International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
SN: 3068-272X www.ijdim.com Original Research Paper

AI-BASED ANAMOLY DETECTION IN FINANCIAL AND TRANSACTION RECORDS

[1]Dr. P.V.S. Sarma,[2] V. Indu Gayatri,[3]P. Sai Varshitha,[4]S. S. M. Sandeep

[1]Associate Professor, Dept of Computer Science and Engineering, St. Ann's College of Engineering and Technology, Chirala-523187, India.

[2,3,4]U. G Student, Dept of Computer Science and Engineering, St. Ann's College of Engineering and Technology, Chirala-523187, India.

ABSTRACT- ***This project presents an AI-Based Anomaly Detection in Financial Transactions and Records system that uses Machine Learning to detect fraudulent financial transactions in real time. The proposed system improves transaction security by analyzing multiple transaction parameters and identifying suspicious activities with high accuracy. It ensures secure and intelligent decision-making through Artificial Intelligence and Machine Learning techniques. The system uses a Flask-based web application and an SQLite database to process transactions, classify them as Normal, Suspicious, or High Risk, and automatically perform appropriate security actions such as fraud alerts, user verification, and temporary card freezing. Traditional fraud detection methods mainly rely on predefined rules and manual verification, resulting in delayed detection and reduced accuracy. Therefore, there is a need for an intelligent, secure, and cost-effective financial fraud detection system that can protect digital transactions and reduce financial risks in modern banking environments.***

KEYWORDS: ***Artificial Intelligence (AI), Machine Learning (ML), Financial Fraud Detection, Anomaly Detection, Digital Banking, Transaction Monitoring, Flask, SQLite, Cybersecurity.***

INTRODUCTION

The rapid growth of digital banking, online payment systems, and electronic financial services has significantly transformed the financial sector by providing faster, more convenient, and secure transaction methods. However, this digital transformation has also increased

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
SN: 3068-272X www.ijdim.com Original Research Paper

the number of fraudulent activities, unauthorized transactions, and financial cyber threats. With the advancement of Artificial Intelligence (AI) and Machine Learning (ML), anomaly detection has become an effective approach for identifying suspicious transaction patterns and preventing financial fraud. This project combines AI-powered anomaly detection with real-time financial transaction monitoring to improve security and enhance the reliability of digital financial systems. The proposed system not only detects fraudulent transactions accurately but also provides intelligent risk classification, automated fraud alerts, and proactive security measures to protect users and financial institutions

LITERATURE SURVEY

Financial fraud detection has gained significant attention in recent years due to the rapid growth of digital banking, online payment systems, and electronic financial services. A financial fraud detection system is generally defined as an intelligent framework that integrates Artificial Intelligence (AI), Machine Learning (ML), and data analysis techniques to identify suspicious transactions and enhance financial security. The core concept of these systems revolves around analyzing transaction patterns, detecting anomalies, and making intelligent decisions using real-time financial data to prevent fraudulent activities.

RELATED WORK

Several researchers have contributed to the development of intelligent financial fraud detection systems with the aim of improving transaction security, fraud prevention, and real-time monitoring. Early research mainly focused on rule-based fraud detection methods, where suspicious transactions were identified using predefined rules and threshold values. These traditional systems relied on manual verification and fixed conditions, offering limited accuracy and adaptability against emerging fraud patterns. Recent studies have introduced Artificial Intelligence (AI) and Machine Learning (ML) techniques to analyze transaction behavior, detect anomalies, and improve fraud detection performance. These approaches provide faster decision-making, higher accuracy, and better scalability for modern digital financial systems.

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
SN: 3068-272X www.ijdim.com Original Research Paper

EXISTING SYSTEM

The existing financial fraud detection systems mainly rely on predefined rules, manual verification, and basic statistical methods to identify suspicious transactions. Financial institutions use fixed thresholds and rule-based mechanisms to detect fraudulent activities, which are often ineffective against new and sophisticated fraud patterns. These systems generate a high number of false alerts and require continuous human monitoring. Since fraud is frequently detected only after a transaction is completed, financial losses and delayed responses become common. Moreover, traditional systems lack intelligent decision-making, real-time anomaly detection, and adaptive learning capabilities. Overall, the existing system provides limited accuracy, reduced scalability, and inadequate protection against evolving financial fraud**.**

PROPOSED SYSTEM

The proposed system implements an AI-based anomaly detection framework for secure financial transaction monitoring using Machine Learning techniques.It continuously analyzes financial transactions in real time to identify suspicious and fraudulent activities based on multiple transaction parameters. Transactions are automatically classified as Normal, Suspicious, or High Risk, enabling timely security actions. Genuine transactions are approved, while suspicious transactions trigger additional verification and high-risk transactions generate fraud alerts and temporary card freezing. The system is developed using Python Flask with a secure SQLite database to store user information and transaction records. This intelligent approach enhances fraud detection accuracy, reduces manual intervention, and strengthens the security of digital financial transactions.

SYSTEM ARCHITECTURE

The architecture of the proposed AI-Based Anomaly Detection in Financial Transactions and Records consists of a user interface, frontend layer, Flask backend, AI fraud detection engine, SQLite database, and administrator dashboard. Users and administrators access the system through a responsive web application developed using HTML, CSS, JavaScript, and Jinja2 templates. The Flask backend manages user

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
SN: 3068-272X www.ijdim.com Original Research Paper

authentication, transaction processing, fraud prediction, and alert generation. The AI fraud detection engine performs feature extraction, data preprocessing, Machine Learning-based anomaly detection, and risk score prediction to classify transactions as Normal, Suspicious, or High Risk. All user information, transaction records, and fraud alerts are securely stored in the SQLite database. The administrator dashboard provides transaction monitoring, fraud analysis, user management, and report generation. This architecture ensures secure, intelligent, and real-time financial transaction monitoring.

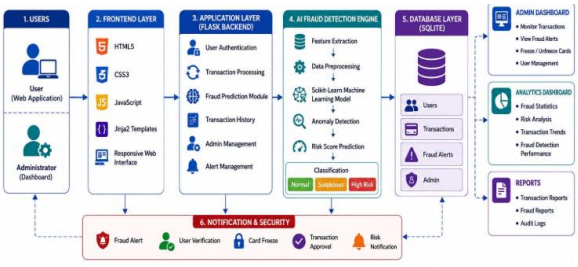


Fig 1: System Architecture

METHODOLOGY DESCRIPTION

The methodology of the proposed AI-Based Anomaly Detection in Financial Transactions and Records system is designed to provide intelligent fraud detection, real-time transaction monitoring, and enhanced financial security using Artificial Intelligence (AI) and Machine Learning (ML). The system follows a structured approach that includes user authentication, transaction data collection, feature preprocessing, Machine Learning-based anomaly detection, risk classification, and automated security actions. Based on the prediction results, transactions are classified as Normal, Suspicious, or High Risk, enabling appropriate actions such as transaction approval, user verification, fraud alert generation, or temporary card freezing. This methodology ensures accurate, secure, and efficient detection of fraudulent financial transactions while reducing manual intervention.

RESULTS AND DISCUSSION

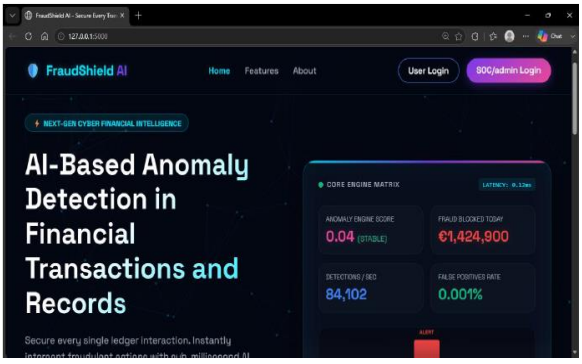


Fig2: Home page

The Home Page is the main screen of the AI-Based Anomaly Detection system. It provides a simple and user-friendly

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
SN: 3068-272X www.ijdim.com Original Research Paper

interface for users to access important features such as login, transaction processing, fraud detection, and transaction history. The page allows users to navigate the application easily and securely.

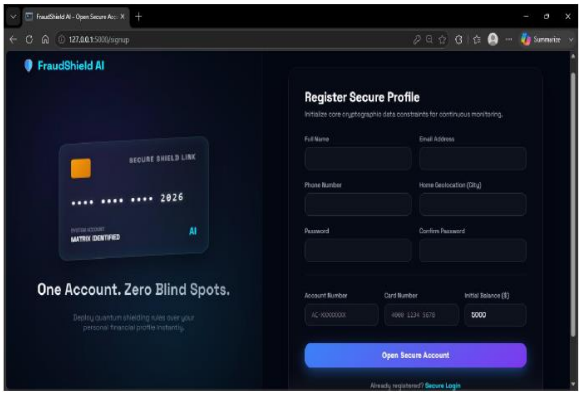


Fig 3: User Registration

The User Registration page allows new users to create an account by entering their personal and account details securely.

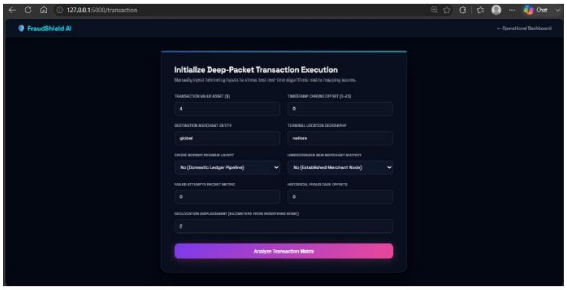


Fig 4: Transaction Analysis

The Transaction Analysis page allows users to enter transaction details and analyze them using the AI-based fraud detection model.

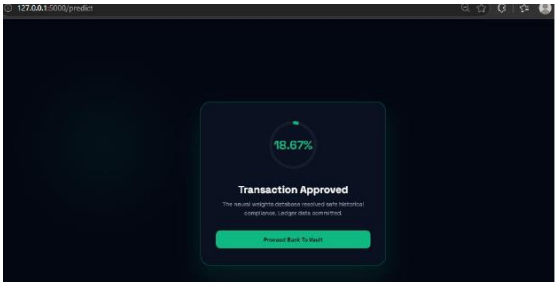


Fig 5: Fraud Prediction Result

The system analyzes the transaction and displays the prediction result as Normal, Suspicious, or High Risk, helping users identify fraudulent activities in real time**.**

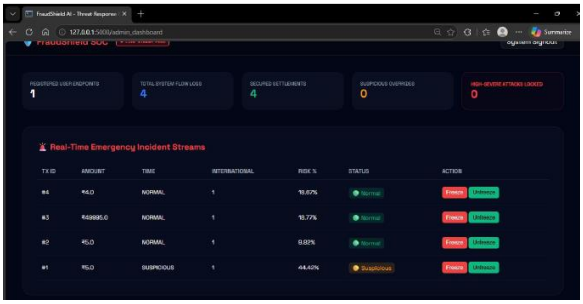


Fig. 6: Admin Dashboard

The Admin Dashboard helps the administrator monitor transactions, manage users, and view fraud alerts. It provides easy access to important system information and security controls.

CONCLUSION

The proposed AI-Based Anomaly Detection in Financial Transactions and Records

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
SN: 3068-272X www.ijdim.com Original Research Paper

system improves the security of digital financial transactions by detecting fraudulent activities using Machine Learning. By analyzing transaction details in real time and classifying them as Normal, Suspicious, or High Risk, the system helps prevent financial fraud and reduces manual effort. Overall, the proposed system provides a secure, reliable, and intelligent solution for modern financial transaction monitoring.

FUTURE SCOPE

The proposed system can be further enhanced by integrating advanced Deep Learning models to improve fraud detection accuracy. Multi-factor authentication, such as OTP and biometric verification, can be added to strengthen security. The system can also be extended with cloud databases, banking API integration, and mobile applications for real-time monitoring. Additionally, blockchain technology and AI-powered analytics dashboards can be incorporated to improve transaction transparency and fraud prevention.

REFERENCES

1. D. P. Harini, "Electronic Health Record Stage Identification using Principal Component Analysis," *Machine Intelligence Research,* vol. 18, no. 01, pp. 864- 873, 17 8 2024.
2. D. P. Harini, "Two Level Intrusion Detection For Detecting Intruders in Multitier Web Applications," *International Journal of Engineering & Science Research,* vol. 3, no. 9, pp. 472-478, 2013.
3. D. P. Harini, "Analyze and Predict of Human Cyber Attackers using Artificial Neural Network," *Journal of Basic Science and Engineering,* vol. 21, no. 1, pp. 1529 - 1536, 8 7 2024.
4. **Manoharan et al., 2024 – "Machine Learning-Based Real-Time Fraud DetectionSystem"(IEEE)**
   The proposed framework detects suspicious financial transactions using Machine Learning techniques. It provides real-time monitoring and improves transaction security.
5. **. Sarna et al., 2025 – "AI Driven Fraud Detection Models in Financial Networks"(IEEE)**
   This research focuses on AI-based fraud detection models for digital financial systems. The proposed approach identifies complex fraud patterns with improved accuracy.
6. **Hernandez Aros et al., 2024 – "Financial Fraud Detection through Machine Learning Techniques"**
   This review discusses recent Machine Learning techniques for financial fraud detection. It concludes that AI-based systems

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
SN: 3068-272X www.ijdim.com Original Research Paper

provide better accuracy and real-time fraud detection than traditional methods.

7. **Ali et al., 2022 – "Financial Fraud Detection Based on Machine Learning"** This paper reviews various Machine Learning algorithms used for fraud detection. It highlights their applications, advantages, and limitations in digital payment systems.
8. **Randhawa et al., 2018 – "Credit Card Fraud Detection Using AdaBoost and MajorityVoting"** This paper presents an intelligent fraud detection model using AdaBoost and majority voting techniques. The proposed approach improves detection accuracy and reduces false alarms in credit card transactions.
9. **Carcillo et al., 2019 – "Combining Unsupervised and Supervised Learning in Credit Card Fraud Detection"** This paper combines supervised and unsupervised Machine Learning techniques for detecting fraudulent transactions. The proposed method enhances fraud detection performance and supports real-time financial monitoring.
10. **Jurgovsky et al., 2018 – "Sequence Classification for Credit Card Fraud Detection"** This paper introduces a sequence-based Machine Learning approach for identifying fraudulent credit card transactions. The proposed model effectively detects transaction anomalies and improves fraud prediction accuracy.
11. Kumar, Anuj. "Battery Thermal Management Systems for Electric Vehicles Using Phase Change Materials." International Journal of Engineering, Science and Mathematics, Vol. 10, Issue 3, 2021, pp. 202-211