International Journal of Science, Strategic Management and Technology
Volume **02** Issue **06** June-**2026** | ISSN: **3108-1762 (Online)** | Impact Factor: 3.8
An International, Peer-Reviewed, Open Access Scholarly Journal Indexed in recognized academic databases

AI-Based Fraud Detection System

Ankita Jena
Department of Master of Computer Application (MCA)
GIFT Autonomous, Bhubaneswar, Odisha, India, ankitajena2024@gift.edu.in

Subhendu Sekhar Sahoo
Assistant Professor, Department of Master of Computer Application (MCA)
GIFT Autonomous, Bhubaneswar, Odisha, India, ssahoo@gift.edu.in

https://doi.org/10.55041/ijsmt.v2i6.062

Cite this Article: Jena, A. (2026). AI-Based Fraud Detection System. International Journal of Science, Strategic Management and Technology, *02*(6). https://doi.org/10.55041/ijsmt.v2i6.062

License: This article is published under the Creative Commons Attribution 4.0 International License (CC BY 4.0), permitting use, distribution, and reproduction in any medium, provided the original author(s) and source are properly credited.

ABSTRACT

Financial fraud in digital payment systems and online banking platforms has become a major technological and security challenge due to the rapid growth of online transactions and electronic financial services. Although many existing fraud detection systems provide transaction monitoring and alert mechanisms, most of them rely on predefined rules and manual verification processes, which are often unable to identify fraudulent activities in real time or analyze complex transaction behavior intelligently. This paper presents the AI-Based Fraud Detection System, an intelligent fraud prevention platform that combines real-time transaction monitoring, machine learning-based risk prediction, and automated fraud alert generation.

The proposed system evaluates multiple transaction-related parameters, including transaction amount, transaction frequency, login location, device information, IP address, user behavior patterns, and unusual account activity to estimate the probability of fraudulent transactions. Based on this analysis, the system classifies transactions into Low Risk, Medium Risk, or High Risk categories. When a high-risk transaction is detected, the application automatically generates a fraud alert and notifies administrators for immediate action and transaction verification.

The application is developed using React and TypeScript for the user interface, Python and FastAPI for backend services, SQLite/MySQL for data management, and JWT authentication for secure user access and authorization. Experimental testing confirms that the system provides accurate fraud detection, efficient risk classification, secure authentication, and reliable real-time monitoring of transactions.

The AI-Based Fraud Detection System transforms traditional fraud monitoring approaches into an intelligent and proactive financial security platform capable of reducing financial losses, improving transaction safety, and enhancing real-time fraud prevention.

Keywords: Fraud Detection, Machine Learning, FastAPI, Transaction Monitoring, Risk Prediction, JWT Authentication, Real-Time Alert System, Financial Security.

1. INTRODUCTION

Financial fraud has emerged as a critical issue in modern digital banking, online payment systems, and e-commerce platforms due to the increasing number of electronic transactions and cyber-related financial crimes. Fraudulent activities such as unauthorized transactions, identity theft, account takeover, and suspicious payment behavior can result in severe financial losses for both

© Author(s). This work is peer-reviewed, openly published, and permanently archived
This article is openly accessible and reusable with proper attribution.

organizations and customers. Traditional fraud prevention approaches, including manual verification and rule-based monitoring systems, are often inefficient because they cannot process large transaction volumes or identify complex fraud patterns effectively.

With the rapid advancement of online financial services and digital payment technologies, intelligent transaction monitoring systems have become essential for ensuring financial security and minimizing fraud risks. However, many existing fraud detection systems are reactive in nature. They mainly depend on predefined rules and generate alerts only after suspicious activities have already occurred. These systems generally fail to analyze contextual transaction behavior or predict fraud proactively.

The AI-Based Fraud Detection System addresses these limitations by integrating machine learning algorithms with real-time transaction analysis and automated alert generation. The system continuously evaluates transaction-related parameters such as transaction amount, login location, transaction frequency, device information, IP address, and user behavior patterns to calculate fraud risk levels and identify suspicious activities automatically.

By automating fraud analysis, risk prediction, and alert generation, the proposed system improves fraud detection accuracy, reduces response time, and enhances the overall security of digital financial transactions.

2. OBJECTIVES OF THE PROJECT

The principal objectives of the proposed system are:

1. To develop a secure AI-based fraud detection system with real-time transaction monitoring capabilities.
2. To analyze digital transactions and identify suspicious activities automatically.
3. To store user information, transaction details, and fraud records securely.
4. To predict fraudulent transactions using machine learning techniques.
5. To classify transactions as Low Risk, Medium Risk, or High Risk.
6. To automatically generate fraud alerts when suspicious transactions are detected.
7. To provide secure authentication and authorization using JWT technology.
8. To maintain transaction history and fraud alert records for future analysis.
9. To provide an administrative dashboard for monitoring transactions and fraud activities.
10. To build a scalable and intelligent platform for future fraud prevention enhancements.

3. LITERATURE SURVEY

A number of research efforts have focused on fraud detection systems for digital banking, online transactions, and financial security. Most existing systems provide features such as transaction monitoring, suspicious activity detection, and alert generation based on predefined rules and security conditions.

Various researchers have proposed machine learning-based fraud detection models capable of identifying fraudulent transactions using behavioral analysis and transaction pattern recognition. Random Forest, Decision Tree, Logistic Regression, and Neural Network algorithms are widely used for fraud prediction and anomaly detection in financial systems.

Research studies indicate that traditional rule-based fraud detection systems are often unable to detect complex fraud patterns efficiently and may generate high false-positive rates. Several modern systems focus on transaction analysis, risk scoring, user authentication, and automated fraud alert generation to improve financial security.

Recent research also highlights the importance of real-time fraud monitoring, secure authentication mechanisms, administrative dashboards, and predictive risk analysis in modern financial systems. However, many existing systems still lack intelligent automation, scalable architecture, and efficient real-time fraud prevention capabilities.

These observations motivated the development of a more comprehensive and intelligent AI-Based Fraud Detection System capable of performing real-

© Author(s). This work is peer-reviewed, openly published, and permanently archived
This article is openly accessible and reusable with proper attribution.

time transaction monitoring, machine learning-based fraud prediction, automated alert generation, and secure financial risk management.

4. EXISTING SYSTEM

Several fraud detection systems have been developed in recent years to provide security for online banking, e-commerce platforms, and digital payment applications. These systems are generally implemented using rule-based techniques, transaction monitoring systems, and traditional security mechanisms to identify suspicious financial activities.

Existing fraud detection applications analyze transaction details such as transaction amount, account activity, login attempts, and payment frequency to identify unusual behavior. Many banking and financial platforms generate alerts whenever suspicious transactions exceed predefined limits or violate security rules. Some systems also include OTP verification, account blocking, and manual transaction verification to reduce fraud risks.

Most of these systems are built using a three-tier architecture consisting of a frontend interface, backend server, and database management system. The frontend provides user registration, login, transaction management, and account monitoring interfaces. The backend processes transaction requests, performs verification, and communicates with databases and security APIs. Databases such as MySQL, PostgreSQL, and Firebase are commonly used to store user information, transaction records, and fraud history.

For example, traditional banking fraud systems monitor unusual transaction amounts and repeated failed login attempts, while payment gateways use rule-based engines to block suspicious payments. Some modern systems also implement behavioral analysis and transaction tracking for improving financial security.

Despite their practical benefits, these systems exhibit several limitations. Most existing systems are reactive and generate alerts only after suspicious transactions have already occurred. They mainly depend on predefined rules and manual verification processes, which are often unable to identify complex fraud patterns efficiently. In addition, many systems generate high false-positive rates and lack intelligent machine learning models capable of performing predictive fraud analysis.

Another limitation is the absence of real-time automated decision-making. Existing systems often fail to analyze contextual transaction parameters such as user behavior patterns, login location, device information, IP address, transaction frequency, and unusual account activity simultaneously. Consequently, they are unable to predict fraudulent behavior proactively or provide intelligent risk classification.

These shortcomings demonstrate the necessity for a more intelligent and proactive fraud detection platform that combines real-time transaction monitoring, machine learning-based fraud prediction, automated alert generation, and secure financial risk management.

5. PROPOSED SYSTEM

The proposed AI-Based Fraud Detection System is an intelligent financial security platform that not only monitors digital transactions in real time but also analyzes transaction behavior to detect fraudulent activities automatically. The system is designed to identify suspicious transactions and provide immediate fraud alerts with minimal manual intervention.

The application starts with a secure registration and authentication process where users create accounts and securely log in using JWT-based authentication. The system securely stores user profiles, transaction records, and fraud history in the database.

The core functionality of the system is the Transaction Analysis feature. Whenever a transaction is performed, the application analyzes several parameters such as transaction amount, transaction frequency, login location, IP address, device information, payment behavior, and unusual account activity. Using these inputs, the system predicts the fraud risk level and classifies transactions as:

- Low Risk (Risk 0) – The transaction is considered safe and legitimate.

© Author(s). This work is peer-reviewed, openly published, and permanently archived
This article is openly accessible and reusable with proper attribution.

• Moderate Risk (Risk 1) – The transaction appears suspicious and requires monitoring.

• High Risk (Risk 2) – The transaction is considered potentially fraudulent and requires immediate attention.

The predicted result is displayed on the dashboard along with transaction details, risk score, and transaction status.

If the transaction is classified as High Risk, the application automatically activates the Fraud Alert Module. An alert message containing transaction details, user information, risk status, and transaction timestamp is instantly sent to administrators for verification and further action.

In addition to automatic fraud detection, the application also provides a Fraud Simulator feature that allows administrators to test and analyze suspicious transaction behavior in real time.

The Real-Time Transaction Monitoring feature continuously analyzes user activities and transaction patterns to identify unusual financial behavior and prevent unauthorized transactions.

The system also maintains a complete transaction history and fraud alert record, allowing users and administrators to review previous activities and security events.

An Admin Dashboard is included to monitor registered users, transaction activities, fraud alerts, risk statistics, and system performance.

Key Features of the Proposed System

• Secure user registration and login using JWT authentication

• Real-time transaction monitoring

• Machine learning-based fraud prediction

• Automatic high-risk transaction detection

• Fraud alert generation and notification system

• Fraud simulation and testing module

• Transaction and fraud history management

• Role-based access control for users and administrators

• Interactive analytics dashboard

• Scalable and secure financial monitoring architecture

By combining predictive fraud analysis, automated alert generation, and real-time transaction monitoring, the proposed system offers a proactive and reliable approach to improving financial security and reducing fraudulent activities.

6. SYSTEM REQUIREMENTS

6.1 Hardware Requirements

• Intel Core i3 Processor or above
• 4 GB RAM or higher
• 500 GB Hard Disk
• Stable Internet Connection
• Multi-Core Processor for faster transaction processing

6.2 Software Requirements

• Operating System: Windows/Linux

• Frontend: React, TypeScript, Tailwind CSS

• Backend: Python, FastAPI

• Database: SQLite / MySQL

• APIs: JWT Authentication API, REST APIs

• Development Tool: Visual Studio Code

• Libraries: Pandas, Scikit-learn, NumPy, SQLAlchemy, Axios, Recharts

7. SYSTEM ARCHITECTURE

The AI-Based Fraud Detection System is designed using a modular client-server architecture that ensures secure communication, real-time

© Author(s). This work is peer-reviewed, openly published, and permanently archived
This article is openly accessible and reusable with proper attribution.

transaction monitoring, and efficient fraud management. The architecture consists of several interconnected modules that work together to perform user authentication, transaction processing, fraud analysis, alert generation, and administrative monitoring. This structured design improves scalability, maintainability, and overall system performance while ensuring secure handling of financial data.

The system architecture mainly consists of the following components:

- Frontend Module
- Backend Module
- Transaction Module
- Rule Engine Module
- Fraud Alert Module
- Database Module
- Admin Module

The Frontend Module provides a user-friendly interface through which users can register, log in, perform transactions, monitor transaction history, and view fraud alerts. It also displays transaction status and dashboard analytics.

The Backend Module manages the core logic of the system. It processes user requests, handles transaction data, communicates with the rule engine, generates fraud alerts, and stores records in the database.

The Transaction Module continuously monitors transaction activities and analyzes transaction details such as amount, frequency, location, and unusual user behavior to identify suspicious activities.

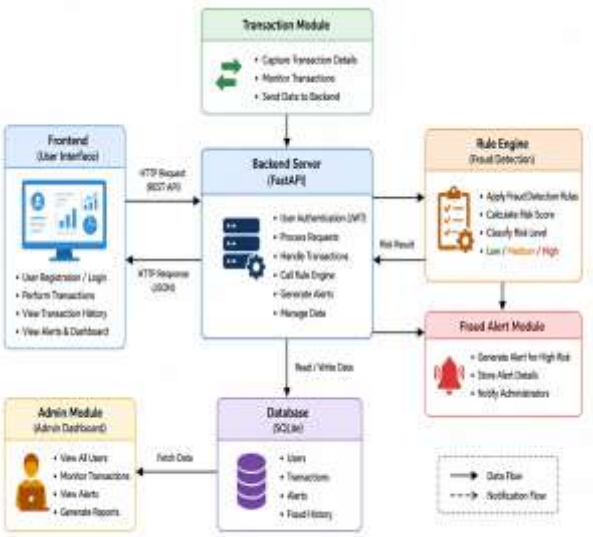
The Rule Engine Module acts as the intelligence component of the system. It analyzes transaction parameters and calculates a risk score using predefined fraud detection rules. Based on the analysis, transactions are classified as Low Risk, Medium Risk, or High Risk.

The Fraud Alert Module generates notifications whenever a High Risk transaction is detected. Alert details are sent to administrators for immediate verification and further action.

The Database Module stores user profiles, transaction records, fraud history, authentication data, and alert details securely for future analysis and monitoring.

The Admin Module enables administrators to monitor transactions, view fraud alerts, analyze reports, and manage the entire system through an admin dashboard.

Overall, the system architecture of the AI-Based Fraud Detection System provides a secure, scalable, and reliable framework for detecting and preventing fraudulent activities using real-time transaction monitoring and rule-based fraud analysis.



8. DATA FLOW DIAGRAM

The Data Flow Diagram (DFD) represents the movement of information within the AI-Based Fraud Detection System. It illustrates how transaction data is collected from users, processed by different modules, analyzed using fraud detection rules, and stored securely in the database. The DFD provides a clear understanding of how user authentication, transaction monitoring, fraud

© Author(s). This work is peer-reviewed, openly published, and permanently archived
This article is openly accessible and reusable with proper attribution.

analysis, and alert generation are handled by the system.

The main entities involved in the system are the User, Admin, Transaction Module, Rule Engine Module, Fraud Alert Module, and Database. Each entity interacts with the system to perform specific operations related to transaction processing and fraud management.

The data flow begins with the user registration process. During registration, the user enters personal details such as username, email address, password, and account information. These details are validated and securely stored in the database. Each user is assigned a unique identifier to maintain consistency and security.

After registration, the user logs into the application using valid credentials. Once authenticated, the user gains access to the dashboard, where features such as transaction management, fraud status monitoring, and transaction history are available.

When the user performs a transaction, the application collects transaction-related information such as transaction amount, transaction frequency, login location, IP address, device information, and payment details.

These transaction parameters are forwarded to the Rule Engine Module, which analyzes the input data using predefined fraud detection rules and risk analysis techniques. The system calculates a fraud risk score and classifies the transaction into one of three categories: Low Risk, Medium Risk, or High Risk.

The predicted fraud result is displayed immediately on the user dashboard and simultaneously stored in the database along with transaction details, timestamp, and risk status.

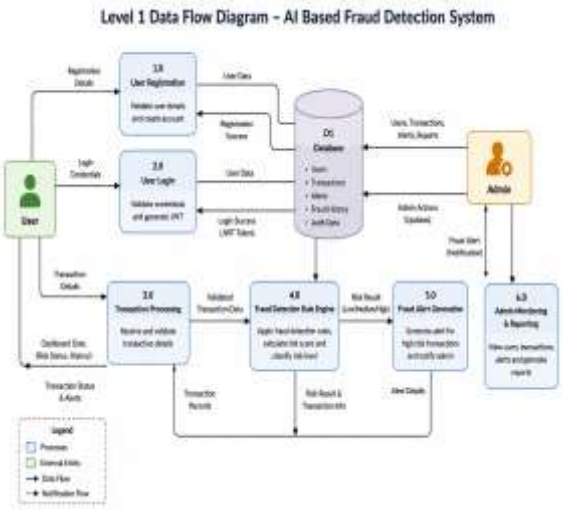
If the transaction is classified as High Risk, the system automatically activates the Fraud Alert Module. The module generates an alert containing user information, transaction details, risk status, and transaction time. The alert is then sent to the administrator for immediate verification and action.

The Admin Module continuously interacts with the database to monitor registered users, transaction activities, and fraud alerts. Administrators can review transaction history, analyze fraud reports, and ensure the proper functioning of the application.

Security is maintained throughout the data flow process. User credentials, transaction records, fraud alerts, and authentication data are stored securely, and access to administrative functions is restricted to authorized users only.

The DFD helps in understanding how information moves through the AI-Based Fraud Detection System and how different modules cooperate to provide secure transaction monitoring and fraud prevention.

Overall, the Data Flow Diagram demonstrates the complete flow of data from user registration to fraud analysis and alert generation, ensuring a secure, reliable, and efficient fraud detection system.



9. DATABASE DESIGN

The database design is one of the most important components of the AI-Based Fraud Detection System because it stores and manages all information related to users, transactions, fraud analysis, alerts, and administrators. A well-structured database ensures secure data storage, efficient transaction processing, quick retrieval of

© Author(s). This work is peer-reviewed, openly published, and permanently archived
This article is openly accessible and reusable with proper attribution.

records, and smooth communication between all modules of the system.

The system uses a relational database structure where all tables are connected through primary keys and foreign keys. Each registered user is assigned a unique User ID, which is used to link transactions, fraud analysis records, and alerts.

The **User Table** stores user information such as user ID, name, email, phone number, password, role, and account status. This table is mainly used for authentication and profile management.

The **Transaction Table** stores all transaction-related details such as transaction amount, payment method, merchant name, transaction type, IP address, device information, location, and transaction status. Every transaction is associated with a specific user.

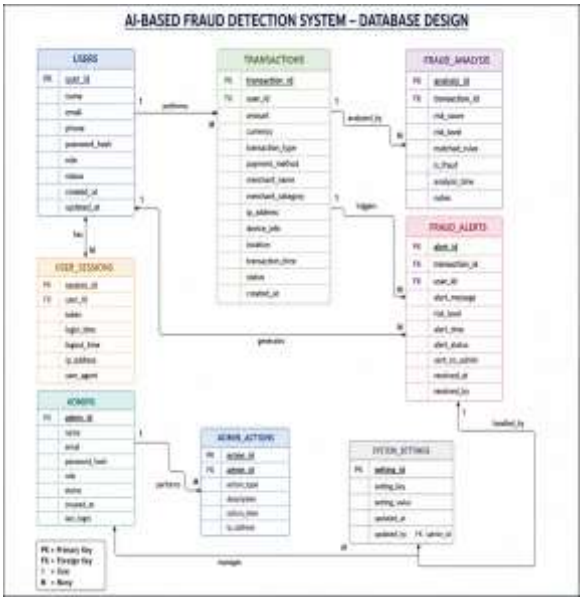
The **Fraud Analysis Table** stores the fraud detection results generated by the Rule Engine. It contains risk score, risk level, matched fraud rules, analysis time, and fraud status.

The **Fraud Alert Table** stores alerts generated when suspicious transactions are detected. It contains transaction ID, user ID, alert message, risk level, alert time, and alert status.

The **Admin Table** stores administrator credentials and access details. Only authorized administrators can monitor transactions, fraud alerts, and reports through the admin dashboard.

The database also maintains relationships between users, transactions, fraud analysis, and alerts, which helps maintain data consistency and improves system performance.

Security is maintained throughout the database using encrypted passwords, authentication mechanisms, and role-based access control. Backup and recovery mechanisms are also implemented to protect important financial records from accidental loss.



10. MODULE DESCRIPTION

10.1 User Registration Module

This module allows users to create an account in the application by entering personal details such as name, email address, phone number, password, usual location, and device information. During registration, the system securely stores user details in the database for authentication and fraud monitoring.

The module validates all input fields and ensures secure registration using encrypted password storage and JWT-based authentication. After successful registration, users can log in and access the fraud detection features of the system.

10.2 Transaction Monitoring Module

The Transaction Monitoring Module is the core component of the system. It continuously monitors transaction activities and analyzes important transaction parameters such as transaction amount, location, IP address, device information, transaction frequency, and payment method.

Based on these inputs, the system calculates the fraud risk score and classifies transactions as Low Risk, Medium Risk, or High Risk. This module helps identify suspicious activities and prevent fraudulent transactions in real time.

10.3 Fraud Alert Module

This module is responsible for generating fraud alerts whenever suspicious or High Risk transactions are detected.

© Author(s). This work is peer-reviewed, openly published, and permanently archived
This article is openly accessible and reusable with proper attribution.

International Journal of Science, Strategic Management and Technology
Volume **02** Issue **06** June-**2026** | ISSN: **3108-1762 (Online)** | Impact Factor: 3.8
An International, Peer-Reviewed, Open Access Scholarly Journal Indexed in recognized academic databases

The alert message includes transaction details, risk level, transaction time, and fraud status. Alerts are instantly sent to administrators for verification and immediate action. The module ensures quick response and efficient fraud management during suspicious activities.

10.4 Admin Module

The Admin Module allows authorized administrators to monitor and manage the entire fraud detection system.

Administrators can view registered users, monitor transaction records, review fraud alerts, analyze risk reports, and manage suspicious activities through the admin dashboard. This module helps maintain transparency and ensures proper functioning of the system.

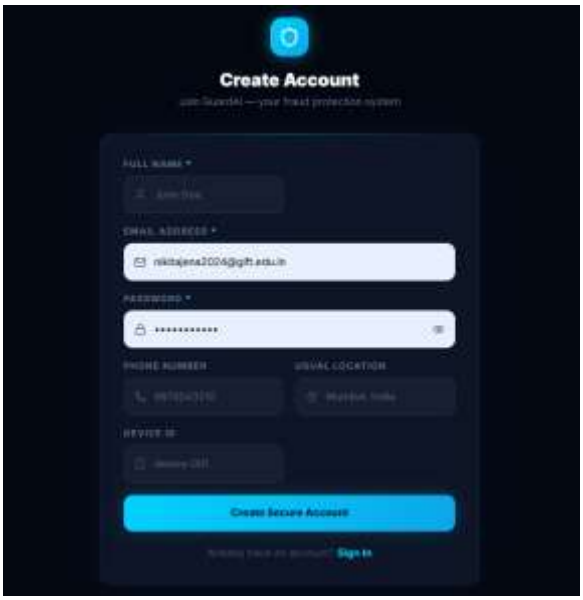


Fig : User Registration Interface

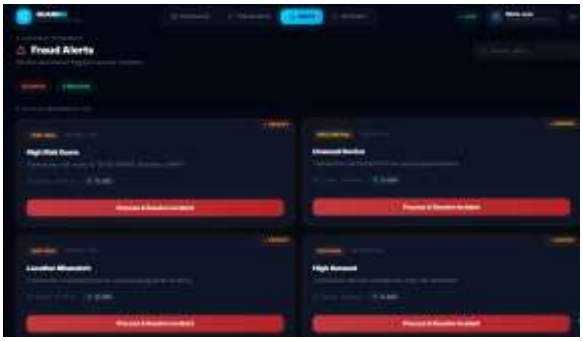


Fig : Emergency Alert Page

11. IMPLEMENTATION

The implementation of the AI-Based Fraud Detection System is carried out using modern web technologies, secure authentication mechanisms, and real-time transaction monitoring services. The application provides a user-friendly interface through which users can register, log in, perform transactions, monitor fraud status, and view fraud alerts.

The User Registration Module stores user details such as name, email address, phone number, password, usual location, and device information securely in the database. Once registered, users can log in and access all transaction and fraud monitoring features through the dashboard.

During a transaction, the system collects important transaction parameters such as transaction amount, transaction type, IP address, location, device information, merchant details, and transaction frequency. These transaction details are analyzed by the Rule Engine Module using predefined fraud detection rules to calculate the fraud risk score.

Based on the analysis, the system classifies transactions into Low Risk, Medium Risk, or High Risk categories. If a transaction is detected as High Risk, the application automatically generates a fraud alert and sends a notification to the administrator for verification and immediate action.

The backend server processes user requests, handles transaction analysis, manages fraud alerts, and communicates with the database to store transaction history, fraud records, and alert details. The frontend interface provides real-time monitoring dashboards, transaction history, fraud alerts, and analytics reports for both users and administrators.

Security features such as JWT authentication, encrypted password storage, role-based access control, and protected database access are incorporated to ensure secure handling of financial and user information.

The system is implemented using React and TypeScript for the frontend, FastAPI and Python for backend development, PostgreSQL/MySQL for

© Author(s). This work is peer-reviewed, openly published, and permanently archived
This article is openly accessible and reusable with proper attribution.

database management, and REST APIs for communication between frontend and backend modules.

12. ALGORITHMS USED

12.1 Fraud Detection Rule Algorithm

The Fraud Detection Rule Algorithm is the core component of the AI-Based Fraud Detection System. It analyzes various transaction parameters to determine the fraud risk level of a transaction.

The algorithm takes inputs such as transaction amount, transaction frequency, IP address, location, device information, merchant details, and transaction time. These parameters are processed using predefined fraud detection rules stored in the Rule Engine Module.

Based on the input values, the system predicts one of the following risk categories:

1. Low Risk
2. Medium Risk
3. High Risk

The predicted result is displayed to the user and administrator immediately after the transaction is analyzed.

12.2 Fraud Alert Trigger Algorithm

The Fraud Alert Trigger Algorithm continuously monitors the output of the fraud analysis process.

If the predicted result is High Risk, the system automatically activates the Fraud Alert Module. The algorithm generates a fraud alert containing transaction details, user information, transaction timestamp, fraud risk status, and transaction amount.

When fraud is detected, the system automatically sends an alert email to the registered user using the SMTP Email Service. The email contains transaction details, fraud risk level, and verification options such as approving or blocking the transaction.

The administrator also receives fraud notifications for monitoring and verification purposes. In critical situations, suspicious transactions can be temporarily blocked until user verification is completed.

Users can verify whether the transaction was performed by them through the verification link provided in the email alert.

This algorithm ensures that fraud alerts and email notifications are generated instantly whenever the system detects suspicious or potentially fraudulent transaction activity.

13. RESULTS AND DISCUSSION

The AI-Based Fraud Detection System successfully improves financial security by combining real-time transaction monitoring, rule-based fraud analysis, and automated email alert generation. Testing results indicate that the system accurately identifies suspicious transactions and provides timely fraud alerts during high-risk activities.

The application successfully analyzes transaction details such as transaction amount, location, IP address, device information, transaction frequency, and unusual account activity. Based on these parameters, the system classifies transactions as Low Risk, Medium Risk, or High Risk.

When a High Risk transaction is detected, the system automatically generates a fraud alert and sends an email notification to the registered user. The email contains transaction details, fraud risk level, and verification options that allow the user to approve or block the transaction instantly.

The transaction monitoring module accurately processes user transactions and detects suspicious activities in real time. The fraud alert module also functions correctly and provides quick notification delivery to both users and administrators.

The admin module successfully monitors registered users, transaction records, fraud alerts, and fraud history. All transaction activities and alert records are stored securely in the database and can be retrieved efficiently whenever required.

Experimental testing demonstrates that the application performs reliably under different transaction scenarios and provides quick response during suspicious financial activities. The integration of rule-based fraud detection and automated email verification significantly enhances the effectiveness of the system by enabling

© Author(s). This work is peer-reviewed, openly published, and permanently archived
This article is openly accessible and reusable with proper attribution.

proactive fraud prevention and secure transaction monitoring.

14. ADVANTAGES OF THE SYSTEM

- Provides real-time monitoring of transaction activities.
- Automatically detects suspicious and fraudulent transactions.
- Sends instant email alerts to users when fraud is detected.
- Improves financial security and reduces fraud risks.
- Enables administrators to monitor transactions and fraud alerts.
- Supports secure authentication using JWT and encrypted passwords.
- Maintains transaction history and fraud records efficiently.
- Reduces response time during suspicious transaction activities.
- Provides scalable architecture for future enhancements.
- Improves user trust and confidence in digital transactions.

15. FUTURE ENHANCEMENTS

The AI-Based Fraud Detection System can be enhanced further by incorporating advanced technologies and additional security features.

Future improvements include:

1. AI and Machine Learning integration for advanced fraud prediction and intelligent risk analysis.
2. Cloud-based deployment for improved scalability, performance, and secure data accessibility.
3. Mobile application support for real-time fraud monitoring and instant transaction alerts.
4. Biometric authentication such as fingerprint and face recognition for enhanced security.
5. Blockchain integration for secure and tamper-proof transaction verification.
6. Real-time integration with banking systems and payment gateways for faster fraud prevention.
7. Advanced analytics dashboards with graphical fraud reports and risk visualization.
8. Multi-factor authentication and OTP verification for suspicious transactions.
9. Integration with external fraud intelligence APIs for enhanced threat detection.
10. Automated transaction blocking and recovery mechanisms during critical fraud situations.

16. CONCLUSION

The AI-Based Fraud Detection System provides an intelligent and proactive approach to financial security by integrating real-time transaction monitoring, rule-based fraud analysis, secure authentication, and automated email alert generation.

The system improves transaction security by analyzing transaction behavior and detecting suspicious activities before major financial loss occurs. Automatic fraud alert generation and email verification features enable quick response and reduce dependence on manual monitoring during suspicious transaction activities.

The project demonstrates how modern web technologies and intelligent fraud detection techniques can be applied to enhance financial security through real-time monitoring and automated decision-making. Experimental results indicate that the system accurately identifies suspicious transactions and reliably delivers fraud alerts to users and administrators.

Overall, the proposed system offers a practical, secure, reliable, and scalable solution for improving digital transaction security and can serve as a strong foundation for future intelligent fraud prevention applications.

REFERENCES

[1] S. J. Stolfo, W. Fan, W. Lee, A. Prodromidis, and P. K. Chan, “Credit Card Fraud Detection Using Meta-Learning: Issues and Initial Results,” AAAI Workshop on AI Methods in Fraud and Risk Management, 2000.
[2] V. Bhusari and S. Patil, “Study of Hidden Markov Model in Credit Card Fraudulent Detection,” International Journal of Computer Applications, vol. 20, no. 5, pp. 33–38, 2011.
[3] A. Srivastava, A. Kundu, S. Sural, and A. Majumdar, “Credit Card Fraud Detection Using Hidden Markov Model,” IEEE Transactions on

© Author(s). This work is peer-reviewed, openly published, and permanently archived
This article is openly accessible and reusable with proper attribution.

Dependable and Secure Computing, vol. 5, no. 1, pp. 37–48, 2008.
[4] FastAPI Documentation, Python Framework for Building APIs.
[6] Scikit-learn Documentation
[7] Python Documentation for Web Development and Data Processing.
[8]SQLAlchemy Documentation, Python ORM for Database Management..
[9] JWT Documentation, JSON Web Token Authentication Standard.
[10] Research Articles on Fraud Detection System

© Author(s). This work is peer-reviewed, openly published, and permanently archived
This article is openly accessible and reusable with proper attribution.