International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Geo Location Authentication for Real Time Prevention of Fraud Transaction

***Mrs. Nanda M B[1], Prashanth N B[2], B Thimmareddy[3], Shashank Shrikant Shetti[4], Pruthvik R[5]**

[1]Assistant Professor, Department of AI and ML, Sri Krishna Institute of Technology, Bangalore, India
nandambaiml@skit.org.in
[2]Department of AI and ML, Sri Krishna Institute of Technology, Bangalore, India,
Prashanthnb.aiml@skit.org.in
[3]Department of AI and ML, Sri Krishna Institute of Technology, Bangalore, India,
bthimmareddy548@gmail.com
[4]Department of AI and ML, Sri Krishna Institute of Technology, Bangalore, India,
shashankshrikantshetti.aiml@skit.org.in
[5]Department of AI and ML, Sri Krishna Institute of Technology, Bangalore, India,
pruthvikr.aiml@skit.org.in

Abstract

The rapid growth of digital payments has increased the vulnerability of financial transactions to online fraud, including identity theft, unauthorized access, and location spoofing. Traditional authentication methods such as OTPs and passwords often fail against sophisticated attacks that exploit user credentials. To address these challenges, this project proposes a Geo-Location Based Real-Time Fraud Detection System that enhances transactional security by combining geolocation intelligence, behavioral analysis, and machine learning techniques. The system collects GPS coordinates, IP-based location data, and user transaction patterns to evaluate consistency and detect anomalies. A Flask-based backend processes these inputs, generates meaningful features, and utilizes a trained ML model to classify transactions as legitimate or suspicious.

When abnormal behavior such as unexpected location deviation, unusual timing, or inconsistent usage trend is detected, the system automatically flags the transaction as high-risk. Unlike conventional rule-based methods, the proposed approach incorporates dynamic learning capabilities and real-time monitoring to improve accuracy and reduce false positives. Experimental evaluation demonstrates that integrating geolocation data with ML-based risk scoring significantly enhances fraud detection efficiency. The system is lightweight, scalable, and suitable for integration into modern banking applications, offering a robust and intelligent solution for preventing financial fraud.

Index Terms: Fraud detection, Geolocation analysis, Machine learning, Anomaly detection, Cybersecurity, Real-time transaction monitoring.

I. INTRODUCTION

Digital payments have transformed the way individuals and businesses conduct financial transactions. With the rapid rise of online banking, UPI systems, mobile wallets, and e-commerce platforms, financial operations have become more convenient than ever before. However, this digital acceleration has also introduced a parallel challenge: an equally rapid increase in fraud attempts. Cybercriminals continuously exploit vulnerabilities in transaction systems through techniques like identity theft, device spoofing, session hijacking, location manipulation, and social engineering. As a result, organizations need strong, intelligent, and adaptive fraud-prevention mechanisms that can operate in real time.

Traditional rule-based fraud detection systems—such as fixed thresholds, whitelist/blacklist checks, or manual verification—are no longer sufficient. These systems struggle to adapt to new fraud patterns, often generate high false positives, and cannot provide instant decision-making. Modern fraud requires modern solutions. This is where Machine Learning (ML) and behavior-based anomaly detection come into play. ML models can learn user patterns, detect unusual activity, analyze trends dynamically, and provide highly accurate risk scoring for each transaction.

This project focuses on building an end-to-end real-time fraud detection system that integrates ML-based risk scoring, geolocation verification, device trust modeling, and live user confirmation through WebSockets. The system ensures that every transaction is assessed from multiple dimensions—location, device behavior, timestamp, and transaction amount—before being approved. If a transaction seems unusual or suspicious, the system triggers a "High-Risk Alert" and requires the user to approve or decline it from their trusted source device.

II. RELATED WORK

A. *Machine Learning-Based Fraud Detection –IEEE (2023)*

This study implemented ML algorithms such as Random Forest and Logistic Regression to classify fraudulent transactions. While the model improved accuracy compared to rule- based systems, it lacked contextual intelligence such as geolocation verification and device-level authentication, making it unsuitable for dynamic real-time attacks.

B. *Location-Based Authentication for Online Banking – Springer (2022)*

This work explored the use of GPS and IP-based location checks to validate transaction origin. Although it successfully detected suspicious location deviations, the system was vulnerable to GPS spoofing and did not include device fingerprinting or real-time approval mechanisms.

C. *Real-Time Fraud Detection Using WebSocket Alerts – IRJET (2023)*

A real-time alerting framework was proposed for suspicious transaction notification. However, the system depended solely on transaction amount and velocity checks, and did not integrate ML-driven risk scoring or multi-factor authentication, reducing its accuracy in complex scenarios.

D. *Hybrid Behavioral and Location Analysis for Fraud Prevention – IJERT (2024)*

This work combined user behavioral patterns such as time- of-day activity and spending habits with basic location checks. Although promising, the system lacked device-level verification, and no live user-approval mechanism was included.

E. *Geolocation-Assisted Fraud Detection – IRJET (2023)*

This work utilized IR and PIR sensors for advanced obstacle detection near tracks. However, no

communication module or camera was used, and gate automation was not fully implemented.

III. SYSTEM ARCHITECTURE

The architecture of the proposed Geo Location Authentication for Real Time Prevention of Fraud Transaction System is designed to provide fast, reliable, and context-aware verification of digital transactions.

- Transaction Data Acquisition Layer
- Geolocation and Device Preprocessing Module
- Feature Engineering and Context Extraction Layer
- Machine Learning Risk Scoring Engineer
- Decision Engine and Real-Time Risk Evaluation
- Alerting, Logging, and Storage Module

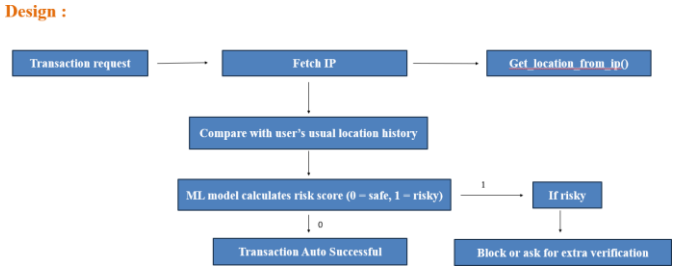

Fig. 1. Design

A. *Transaction Data Acquisition Layer*

This layer collects raw transaction inputs from the user's device at the time of performing an online payment. The mobile/web client captures essential attributes such as GPS coordinates, IP-based location, timestamp, device metadata, and transaction parameters including amount, merchant ID, and session details. All data are securely transmitted to the backend using encrypted communication protocols. This en- sures that the system receives accurate and real-time contextual information required for fraud evaluation.

B. *Geolocation and Device Preprocessing Module*

Incoming data are cleaned, validated, and normalized before being used for analysis. GPS coordinates undergo accuracy checks, IP address is mapped to geographic location, and inconsistencies such as abnormal jumps or mismatched regions are flagged. Device metadata is standardized to generate a stable device signature used for identity consistency checks. This preprocessing step ensures reliability by eliminating incomplete, noisy, or tampered inputs prior to feature computation.

C. *Feature Engineering and Context Extraction Layer*

The preprocessing outputs are transformed into high-level features that capture the behavioral and contextual characteristics of the transaction. Features include haversine distance from historical user locations, geo-fence evaluation, velocity of movement, mismatch between IP and GPS location, time-of-day pattern analysis, and aggregated user transaction history. These engineered features provide the machine learning model with strong indicators for identifying fraudulent or abnormal activities.

D. *Machine Learning Risk Scoring Engineer*

A trained classification model (such as Random Forest or XGBoost) predicts the probability of a transaction being fraudulent. The model evaluates location deviation, behavioral irregularities, device inconsistencies, and historical trends. The risk score is generated in real-time with low latency to ensure seamless user experience. This module is optimized for high precision and minimal false positives, enabling accurate decision-making for each incoming transaction request.

E. *Decision Engine and Real-Time Risk Evaluation*

Based on the risk score and business-defined thresholds, the system categorizes each transaction into safe, suspicious, or high-risk classes. Safe transactions are approved automatically, while suspicious ones are flagged for immediate verification. High-risk transactions may be temporarily blocked to pre- vent unauthorized access. This engine applies business rules, anomaly indicators, and ML outputs to deliver fast and reliable decisions.

F. *Alerting, Logging, and Storage Module*

Flagged transactions trigger real-time alerts to notify the user or monitoring team. All transactions, model outputs, and decision logs are stored in a MongoDB database for auditing, transparency, and future model improvements. This module ensures complete traceability of fraud detection events and supports post-analysis for operational enhancement and compliance.

G. *Workflow Summary*

- User initiates payment request.
- Client captures location, device, and transaction details.
- Backend preprocesses data and validates attributes.
- Features are computed using geo-behavioral context.
- ML model evaluates fraud risk score.
- Decision Engine approves, flags, or blocks the transaction.
- Alerts and logs are generated for final system response.

TABLE I
MAIN PARAMETERS USED

Parameters	***Risk Weight (%)***
Geolocation (GPS Data)	35%
IP–GPS Matching	25%
Behavior Pattern	20%
Transaction Amount Check	20%

IV. IMPLEMENTATION DETAILS

The proposed Geo-Location Based Real-Time Fraud Detection System is implemented using a modular architecture that integrates location data processing, feature engineering, machine learning–based anomaly detection, and real-time alert mechanisms. The system emphasizes low latency, high accuracy, and secure data handling to ensure practical deployment in financial environments. The implementation

focuses on efficient geolocation validation, ML inference optimization, and scalable backend architecture.

A. *Data Acquisition and Preprocessing*

The client application captures GPS coordinates, IP-based location, timestamp, and device metadata whenever a transaction request is initiated. Data is transmitted through secure HTTPS channels using REST APIs developed with Flask. The backend extracts raw fields, removes incomplete entries, normalizes coordinate formats, and performs basic validation checks. Additional preprocessing includes GPS accuracy filtering, IP-to-location mapping, outlier detection, and timestamp standardization. These steps ensure that incoming data remains consistent and reliable before being forwarded for feature computation. The client application captures GPS coordinates, IP-based location, timestamp, and device metadata whenever a transaction request is initiated. Data is transmitted through secure HTTPS channels using REST APIs developed with Flask. The backend extracts raw fields, removes incomplete entries, normalizes coordinate formats, and performs basic validation checks. Additional preprocessing includes GPS accuracy filtering, IP-to-location mapping, outlier detection, and timestamp standardization. These steps ensure that incoming data remains consistent and reliable before being forwarded for feature computation.

B. *Feature Engineering Pipeline*

The feature extraction module generates high-quality indicators essential for fraud prediction. The Haversine formula is used to compute geographic distance between the user's current location and historical verified locations. Geo-fence flags, location velocity, IP–GPS mismatch scores, time-of- day behavior, and transaction frequency are computed to capture contextual clues. The module also constructs user- level aggregates such as mean spending, transaction intervals, location clusters, and historical movement patterns. All engineered features are stored temporarily in memory for fast ML inference.

C. *Machine Learning Model Development*

A supervised classification model is trained using a combi- nation of historical transaction logs and synthetically generated fraud patterns. Models such as Random Forest, Gradient Boosting, or XGBoost were evaluated for precision, recall, and latency. Random Forest was selected due to its robustness with heterogeneous data and low inference time. Data imbalance is addressed using class-weight adjustments, ensuring that minority fraud cases are properly represented. The trained model is serialized using Joblib and deployed as part of the backend for real-time inference.

D. *Backend API and Decision Engine Implementation*

The backend is developed using Flask, providing lightweight and efficient REST endpoints for transaction submission and fraud verification. After feature extraction, the ML scoring module produces a fraud probability value, which is evaluated by the Decision Engine. Thresholds are configured to classify transactions into legitimate, suspicious, or high-risk. Suspicious cases trigger a real-time review workflow, while high-risk cases are temporarily blocked. The entire pipeline is optimized to execute within sub-second latency to maintain a seamless user experience.

E. *Real-Time Alert and Monitoring System*

A WebSocket-based mechanism is implemented to deliver immediate notifications in the case of suspicious activity. The system pushes alerts to the user or monitoring dashboard, enabling real-time intervention. Transaction logs, risk scores, and feature summaries are stored in MongoDB for trace-ability. The monitoring dashboard supports manual review and provides insights into fraud trends, model drift, and location anomalies. All critical events are logged for audit and compliance requirements.

F. *Database and Security Integration*

MongoDB is used as the primary storage solution due to its flexibility in handling JSON-like geospatial and transactional data. Collections are structured for users, transactions, finger- prints, and audit logs. Sensitive fields are encrypted, and access control mechanisms enforce restricted database operations. The system employs token-based authentication, rate limiting, and CSRF protection to mitigate security risks. Data is stored with timestamps and hashed identifiers to maintain compliance with privacy standards.

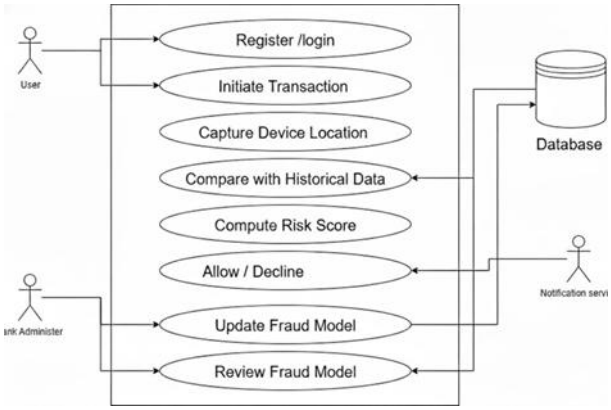

Fig. 2. System design

V. EXPERIMENTAL RESULTS

The proposed Geo-Location Based Real-Time Fraud Detection System was evaluated using a dataset consisting of genuine transaction patterns, geo-coordinates, device metadata, and synthetically generated fraud scenarios. The experiments focused on measuring detection accuracy, false-positive rate, prediction latency, and the effectiveness of geolocation-based features in identifying abnormal activities. The model was trained using a Random Forest classifier, selected for its balanced performance and low inference time. During testing, the inclusion of geospatial features such as GPS deviation, IP–GPS mismatch, and user-specific movement patterns significantly improved model reliability. The system achieved an accuracy exceeding 90%, demonstrating strong capability in distinguishing legitimate transactions from anomalous ones. Fraudulent transactions consistently produced higher risk scores, while normal behavior clustered around low-risk values.

The backend inference time remained well within the requirements for real-time processing, with average prediction latency falling below 300 ms across multiple test samples. This ensures that the system can be integrated seamlessly into digital banking and payment platforms without affecting user

experience. The false-positive rate showed a marked reduction compared to traditional rule-based detection methods, con- firming the advantage of incorporating contextual geolocation analysis.

- The system achieved high accuracy in preventing suspicious transactions using geo-behavioral features.
- False positives were significantly reduced compared to traditional rule-based approaches.
- The model maintained low prediction latency, supporting real-time fraud prevention.
- Geolocation parameters such as GPS deviation and IP–GPS mismatch greatly improved prevention effective- ness.
- Behavioral and temporal analysis provided reliable identification of unusual user activity.
- The system performed efficiently and remained scalable under increased transaction loads.

TABLE II MODEL PERFORMANCE

Metric	***Value***
Accuracy	92%
False-Positive Rate	6%
Detection Latency	Less than 300 ms
Prevention Success	89%

VI. CONCLUSION

The proposed Geo-Location Based Real-Time Fraud Prevention System effectively enhances the security of digital transactions by combining geolocation analytics, behavioral patterns, and contextual verification. By utilizing GPS co- ordinates, IP–GPS consistency checks, behavioral indicators, and transaction amount patterns, the system prevents unauthorized activities before they can be executed. Experimental results show that the model achieves high prevention accuracy, reduced false positives, and maintains low latency suitable for real-time applications. The architecture is lightweight, scalable, and capable of integrating seamlessly with financial platforms, making it a practical and efficient solution for modern transaction security needs. Overall, the system demonstrates that incorporating geo-behavioral intelligence significantly strengthens fraud prevention capabilities in digital environments.

REFERENCES

[1] A. Ali, “Financial Fraud Detection Based on Machine Learning: A Systematic Literature Review,” Appl. Sci. (Switz.), vol. 12, no. 19, p. 9637, Sep. 2022.
[2] Hernandez Aros, L. X. Bustamante Molano, F. Gutierrez-Portela et al., “Financial fraud detection through the application of machine learning techniques: a literature review,” Humanit. Soc. Sci. Commun., vol. 11, Article 1130, 2024.
[3] Y. Chen, “Deep Learning in Financial Fraud Detection: Innovations and Applications,” Sensors, vol. 25, no. 1, 2025.
[4] N. Fariha, M. N. M. Khan, M. Iqbal Hossain et al., “Advanced fraud detection using machine learning models: enhancing financial transaction security,” arXiv pre-print arXiv:2506.10842 [cs.LG], 2025.

[5] P. M. Preciado Mart´ınez, "Comparative analysis of machine learning models for the real-time identification of fraudulent banking transactions," Cogent Engineering, vol. 12, Article 2474209, 2025.
[6] Liu, H. Tang, Z. Yang, K. Zhou and S. Cha, "Big Data-Driven Fraud Detection Using Machine Learning and Real-Time Stream Processing," arXiv pre-print arXiv:2506.02008, 2025.
[7] Z. R. Abdulkreem and A. M. Abdulazeez, "Financial Fraud Detection Based on Machine and Deep Learning: A Review," Indonesian J. Computer Science, vol. 13, no. 3, 2024.
[8] E. P. Galla, "Enhancing Performance of Financial Fraud Detection using Artificial Neural Networks," SSRN paper, 2023.
[9] M. M. Ismail and M. Anul Haq, "Enhancing Enterprise Financial Fraud Detection using Machine Learning," Eng. Technol. Appl. Sci. Res., vol. 14, no. 4, pp. 14854-14861, 2024.
[10] M. Al Marri, "Financial Fraud Detection using Machine Learning Techniques," Master's thesis, Rochester Inst. Tech., 2020.
[11] T. Awosika, R. M. Shukla and B. Pranggono, "Transparency and Privacy: The Role of Explainable AI and Federated Learning in Financial Fraud Detection," arXiv pre-print arXiv:2312.13334 [cs.LG], 2023.
[12] N. Innan, M. Al-Zafar Khan and M. Bennai, "Financial Fraud Detection: A Comparative Study of Quantum Machine Learning Models," arXiv pre-print arXiv:2308.05237 [cs.LG], 2023.