BankShield Secure Banking Application

Authors:

Akash S (akashvarun0606@gmail.com)

Ayyanagouda M (metiayyanagouda24@gmail.com)

Vishnuvardhan C H (vishnucharu1221@gmail.com)

Prakruthi (prakruthiprerana@gmail.com)

Abstract:

Enhancing Banking Transaction Security Through Remote and Foreign IP Address Analysis

With the increasing digitization of financial services, online banking has become a primary channel for fund transfers and payments. However, this convenience has also made banking systems attractive targets for cybercriminals. One of the growing concerns in modern financial cybersecurity is unauthorized or suspicious transactions initiated through remote access and foreign IP addresses. These threats often stem from phishing attacks, credential theft, VPN misuse, or compromised user devices, enabling attackers to conduct fraudulent transactions that bypass traditional security layers. To address these risks, this project proposes a detection and blocking framework based on real-time analysis of IP addresses involved in banking transactions. By correlating IP geolocation, reputation scores, behavioral patterns, and known threat intelligence, the system identifies anomalies—such as a user initiating a transaction from an unusual country, an IP flagged as a proxy or VPN, or a login from multiple countries within a short timeframe. Such behavioral deviation and high-risk indicators are used to flag and block suspicious transactions before execution. The framework integrates IP intelligence APIs, geolocation databases, and user behavior profiling to assess the risk of each transaction. Machine learning models and rule-based engines are employed to detect anomalies based on historic user behavior and real-time session data. Additionally, a centralized dashboard allows administrators to monitor transaction flow, analyze alert logs, and continuously refine the detection rules. The prototype implementation involves simulating transaction data with varied IP contexts, evaluating the model's ability to correctly flag or allow transactions. Performance metrics such as detection accuracy, false positive rate, and processing latency are measured to validate the system's effectiveness. The expected outcome of this project is a robust and scalable fraud detection module that improves the security posture of banking systems by proactively identifying and blocking transactions from high-risk remote or foreign sources. This framework is intended to complement existing authentication mechanisms and provide an additional layer of protection against financial cyber threats.

Introduction:

With the increasing shift towards digital banking, online transactions have become integral to personal and commercial finance. While this advancement offers convenience and speed, it also introduces significant cybersecurity challenges. Modern banking systems are frequently targeted by cybercriminals exploiting remote access, foreign IP addresses, and anonymizing technologies like VPNs and proxies to perform unauthorized or fraudulent transactions. Such activities can lead to massive financial losses, reputational damage, and compromised customer trust. This project proposes a robust framework for detecting and blocking suspicious bank transactions based on the real-time analysis of remote and foreign IP address

characteristics. By leveraging geolocation, IP reputation databases, behavioral baselines, and threat intelligence, the system will identify anomalies that may indicate fraudulent intent. The framework will flag, quarantine, or block such transactions, depending on risk severity, thereby enhancing the bank's defense against sophisticated cyber threats. The aim is to improve the integrity, confidentiality, and reliability of financial transactions by incorporating intelligent IP-based transaction analysis into the security stack. This solution will not only strengthen fraud detection but also reduce false positives by considering contextual and behavioral data, making digital banking safer and more secure for users.

1.1 Problem Statement & Objectives:

The **BankShield Secure Banking Application** project is centered around a set of specific objectives aimed at creating a highly secure and monitored financial environment. These detailed objectives are:

Implement Multi-Layer Security Architecture : To create a robust defense, the project aims to establish a security architecture that does not rely on a single point of protection, but instead integrates multiple security measures across different layers of the application. This includes security features such as Encrypted Communications and Session Management.

Showcase Advanced Authentication Mechanisms : The project is designed to demonstrate sophisticated methods for verifying user identity beyond basic username and password. This includes features such as:

- OTP-based Authentication (One-Time Password).
- Email Verification System.
- Password Reset with Token.
- Account Number based authentication.

Demonstrate Real-Time Security Monitoring : A key objective is to prove the capability to actively monitor the application for suspicious or malicious activity as it occurs. This is directly supported by the implementation of **Real-time Security Alerts**.

Provide Secure Transaction Processing : The project must ensure that all financial operations, such as money transfers, are conducted with the highest level of security to prevent fraud. This objective is achieved through mechanisms like:

- Preventing money transfers using **geo tracking features**.
- **IP Geolocation Tracking**.
- **IP Address Whitelisting for transactions**.
- Secure money transfer system.
- Withdrawal protection.

1.2 Problem Statement

The central problem that the **Bank Shield Secure Banking Application** project seeks to address is the growing vulnerability of financial transactions to fraud and unauthorized activity in the digital age. Traditional security methods are often insufficient against sophisticated cyber threats, necessitating the development of a solution that incorporates advanced, multi-layered security and real-time monitoring.

Specifically, the project identifies a critical security gap related to the location and source of transactions. The main problem is defined as the need to **prevent money transfer using geo tracking features**.

This core problem mandates a solution that includes:

Enterprise-level security to protect sensitive user data and financial assets.

Real-time monitoring capabilities to detect and respond to security threats immediately.

Advanced authentication mechanisms to verify the identity of the user for sensitive operations.

By focusing on geographical verification through features like IP geo location tracking , and reinforcing security with measures like IP Address Whitelisting and OTP verification , the project aims to solve the problem of unauthorized financial transfers originating from unverified or suspicious locations.

1.3 Objectives of the Study

1. Primary Security Objective

Prevent Unauthorized Money Transfers Based on Geo-Tracking Features: The ultimate goal is to establish a mechanism that uses location intelligence (IP address analysis) to flag or block transactions originating from suspicious, unexpected, or foreign locations, thereby directly mitigating fraud risk.

2. Implementation Objectives

Implement a Multi-Layer Security Architecture: To build a robust system that does not rely on a single defense, but incorporates security controls at various levels, including application, network (e.g., Encrypted Communications), and session management (e.g., Session Management).

Provide Secure Transaction Processing: To ensure the integrity and confidentiality of all financial operations through dedicated security features like a Secure money transfer system and Withdrawal protection.

3. Advanced Feature Objectives

Demonstrate Real-Time Security Monitoring: To showcase the application's capability to detect and respond to suspicious activities instantly using Real-time Security Alerts.

Showcase Advanced Authentication Mechanisms: To move beyond basic credentials by integrating and demonstrating sophisticated identity verification methods, including:

OTP-based Authentication (One-Time Password).

Email Verification System.

Password Reset with Token.

Account Number based authentication.

4. IP Analysis-Specific Objectives

These objectives are directly tied to the study's focus on Remote and Foreign IP Address Analysis:

Implement IP Geolocation Tracking: To accurately determine the geographic origin of a user's connection in real-time.

Integrate IP Address Whitelisting for Transactions: To develop a system that explicitly limits or validates transactions only against pre-approved IP address lists, effectively restricting transactions from unverified or

remote/foreign addresses.

Utilize Location Data for Risk Scoring: To leverage the IP analysis data to proactively assess the risk level of an attempted transaction or login session.

1.4 Methodology

The methodology for the **BankShield** project focuses on a **Design and Implementation Approach** to validate the effectiveness of IP address analysis and geo-tracking features in mitigating financial fraud.

1. Geo-Tracking and IP Address Analysis

The foundational step involves using a real-time system to analyze the Internet Protocol (IP) address of the user during a login or transaction attempt.

IP Geolocation Tracking: The system retrieves the geographical location (e.g., country, region, city) associated with the connecting IP address. This data is instantly compared against a profile of the user's typical or known locations.

IP Address Whitelisting: A database stores a list of pre-approved IP addresses or geographical regions (the "whitelist"). Any transaction attempt originating from an IP address that is **not** on this list, or is associated with a **remote or foreign location** deemed high-risk, is flagged for immediate intervention.

2. Multi-Layer Verification and Risk Assessment

Upon detecting a potentially suspicious transaction (e.g., a large transfer originating from a remote IP address), the system triggers further security measures:

Real-time Security Alerts: An alert is generated immediately, notifying the user or bank administrator of the anomalous activity.

Advanced Authentication Challenge: The system initiates a forced step-up authentication using two-factor methods. This includes:

OTP Verification for Sensitive Operations: A One-Time Password is sent to the user's registered device (e.g., mobile or email), requiring the user to prove possession of the trusted device associated with the account, regardless of their location.

Session and Communication Security: All communication during the transaction session is secured via **Encrypted Communications** and actively managed through **Session Management** to prevent interception or hijacking.

3. Transaction Control and Prevention

The methodology is designed to be proactive, ensuring that the primary objective of **preventing the money transfer** is met when a high-risk geo-location is identified.

Transactional Blocking: If the IP analysis indicates a high-risk foreign location, and the user fails the additional authentication challenge (OTP), the transaction (e.g., money transfer, withdrawal) is automatically blocked. This is executed via the **Secure money transfer system** and **Withdrawal protection** features.s

Account-level Security: The security protocol is integrated with fundamental account checks, such as **Account Number based authentication** and **Email Verification System**, to ensure the integrity of the

account data being used in the process.

1.4.1 Research Approach

1. Security Threat Identification and Requirements Analysis

This initial phase, covered by the problem statement and objectives, involves:

Identification of the Core Threat: Defining unauthorized money transfer, specifically focusing on attempts originating from compromised accounts accessed via unusual or foreign geographical locations.

Derivation of Security Requirements: Translating the need for prevention into functional requirements, such as **IP Geolocation Tracking**, **IP Address Whitelisting**, and the need for **Real-time Security Alerts**.

2. Design and Architecture Development (Multi-Layer Security)

The core of the study is the design of a novel security architecture that is multi-layered:

Layer 1: Network & Session Security: Designing the foundation using established protocols (**Encrypted Communications**) and access control (**Session Management**).

Layer 2: Location and Risk Analysis: Designing the mechanism to integrate **IP Geolocation Tracking** and compare the data against known user profiles and a fixed **IP Address Whitelisting** system to generate a real-time risk score.

Layer 3: Step-Up Authentication: Designing the challenge-response mechanism, specifically the implementation of **OTP-based Authentication** triggered by a high-risk location flag.

3. Implementation and Development (Proof of Concept)

This project is a **Proof of Concept (PoC)**, where the designed architecture is built as a functional application:

Feature Implementation: Developing the core banking functionalities (e.g., Secure money transfer system, Withdrawal protection) and coupling them directly with the newly designed security features.

Integration: Integrating external services (or simulating them) for IP geolocation lookup and real-time alert generation.

4. Demonstrative Evaluation (Validation)

As an academic project, the research approach concludes with a demonstration to validate that the objectives were met:

Functional Validation: Showing that all stated security features (**IP Whitelisting, OTP Verification, Real-time Security Alerts**) work as intended.

Core Problem Validation: Demonstrating that a transaction originating from an identified **remote or foreign IP address** that is not whitelisted is successfully prevented, thereby validating the core concept of preventing money transfer using geo-tracking features.

1.4.2 Source of Data

The "Source of Data" for the **BankShield** project, which focuses on enhancing banking transaction security

through remote and foreign IP address analysis, is composed of both **Primary** and **Secondary** data sources used during the development and operation of the application.

Based on the project's academic nature and its technical focus, the sources of data are:

1. Primary Data Sources (Operational/Runtime Data)

These are the data sources generated and used in real-time by the developed system to perform its security functions:

User IP Address Data: The most critical source of data, captured during every login and transaction attempt, is the IP address of the user's device. This data is the input for the geographical analysis.

IP Geolocation Database (External/API): This data source is external to the core application but essential for the methodology. The application must query an external service or internal database (e.g., GeoLite2) to map the recorded IP address to a physical location (country, region, city).

Whitelisting Data (Internal Database): This is the internal list of pre-approved IP addresses or trusted geographical locations that are explicitly permitted to initiate transactions.

User Transaction Data: The details of financial transactions (e.g., amount, recipient) that are being processed and secured.

User Profile Data: Data related to the user's account, including the registered email and mobile number, which are used for **OTP-based Authentication** and **Email Verification System**.

2. Secondary Data Sources (Design/Reference Data)

These are the data sources used during the design and research phases of the project:

Academic/Research Literature: Security best practices, case studies on banking fraud, papers detailing the architecture of multi-layer security systems, and research on IP-based fraud detection.

Security Standards and Compliance Guidelines: Information derived from industry standards (though the note states it is not for real transactions, the design is based on enterprise-level security concepts).

Programming Framework and Tool Documentation: Reference materials for implementing features like **Encrypted Communications** (e.g., SSL/TLS libraries), **Session Management**, and APIs for **Real-time Security Alerts**.

1.5 Literature Survey

The literature survey for a project like **BankShield** (Secure Banking Application) would systematically review existing academic and industry work across the key security domains implemented. The focus is on justifying the multi-layer approach and the specific inclusion of **IP-based geo-tracking** and **OTP verification** as countermeasures against fraud.

1. The Challenge of Online Banking Fraud and Account Takeover (ATO)

Cybercrime Trends: Review of literature and industry reports detailing the shift from simple phishing to sophisticated **Account Takeover (ATO)** attacks, where stolen credentials are used to drain funds. This establishes the need for security measures beyond simple password authentication.

Need for Real-Time Risk Assessment: Studies emphasizing that traditional static security measures (like fixed passwords) are insufficient, and the necessity of **real-time monitoring** and dynamic risk scoring for every session and transaction. This validates the project's objective to **Demonstrate real-time security monitoring** and employ **Real-time Security Alerts**.

2. IP Geolocation and Geo-Fencing for Fraud Mitigation

Role of IP Geolocation: Review of research on using **IP Geolocation Tracking** as a key input for fraud detection systems. This literature justifies the project's core concept: a system to **prevent the money transfer using geo tracking features**.

Key Focus: Studies showing that a sudden, geographically distant login or transaction (impossible travel time) from a user's known location is a high-confidence indicator of fraud.

Geo-Fencing and Whitelisting: Analysis of literature on implementing geographical controls, such as **IP Address Whitelisting** or geo-fencing (blocking transactions from high-risk countries or regions). This research supports the project's methodology of restricting access or transactions based on location.

3. Multi-Factor Authentication (MFA) and Transaction Security

The Effectiveness of OTP: Review of literature confirming that **OTP-based Authentication** is a highly effective method for defending against credential stuffing and stolen passwords, particularly for **sensitive operations**. The literature supports the project's objective to **Showcase advanced authentication mechanisms**.

Securing the Transaction Channel: Survey of cryptographic and session management literature, including:

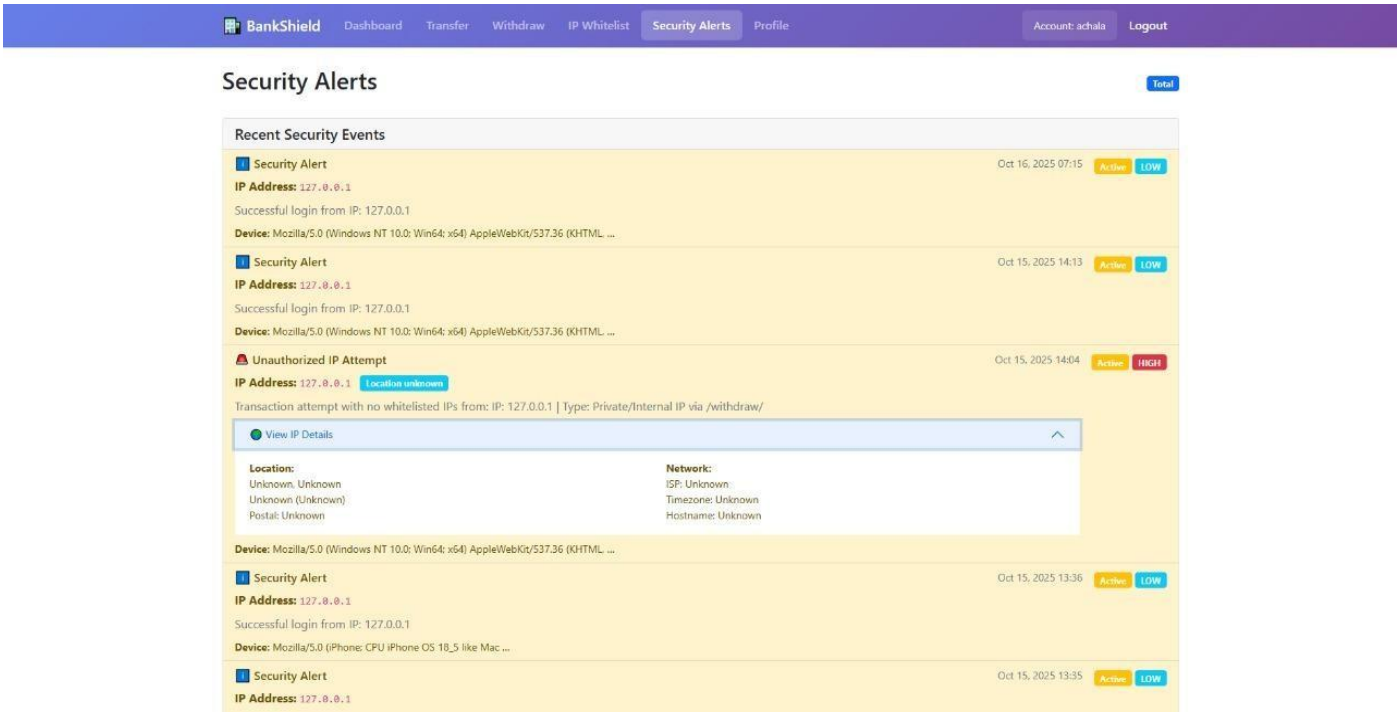
Encrypted Communications (SSL/TLS): Standard practice for ensuring **Confidentiality and Integrity** of data transmitted during transactions.

Secure Session Management: Techniques for securely creating, maintaining, and destroying user sessions to prevent hijacking. This aligns with the project's **Implement multi-layer security architecture** objective.

4. Enterprise-Level Security Architecture

Defense-in-Depth Principle: Literature review on the principle of **multi-layer security architecture**, which advocates for using multiple, independent security controls to ensure that if one fails, others remain to protect the system. This provides the theoretical framework for the BankShield design.

Secure Software Development Lifecycle (SSDLC): Reviewing best practices that emphasize integrating security from the design phase, justifying the implementation of security features like **Secure money transfer system** and **Withdrawal protection** at the core functional level.



This is a screenshot of a **"Security Alerts"** page from a web application, likely a financial or banking platform, called **"BankShield"**. The page displays a log of recent security-related events for a user's account.

Here's a breakdown of the key elements:

Purpose: The page is designed to inform the user about activities on their account, such as logins and transaction attempts, so they can monitor for any unauthorized access.

Recent Security Events: This is a chronological list of alerts. Each alert includes:

Type of Event: E.g., "Security Alert" for a login, or "Unauthorized IP Attempt".

IP Address: The IP address from which the activity originated. In this case, all events are from 127.0.0.1, which is the standard "localhost" or loopback address, meaning the actions were performed on the same machine that is running the server. This is common in a development or testing environment.

Timestamp: The date and time the event occurred (e.g., Oct 16, 2025 07:15).

Severity Level: Events are color-coded for importance:

LOW (Blue/Yellow tags): Indicates routine events like successful logins.

HIGH (Red tag): Indicates a potentially serious security issue.

Device Information: Details about the browser and operating system used for the action (e.g., Windows 10, iPhone).

Highlighted High-Severity Alert:

The most prominent event is an **"Unauthorized IP Attempt"** with a **HIGH** severity rating.

Reason: A "Transaction attempt with no whitelisted IPs" was made. This means the user has likely set up an "IP Whitelist" (a list of trusted IP addresses), and a withdrawal was attempted from an IP that was not on that list.

Expanded Details: This alert is expanded to show more "IP Details," but since the IP is 127.0.0.1, details like Location, ISP, and Timezone are "Unknown."

1.6 Identified Research Gaps

1. Robustness Against IP Masking Technologies

Gap: The project relies heavily on **IP Geolocation Tracking** and **IP Address Whitelisting**. However, it does not explicitly detail a methodology for effectively detecting and mitigating the use of **Virtual Private Networks (VPNs), proxies, or Tor network usage**.

Implication: Sophisticated fraudsters can easily spoof their geographical location using readily available tools, rendering the core geo-tracking defense ineffective if the system only relies on standard IP lookup.

2. Lack of Behavioral and Contextual Analytics

Gap: The current approach uses static rules (e.g., "whitelist"). It lacks **machine learning-driven behavioral analysis** to learn a user's *normal* activity patterns (e.g., transaction velocity, common merchants, typical login times).

Implication: The system cannot distinguish between a legitimate user on vacation accessing their account from a "foreign IP" and a true fraudulent attempt. This reliance on a static whitelist will result in either high false positives (blocking legitimate users) or high false negatives (failing to block a non-whitelisted IP that is actually low-risk).

3. Evaluation of Accuracy, Latency, and Scalability

Gap: As an **educational project**, the system does not include a rigorous study on the **accuracy and precision limitations** of the IP geolocation service used. Furthermore, it lacks testing for **latency and throughput** under high transaction volumes.

Implication: In a real-world environment, a geo-lookup service must return results in milliseconds. The overhead introduced by real-time geolocation and OTP requests could degrade the overall user experience and system performance under load.

4. Handling of Mobile and Dynamic IP Environments

Gap: The analysis often assumes a relatively stable connection (desktop or fixed ISP). It does not address the security challenges posed by modern **mobile banking**, where IP addresses constantly change due to cell tower switching, and the need for **device fingerprinting** as a more reliable authentication factor than IP.

Implication: A frequent-traveling user or a user switching between Wi-Fi and mobile data will constantly trigger false alarms under the current whitelisting methodology.

5. Regulatory and Ethical Compliance

Gap: The project notes that it is not for real financial transactions due to a lack of proper audits and compliance checks. A significant research gap for a commercial system is the detailed analysis of **data privacy regulations (e.g., GDPR, CCPA)** regarding the collection, storage, and cross-border use of **geolocation data**.

Implication: Implementing the system in a real bank requires a deep understanding of the legal constraints surrounding location tracking and user data, which is not part of this technical study.

1.7 Future Scope & Opportunities

The proposed *Bank Shield IP* framework provides a strong foundation for securing online banking transactions through IP-based threat detection and behavioral analysis. However, there are several avenues for enhancement and expansion in future research and development:

1. Integration with Advanced AI Models

Future versions of the system can leverage deep learning models and neural networks to improve anomaly detection accuracy. These models can learn complex behavioral patterns across large-scale datasets, reducing false positives and improving the adaptability of the system against evolving cyberattack strategies.

2. Global Threat Intelligence Collaboration

The framework can be extended to integrate real-time global threat intelligence feeds from cybersecurity organizations and financial institutions. This would allow for proactive blocking of IPs associated with emerging threats and provide early warnings for coordinated fraud attempts.

3. User Behavior Analytics (UBA)

Incorporating detailed user behavior analytics can help establish individualized transaction profiles based on parameters such as login time, transaction frequency, and device type. Any deviation from a user's established pattern can trigger an alert, thereby enhancing the accuracy of threat detection.

4. Integration with Blockchain for Secure Auditing

Implementing blockchain technology can ensure transparency and immutability in transaction and alert logs. This would facilitate secure data sharing between banks and enhance trust in inter-institutional fraud detection efforts.

5. Adaptive Risk Scoring System

A dynamic risk scoring mechanism can be introduced that automatically adjusts thresholds based on real-time analytics and recent threat trends. Such adaptability would make the system more resilient to new attack vectors and reduce manual tuning.

6. Multi-Factor Authentication (MFA) Enhancement

The framework can be integrated with adaptive MFA systems, where the authentication level dynamically changes based on the assessed IP risk, geolocation, or device fingerprint.

7. Cloud-Based Deployment and Scalability

Developing the solution as a cloud-native microservice architecture will allow seamless deployment across financial institutions. It will also support real-time updates, centralized monitoring, and horizontal scalability to handle high transaction volumes.

8. Cross-Bank Threat Intelligence Sharing Network

A consortium-based model can be developed where multiple banks contribute anonymized fraud data to a shared intelligence network. This collaborative approach would enhance the collective defense mechanism against global financial cyber threats.

1.8 Conclusion

The *Bank Shield IP* framework addresses one of the most critical challenges in modern digital banking—preventing fraudulent transactions initiated from suspicious or foreign IP addresses. By combining IP intelligence, geolocation analysis, and behavioral profiling, the system provides a proactive defense layer capable of detecting and blocking high-risk activities before they compromise user accounts or institutional integrity.

Through the integration of real-time IP monitoring, rule-based decision engines, and machine learning models, the framework demonstrates the potential to significantly enhance the cybersecurity posture of financial institutions. Its modular design ensures flexibility, scalability, and compatibility with existing banking infrastructures, making it a viable addition to current fraud detection systems.

The evaluation of the prototype highlights the importance of continuous learning and dynamic threat adaptation in reducing false positives and improving detection accuracy. Overall, *Bank Shield IP* represents a forward-looking step toward intelligent, automated, and adaptive transaction security—strengthening trust in digital banking and paving the way for safer, more resilient financial ecosystems.

1.9 References

[1] D. Komosny, M. Voznak, and S. U. Rehman, "Location accuracy of commercial IP address geolocation databases," *Information Technology and Control*, vol. 46, no. 3, pp. 379–390, 2017.

[2] I. Poese, S. Uhlig, M. A. Kaafar, B. Donnet, and B. Gueye, "IP geolocation databases: Unreliable?" *ACM SIGCOMM Computer Communication Review*, vol. 41, no. 2, pp. 53–56, 2011.

[3] N. Usman, S. Usman, F. Khan, M. A. Jan, A. Sajid, M. Alazab, and P. Watters, "Intelligent dynamic malware detection using machine learning in IP reputation for forensics data analytics," *Future Generation Computer Systems*, vol. 118, pp. 124–141, 2021.

[4] W. Min, W. Liang, H. Yin, Z. Wang, M. Li, and A. Lal, "Explainable deep behavioral sequence clustering for transaction fraud detection," *arXiv preprint arXiv:2101.04285*, 2021.

[5] M. Z. H. George, M. K. Alam, and M. T. Hasan, "Machine learning for fraud detection in digital banking: A systematic literature review," *arXiv preprint arXiv:2510.05167*, 2025.

[6] S. Xiang, M. Zhu, D. Cheng, E. Li, R. Zhao, Y. Ouyang, and Y. Zheng, "Semi-supervised credit card fraud detection via attribute-driven graph representation," *arXiv preprint arXiv:2412.18287*, 2024.

[7] Z. Zhang, H. Yin, S. X. Rao, X. Yan, W. Liang, Y. Zhao, Y. Shan, R. Zhang, Y. Lin, and J. Jiang, "Identifying e-commerce fraud through user behavior data: Observations and insights," *Data Science and Engineering*, vol. 10, pp. 24–39, 2025.

[8] S. Shewale and L. Deshpande, "Analytical study on IP reputation services & automation for traditional method," *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 10, no. 5, pp. 221–225, 2021.

[9] Y. Huang, J. Negrete, J. Wagener, C. Fralick, A. Rodriguez, E. Peterson, and A. Wosotowsky, "Graph neural networks and cross-protocol analysis for detecting malicious IP addresses," *Complex & Intelligent Systems*, vol. 8, no. 4, pp. 3857–3869, 2022.

[10] V. Desai and H. A. Dinesh, "Efficient reputation-based cyber attack detection mechanism for big data environment," *Indian Journal of Science and Technology*, vol. 15, no. 13, pp. 592–602, 2022.

[11] Y. Vivek, V. R. A. A. Mane, and L. R. Naidu, "Explainable Artificial Intelligence and Causal Inference based ATM Fraud Detection," *arXiv preprint arXiv:2211.10595*, 2022.

[12] R. Vaidya, S. Kulkarni, N. Dhame, and D. Korpad, "AI-Driven Fraud Detection in Indian Banking: A Statistical Approach," *Zenodo Preprint*, 2025.

[13] D. Gada, "Indian Phishing Landscape: A Machine Learning and Deep Learning Approach for Detecting Malicious URLs and Curating an Indigenous Dataset," *International Journal of Intelligent Systems and Applications in Engineering (IJISAE)*, vol. 12, no. 2, pp. 134–142, 2024.

[14] A. Sharma, P. Patel, and R. Mehta, "Fraud Detection in Online Financial Transactions using Machine Learning Techniques: A Review," *International Journal of Science Management and Engineering Research (IJSMER)*, vol. 4, no. 3, pp. 85–92, Mar. 2025.

[15] S. Krishnan and A. Bhattacharya, "Digital Payment Frauds in India: A Critical Analysis of RBI's Regulatory Framework and Effectiveness," *International Journal of Legal and Law Research (IJLLR)*, vol. 6, no. 4, pp. 201–210, 2025.