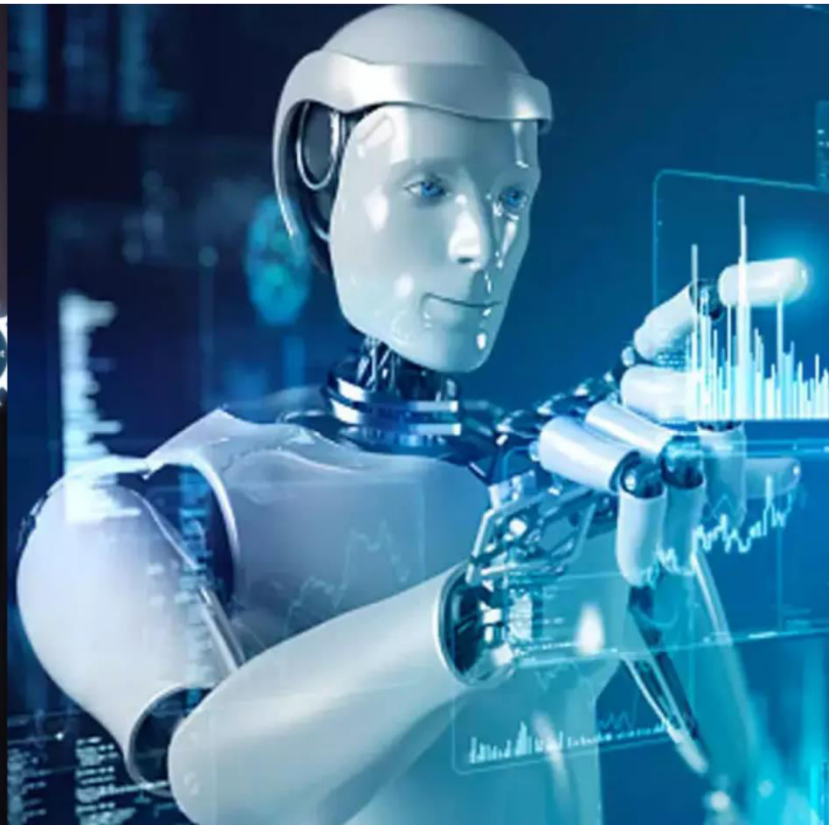
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

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

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



Impact Factor: 8.699

Volume 15, Issue 3, March 2026

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

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503102|

Explainable AI for Secure Analytics in Financial Sectors

Mrs. V. Vanaja[1], G. Chaitanya[2], V. Smaran[3], M. Omkar[4], E. Vamshi[5]

Assistant Professor, Department of CSE (Data Science), ACE Engineering College, Hyderabad, India[1]

IV B. Tech, Department of CSE (Data Science), ACE Engineering College, Hyderabad, India [2,3,4,5]

ABSTRACT: The rapid growth of digital financial services has significantly increased the volume of transactions, making financial fraud detection more complex. Traditional rule-based and conventional machine learning models often fail to detect evolving fraud patterns and usually lack transparency in their decision-making. To address this challenge, this project proposes a Secure Analytics framework using Explainable AI (XAI) for fraud detection. Using the IEEE-CIS Fraud Detection Dataset, the system applies the XGBoost algorithm to handle the issue of class imbalance and improve detection performance through feature engineering and data transformations, achieving around 95% accuracy and a ROC-AUC of about 0.80. The model integrates SHAP (SHapley Additive Explanations) to provide clear insights into how each feature influences predictions, allowing auditors to understand risk indicators such as unusual transaction amounts or device types. The system also ensures data security through anonymization and FastAPI-based backend communication, demonstrating that fraud detection systems can be both accurate, secure, and interpretable for modern banking and Financial Technological applications.

I. INTRODUCTION

The financial sectors generates massive amounts of data due to the rapid growth of digitalization of net-banking, online payments, and Financial services, leading institutions to rely heavily on artificial intelligence and machine learning for tasks such as fraud detection, risk assessment, and transaction analysis. While these models provide high predictive accuracy, many operate as black-box systems, offering little transparency into how decisions are made, which creates challenges related to trust, regulatory compliance, and accountability. At the same time, financial systems face increasing security threats such as fraud, cyber-attacks, and data breaches, making secure and reliable analytics essential. This project addresses these challenges by developing an Explainable AI (XAI)-based secure analytics framework that integrates machine learning with interpretability techniques to provide clear explanations for financial decisions. The system aims to improve transparency, identify key factors influencing predictions, support anomaly and fraud detection, and ensure secure data processing. By combining explainability with secure analytics, the project enhances trust, regulatory compliance, and decision confidence, demonstrating the practical application of interpretable AI in modern financial systems.

II. EXISTING SYSTEM

The existing financial analytics systems used by financial institutions rely on traditional machine learning and deep learning approaches to perform tasks such as fraud detection, transaction monitoring, credit risk assessment, and anomaly detection. Commonly used models include Logistic Regression, Decision Trees, Random Forests, Artificial Neural Networks (ANNs), Recurrent Neural Networks (RNNs), Long Short-Term Memory (LSTM), and Autoencoders, which analyze large volumes of historical transaction data to identify suspicious activities and reduce financial risk. Although these models improve prediction accuracy and help detect fraudulent patterns, they still face several limitations. Most models function as black-box systems and lack explainability, making it difficult to understand why certain transactions are flagged. They also suffer from high false positive rates, issues with handling imbalanced datasets where fraud cases are rare, and difficulties in meeting regulatory requirements that demand transparent decision-making. Additionally, some rule-based and batch-processing systems fail to detect fraud in real time, which can delay response and increase financial losses.

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

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

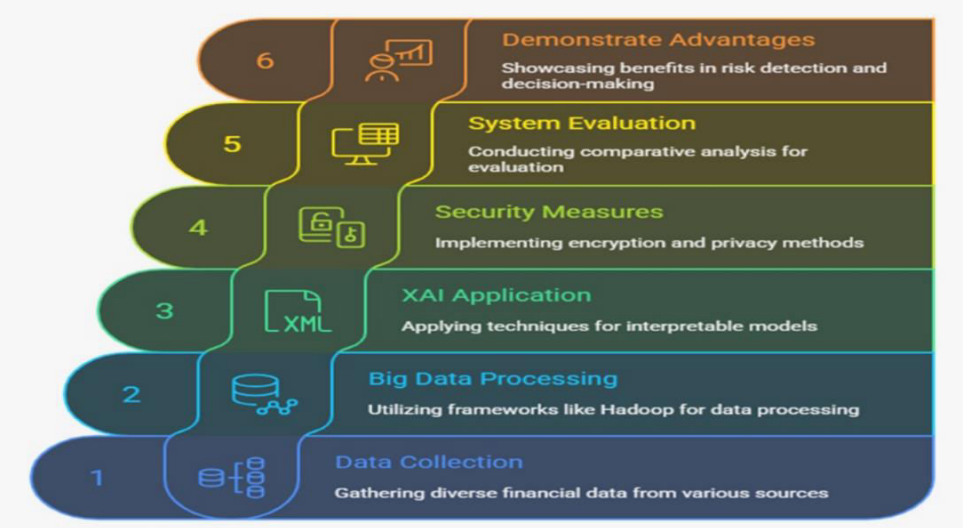
Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503102|

III. PROPOSED SYSTEM

The proposed system introduces a machine learning–driven and explainable fraud detection framework designed to improve both accuracy and transparency in secure financial analytics. It uses the IEEE-CIS Fraud Detection Dataset to simulate real-world financial transactions and capture realistic fraud patterns while addressing the challenge of highly imbalanced data. The system employs XGBoost, an efficient ensemble learning algorithm capable of detecting complex patterns in transaction data with high accuracy and reduced false positives. To overcome the black-box nature of traditional models, SHAP (SHapley Additive Explanations) is integrated to provide both global and transaction-level explanations, allowing analysts to understand why a transaction is classified as fraudulent or legitimate. The framework also incorporates data anonymization and privacy-preserving techniques to protect sensitive financial information during analysis. Overall, the system provides an explainable, scalable, and secure fraud detection solution that improves trust, supports regulatory compliance, and can be applied in real-world scenarios such as digital payment monitoring, banking transaction analysis, credit card fraud prevention, and anti-money laundering system.

IV. METHODOLOGY



1. Data Collection

This module is responsible for gathering financial transaction data from multiple sources such as payment systems, transaction logs, and historical financial records. It ensures that the collected data is relevant, consistent, and suitable for further processing and analysis.

Additionally, it standardizes data formats to maintain consistency and enables seamless integration with downstream processing modules.

2. Big Data Processing

The Big Data Processing Module manages and processes large-scale financial datasets using scalable data-handling techniques. It performs data cleaning, normalization, and feature extraction to prepare high-quality data for analysis. The module supports distributed processing to improve performance and reduce latency. It also ensures efficient storage and fast retrieval of processed data, making the system suitable for high-volume transaction environments.

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

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503102|

3. Explainable AI (XAI) Application

The Explainable AI (XAI) Application Module applies machine learning algorithms to detect fraudulent or high-risk transactions. Along with prediction, it provides clear explanations showing which features influenced the model's decision, improving transparency and user trust. The module supports adaptive learning to handle evolving fraud patterns. It also assists financial analysts in understanding model behavior and making informed decisions.

4. Security Measures

The Security Measures Module ensures the confidentiality and integrity of sensitive financial data throughout the system. It applies encryption techniques during data transmission and storage to prevent unauthorized access The module implements anonymization and role-based access control to protect user privacy. In addition, it enforces secure authentication and authorization mechanisms to strengthen overall system security.

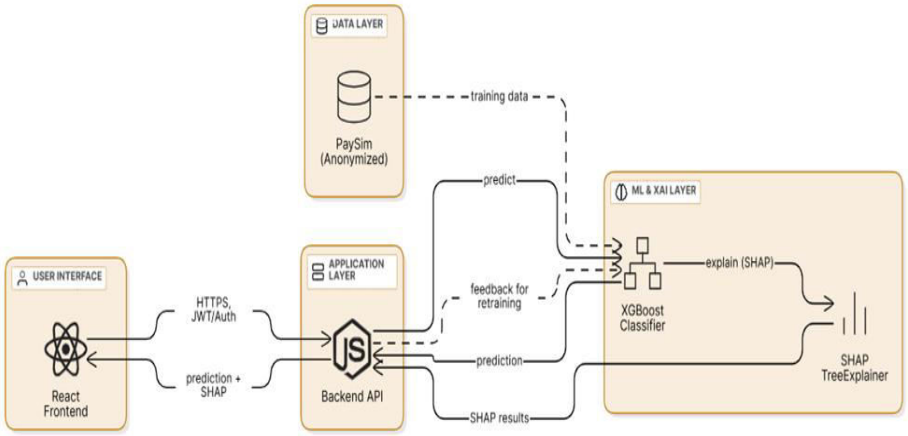
5. System evaluation

The System Evaluation Module assesses the effectiveness and reliability of the proposed system. It uses performance metrics such as accuracy, precision, recall, F1-score, and false positive rate for evaluation. The module tests the system on real-world and simulated datasets to ensure robustness. It also performs comparative analysis with existing fraud detection systems to highlight improvements. and visual integrity.

V. SYSTEM ARCHITECTURE

System architecture defines the overall structure of a system and explains how different components interact with each other to perform the required tasks. It provides a high-level view of the system, showing the organization of hardware, software, data, and communication mechanisms. A well-designed system architecture improves performance, scalability, security, and maintainability.

This architectural design helps in modular development, easy system upgrades, and effective management of resources. It also ensures that changes in one module do not affect other modules, making the system reliable and efficient.



The diagram illustrates the architecture of an Explainable AI–based secure financial analytics system designed for fraud detection. The process begins in the Data Layer, where anonymized financial transaction data such as the PaySim or IEEE-CIS Fraud Detection dataset is stored. This dataset contains transaction details like amount, balances, and transaction type, which are used as training data for the machine learning model. The data is then sent to the ML & XAI Layer, where the XGBoost classifier analyzes transaction patterns and predicts whether a transaction is fraudulent or legitimate. To make the model's decisions understandable, SHAP (SHapley Additive Explanations) is applied using the SHAP TreeExplainer, which identifies the most influential features contributing to each prediction

The predictions and SHAP explanation results are then passed to the Application Layer, which includes the Backend API (Node.js). This layer manages communication between the machine learning model and the user interface while ensuring secure data transfer through HTTPS and JWT-based authentication. Finally, the User Interface Layer,

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

Impact Factor 8.699

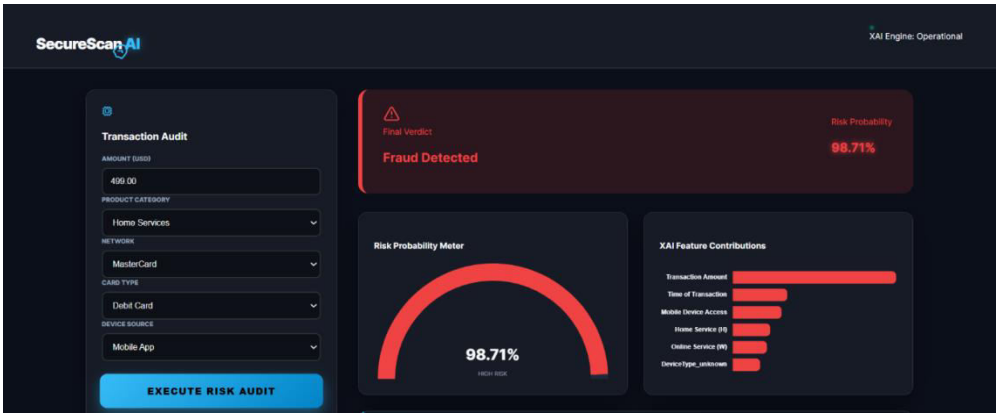
|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

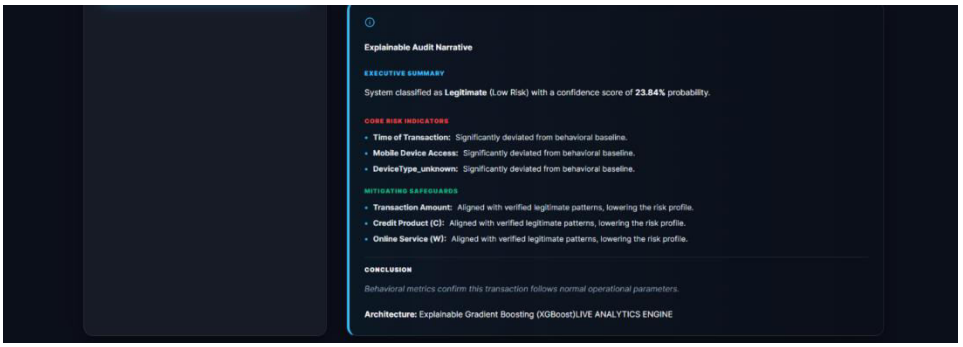
Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503102|

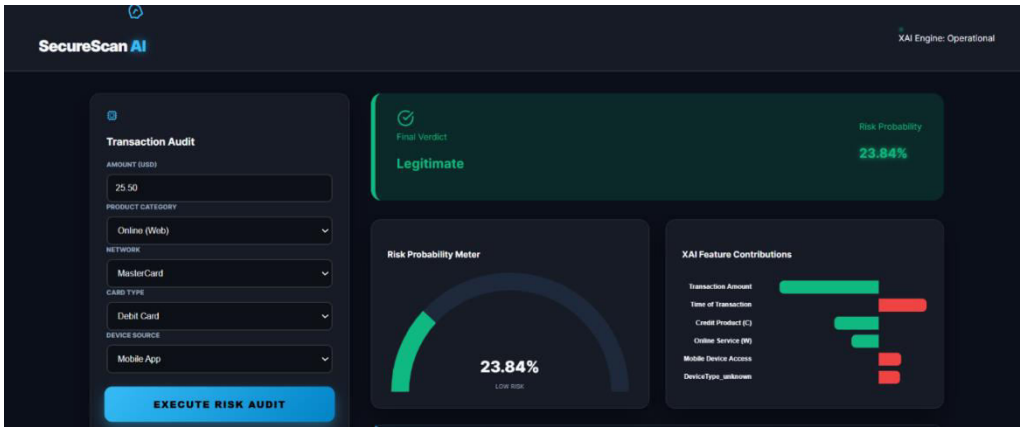
developed using React, allows users or analysts to input transaction details and view fraud predictions along with clear SHAP-based explanations. The architecture also supports a feedback mechanism where prediction results can be used for model retraining, enabling continuous improvement of fraud detection accuracy while maintaining transparency, security, and scalability in financial analytics systems.

VI. RESULTS AND OUTPUT





FRAUD DATA TESTCASE



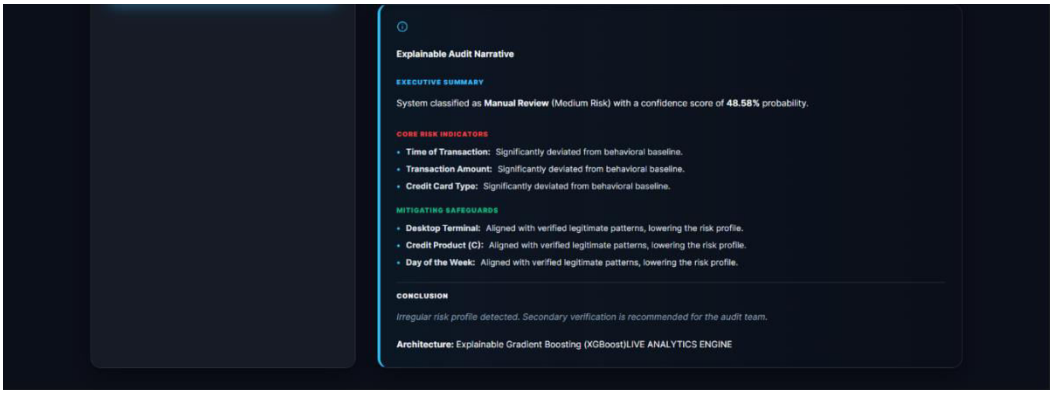
International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503102|



NON-FRAUDULENT CASE

VII. CONCLUSION

The rapid growth of digital financial services has increased the volume and complexity of financial transactions, creating more opportunities for fraudulent activities. Traditional rule-based fraud detection systems are no longer sufficient to address evolving fraud patterns. To tackle this challenge, this project developed an Explainable Artificial Intelligence (XAI)-based fraud detection system that combines machine learning techniques with interpretability tools to improve both detection accuracy and transparency.

The main objective of the project was to design a fraud detection framework that delivers strong predictive performance while ensuring that its decisions are understandable. The system uses the XGBoost algorithm, which is well suited for structured and imbalanced datasets. To improve transparency, SHAP (SHapley Additive Explanations) was integrated into the model to provide clear explanations for predictions at both the overall dataset level and the individual transaction level.

Overall, the system demonstrates that fraud detection models can achieve both high accuracy and transparency. By combining machine learning with explainable AI, the proposed framework improves trust, supports regulatory compliance, and can be applied in real-world financial environments. It also provides a strong foundation for future research and advancements in intelligent financial fraud detection systems.

VIII. FUTURE SCOPE

Future enhancements of the Explainable AI–Based Fraud Detection System can improve its scalability, intelligence, and real-world usability. One major improvement is the introduction of real-time streaming fraud detection, where transactions are analyzed instantly as they occur instead of using batch processing. This would allow financial institutions to detect and stop fraudulent activities immediately, reducing potential financial losses.

Additionally, the project can be expanded by incorporating more advanced machine learning models and continuous learning mechanisms. This would allow the system to improve its fraud detection accuracy over time by learning from new transaction data and evolving fraud patterns.

Some possible future improvements include:

- Real-time transaction monitoring and instant fraud alerts
- Integration with banking and payment gateway systems
- Use of advanced machine learning and deep learning models
- Implementation of role-based access for administrators and analysts
- Deployment as a cloud-based or mobile application

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

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503102|

REFERENCES

1. Chen, T., & Guestrin, C. (2016).
2. XGBoost: A Scalable Tree Boosting System.
3. Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining.
https://doi.org/10.1145/2939672.2939785
4. Lundberg, S. M., & Lee, S.-I. (2017).
5. A Unified Approach to Interpreting Model Predictions.
6. Advances in Neural Information Processing Systems (NeurIPS).
https://proceedings.neurips.cc/paper/2017/hash/8a20a8621978632d76c43dfd28b67767-Abstract.html
7. PaySim Dataset – Mobile Money Simulation Dataset
8. Kaggle Repository.
https://www.kaggle.com/datasets/ealaxi/paysim1
9. Molnar, C. (2022).
10. Interpretable Machine Learning (2nd Edition).
https://christophm.github.io/interpretable-ml-book/
11. European Central Bank (2023).
12. Card Fraud Statistics and Digital Payment Security Reports.
https://www.ecb.europa.eu/pub/cardfraud/html/index.en.html

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details