PayGuard/FraudShield AI:AI- Based Payment Fraud Detection System

Shruti Ghanvat[1], Ms. Shital Waghmare[2], Samruddhi Salunkhe[3], Saniya Dhagare[4]. Vaidehi Biramane[5]. Shradha Dash[6]

[1,2,3,4,5,6]*Department of Computer Science Engineering Yashoda Technical Campus, Satara Maharashtra, India*

Abstract – Online payment fraud has increased rapidly with the growth of digital transactions, UPI payments, and mobile banking services. This paper presents the implementation of PayGuard: AI-Based Payment Fraud Detection System, which helps detect and prevent fraudulent payment activities using Artificial Intelligence and Machine Learning techniques. The system analyzes transaction details such as payment amount, transaction time, user behavior, device information, and transaction history to identify suspicious activities in real time. Additionally, the system stores user transaction records and generates instant fraud alerts and personalized security recommendations to improve payment safety. AI algorithms are used to recognize unusual transaction patterns and reduce the risk of fake or unauthorized payments. The proposed system aims to improve digital payment security, reduce financial fraud, and increase user trust in online payment platforms.

Keywords— Artificial Intelligence (AI), Machine Learning, Payment Fraud Detection, Digital Payments, Cyber Security.

I.INTRODUCTION

In recent years, digital payment systems such as UPI, mobile banking, credit cards, and online wallets have become an important part of daily life. People prefer online transactions because they are fast, simple, and convenient. However, the rapid growth of digital payments has also increased the risk of online payment frauds such as fake payment screenshots, phishing attacks, unauthorized transactions, and identity theft. These fraud activities can cause major financial losses for both users and financial institutions.

Traditional fraud detection methods are often unable to detect new and advanced fraud techniques in real time. Therefore, there is a need for an intelligent and automated system that can identify suspicious activities quickly and accurately. Artificial Intelligence (AI) and Machine Learning (ML) technologies provide powerful solutions for analyzing transaction patterns and detecting unusual behavior.

This project presents PayGuard/ FraudShield: AIBased Payment Fraud Detection System, which is designed to improve the security of digital transactions. The system monitors transaction details such as payment amount, transaction history, device information, and user behavior to identify possible fraud activities. It also stores user transaction records and provides instant fraud alerts and personalized security suggestions. The main objective of PayGuard is to reduce financial fraud, improve transaction security, and increase user trust in digital payment platforms through smart AI-based analysis and real-time monitoring.

1.1 Need for Carbon Footprint Tracking.

- Increasing number of online payment frauds.
- Detection of fake payment screenshots and scams.
- Need for real-time transaction monitoring.
- Reduction of financial losses for users and banks.
- Improvement in digital payment security.
- Fast detection of suspicious activities using AI.

1.2 Role of a Carbon Footprint Tracking System.

- Detects fraudulent payment activities in real time.
- Monitors online transactions continuously.
- Identifies suspicious user behavior using AI and ML.
- Prevents fake payment screenshot scams.
- Sends instant fraud alerts and notifications.

- Protects users from financial losses.
- Stores and analyzes transaction history.
- Improves security and trust in digital payment systems.

1.3 Benefits of the Proposed System

- Provides real-time fraud detection.
- Reduces financial losses caused by online scams.
- Improves security of digital payment systems.
- Detects fake payment screenshots effectively.
- Sends instant alerts for suspicious transactions.
- Increases user trust in online payments.
- Reduces manual monitoring and verification work.
- Uses AI for accurate and fast fraud analysis.

1.4 Limitations of Existing Carbon Tracking Systems

- Existing systems have limited accuracy in detecting new fraud techniques.
- They are unable to detect fake payment screenshots effectively.
- Response time to suspicious transactions is slow.
- There are high chances of false alerts and detection errors.
- Real-time monitoring features are limited or unavailable.
- AI and Machine Learning technologies are not used effectively.
- User behavior and transaction patterns are poorly analyzed.
- Security against advanced cyber attacks is insufficient.

II.LITERATURE SURVEY

The rapid growth of digital payment systems has increased the risk of online payment fraud and cyber attacks. Many researchers have proposed different techniques and systems to detect fraudulent transactions and improve payment security. Traditional fraud detection methods mainly use rule-based systems, but these methods are less effective in identifying new and advanced fraud patterns. Several studies have shown that Artificial Intelligence (AI) and Machine Learning (ML) algorithms can improve fraud detection accuracy by analyzing transaction behavior and identifying suspicious activities in real time. Algorithms such as Decision Tree, Random Forest, Logistic Regression, and Neural Networks are commonly used for fraud detection systems. Some existing systems focus on detecting unauthorized transactions, while others analyze user behavior, device information, and payment history to identify fraud risks. Recent research also highlights the importance of detecting fake payment screenshots and phishing attacks in digital payment platforms. Although many fraud detection systems are available, most of them still face limitations such as delayed detection, false alerts, and lack of real-time monitoring. Therefore, the proposed system, PayGuard: AIBased Payment Fraud Detection System, aims to provide a smarter and more efficient solution using AI-based analysis, instant fraud alerts, and real-time transaction monitoring to improve digital payment security.

2.1 Early Development of Payment Fraud Detection Tools

Early payment fraud detection systems were mainly based on manual verification and simple rule-based methods. Banks and financial institutions used fixed rules such as transaction limits, password verification, and OTP authentication to detect suspicious activities. These systems could identify only basic fraud cases and were not effective against advanced cyber attacks.

As digital payments and online banking increased, fraud techniques also became more complex. Traditional systems faced difficulties in detecting fake payment screenshots, phishing attacks, and unusual transaction patterns in real time. To improve security, researchers started using Artificial Intelligence (AI) and Machine Learning (ML) technologies for automated fraud detection.Modern fraud detection tools now analyze transaction history, user behavior, device information, and payment patterns to identify suspicious activities quickly and accurately. These developments have improved the efficiency and reliability of digital payment security systems.

Strengths:

- Simple and easy transaction monitoring.
- Provides basic security for digital payments.
- Detects suspicious transactions using predefined rules.

- Supports OTP and password authentication.
- Helps reduce basic online payment frauds.
- Stores transaction history for verification.
- Improves safety in online banking systems.

Limitations:
- Unable to detect advanced fraud techniques.
- Limited real-time monitoring capabilities.
- High chances of false alerts.
- Cannot effectively detect fake payment screenshots.
- Depends mainly on fixed rule-based systems.

2.2 Rise of Data Analytics and IoT in Carbon Tracking
With the growth of digital payments and online banking, the use of Data Analytics and Artificial Intelligence (AI) has increased in fraud detection systems. Modern systems collect and analyze large amounts of transaction data such as payment amount, location, device information, and user behavior to identify suspicious activities. Machine Learning algorithms help detect unusual transaction patterns and improve fraud detection accuracy. AI-based systems can monitor transactions in real time and quickly identify fake payments, phishing attacks, and unauthorized access. The rise of Data Analytics and AI has made fraud detection systems faster, smarter, and more efficient compared to traditional rule-based methods. These technologies also help reduce financial losses and improve the security of digital payment platforms.

Limitations:
- Requires large amounts of transaction data for analysis.
- High implementation and maintenance cost.
- Risk of false fraud alerts in some cases.
- Complex AI models may be difficult to manage.
- Data privacy and security concerns.
- Requires continuous system updates and training.
- Dependence on internet and digital infrastructure.

III. METHODOLOGY

The methodology of PayGuard: AI-Based Payment Fraud Detection System involves several phases to detect and prevent fraudulent payment activities effectively.

3.1 Data Collection
In this phase, the system collects transaction-related data from users and digital payment platforms. The collected data includes:
- Transaction amount
- Date and time of payment
- User transaction history
- Device information
- Payment method (UPI, card, wallet, etc.)
- IP address and location details
- Login and user behavior patterns

The collected data is stored securely in the database for further analysis. This information helps the AI and Machine Learning models identify suspicious activities and detect possible fraud transactions accurately.

3.2 Activity Processing and Classification
In this phase, the collected transaction data is processed and analyzed using Artificial Intelligence (AI) and Machine Learning (ML) techniques. The system examines user activities such as transaction amount, payment frequency, device usage, login patterns, and transaction location. After processing the data, the system classifies transactions into two categories:
- Genuine Transaction
- Fraudulent or Suspicious Transaction

Machine Learning algorithms compare current transaction behavior with previous user history to identify unusual activities. If suspicious patterns are detected, the system marks the transaction as risky and generates an alert for further verification.

3.3 Fraud Risk Calculation
In this phase, the system calculates the fraud risk level of each transaction based on analyzed transaction data and user behavior. Factors such as unusual payment amount, unknown device access, multiple failed login attempts, suspicious transaction location, and abnormal transaction frequency are considered.
The AI-based model assigns a risk score to every transaction:
- Low Risk
- Medium Risk
- High Risk

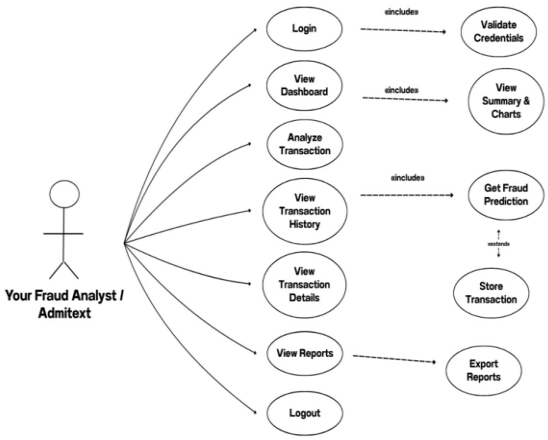
If the transaction receives a high-risk score, the system immediately flags it as suspicious and sends alerts to the user or financial institution for verification. This

process helps in preventing fraudulent transactions and improving digital payment security.

3.4 Response Generation Based on Fraud Risk Level

- In this phase, the system generates responses and alerts based on the calculated fraud risk level of each transaction. The AI-based system analyses the risk
  score and provides appropriate actions for user safety.
- Low Risk: Transaction is approved normally.
- Medium Risk: User receives a warning notification for verification.
- High Risk: Transaction is temporarily blocked, and an instant fraud alert is generated.
- The system also provides personalized security suggestions such as changing passwords, verifying account details, or enabling additional authentication methods. This process helps users take quick action against possible payment frauds and improves overall transaction security.
- High-Risk Transaction: The system identifies the transaction as suspicious or fraudulent, temporarily blocks the payment if required, and sends an instant fraud alert with security recommendations to the user.

Digaram:



3.5 Testing and Deployment

Testing & Deployment Phase: The PayGuard system's efficiency in identifying payment frauds is ensured during this phase, which includes hardware and software needs.

Hardware:

- Intel i5 or higher RAM: Minimum8GB
- Storage: 256 GB or more GPU,
- For faster model training Device: Laptop/Desktop,
- Internet Connection: Required for dataset download and deployment

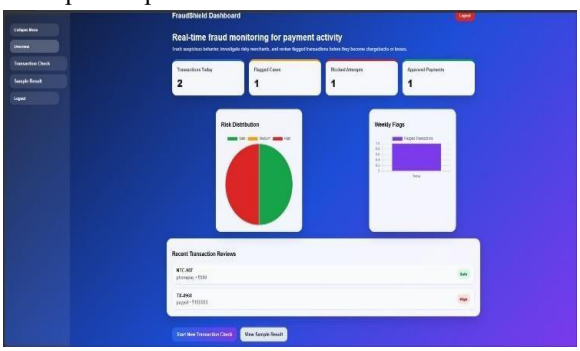
Software:

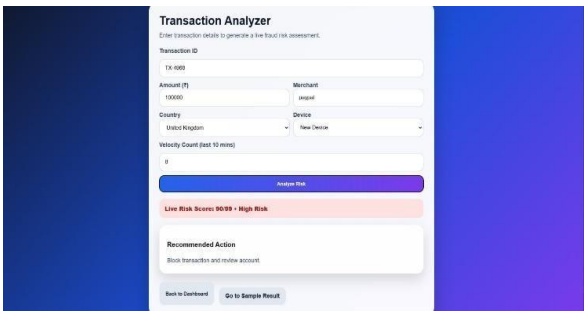
- OS: Windows, Linux, or macOS
- Programming language: Python
- Core AI/ML libraries: Tensorflow/keras, NumPy &
  Pandas, Scikit-learn
- Image & TextProcessing: OpenCV, EasyOCR/ Tesseract
- Development Tools: IDE: VS Code
- Recommended Dataset: PaySim

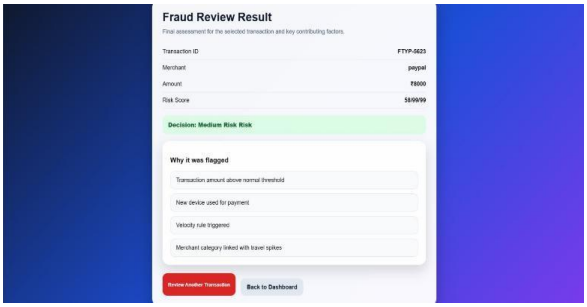
IV. RESULTS AND OUTPUT

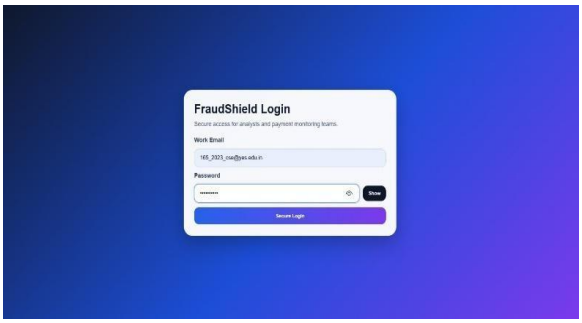
The PayGuard: AI-Based Payment Fraud Detection System is able to identify suspicious and fraudulent payment actions through Artificial Intelligence and Machine Learning algorithm

Example Output:









V.CONCLUSION

The proposed system, PayGuard: AI-Based Payment Fraud Detection System, provides an effective solution for detecting and preventing online payment frauds using Artificial Intelligence and Machine Learning techniques. The system analyzes transaction details, monitors user behavior, and identifies suspicious activities in real time. PayGuard helps improve the security of digital payments by generating instant fraud alerts, detecting fake payment activities, and reducing financial losses. The system also stores transaction history and provides personalized security suggestions to users for safer online transactions. Overall, the project enhances trust, safety, and reliability in digital payment platforms and can be widely used in banking systems, UPI applications, e-commerce platforms, and online financial services.

VI.FUTURE SCOPE

1. Integration with advanced Deep Learning algorithms for higher fraud detection accuracy.
2. Addition of facial recognition and biometric authentication for improved security.
3. Real-time integration with banking and UPI systems.
4. Detection of deepfake payment proofs and advanced cyber scams.
5. Development of a mobile application for instant fraud monitoring.
6. Cloud-based deployment for large-scale transaction analysis.
7. Use of Blockchain technology for secure and transparent transactions.
8. Improved AI models for faster and smarter fraud prediction.

REFERENCES

[1] Praveen Kumar, K. R., Reddy, V. S., & Kumar, A. (2024). Online Payment Fraud Transaction Detection using Machine Learning. In *Proceedings of IEEE International Conference on Computing and CommunicationSystems*. https://ieeexplore.ieee.org/document/10866604

[2] *Artificial Intelligence and Data Engineering*. https://ieeexplore.ieee.org/document/10560838

[3] Patel, R., Shah, D., & Mehta, P. (2025). Real-Time Fraud Detection in Financial Transactions Using SVM and Data Mining Techniques. In *Proceedings of IEEE International Conference on Data Science and Engineering*. https://ieeexplore.ieee.org/document/10956853

[4] Banerjee, S., Roy, P., & Ghosh, S. (2023). Fraud Detection in Banking Transactions Using Machine Learning. In *Proceedings of IEEE International Conference on Intelligent Systems and Applications*. https://ieeexplore.ieee.org/document/10091067

[5] Verma, A., Singh, R., & Kumar, S. (2024). Improving Fraud Detection in Mobile Payments with Machine Learning Ensembles. In *Proceedings of IEEE International Conference on Smart Computing and Communication*, 1–6. https://ieeexplore.ieee.org/document/10800126