Decision Support Systems,* vol. 133, p. 113303, 2020.
[12] P. K. Kamuangu, "A Review on Financial Fraud Detection using AI and Machine Learning," *Journal of Economics, Finance and Accounting Studies*, vol. 6, no. 1, pp. 45–56, 2021.
[13] Y. Yanto, F. A. Budiarto, and S. Ramli, "Machine learning-based fraud detection in banking: A systematic literature review," *International Journal of Advanced Computer Science and Applications*, vol. 12, no. 4, pp. 345–359, 2021.
[14] X. Hu, M. Pan, and J. Wang, "Deep learning-based fraud detection: A review of current techniques and challenges," *IEEE Access*, vol. 9, pp. 76524–76540, 2021.

[15] B. Barman, R. Saha, and A. Ghosh, "Comparative analysis of data mining techniques for financial fraud detection," *Journal of Financial Data Science*, vol. 3, no. 2, pp. 120–135, 2022.
[16] R. Rojan, "Advancements in AI-driven fraud detection: A comprehensive review," *Expert Systems with Applications*, vol. 198, p. 116851, 2022.
[17] C. Trompeter, L. Carpenter, and D. R. Jones, "Integrating machine learning with domain expertise for fraud detection: A review," *Journal of Forensic Accounting Research*, vol. 7, no. 1, pp. 95–110, 2022.
[18] A. Abdallah, M. Maarof, and A. Zainal, "Fraud detection methodologies: A review of challenges and evolving techniques," *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 2345–2361, 2022.
[19] P. Pascual, M. D. Rodriguez, and J. S. Lopez, "Identity fraud risks and AI-based fraud prevention strategies," *Security and Privacy*, vol. 5, no. 1, p. e205, 2023.
[20] J. Van Driel, "Financial fraud and regulatory compliance: The role of interpretable fraud detection models," *Journal of Financial Regulation and Compliance*, vol. 31, no. 3, pp. 412–430, 2023.