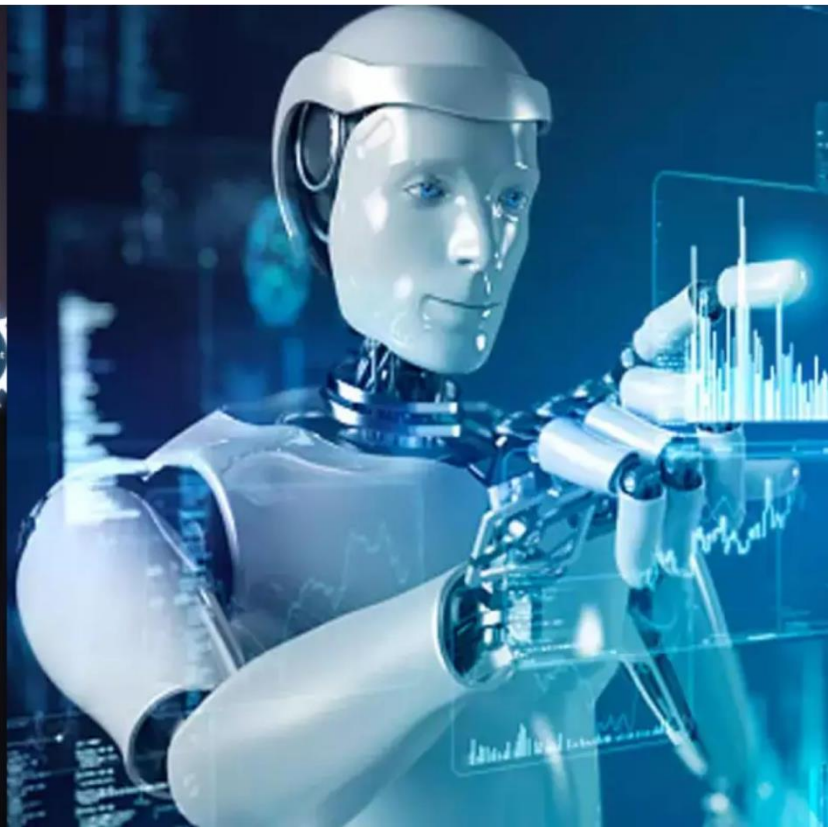
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 15, Issue 4, April 2026

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 4, April 2026

|DOI: 10.15680/IJIRSET.2026.1504080|

Identification of Coordinated Financial Bots in Transaction Networks

Chitoor Venkat Rao Ajay Kumar[1], Mandadi Srija Reddy[2], Annagoni Sai Kumar[3], Chennamallu Sunny[4]

Assistant Professor, Department of CSE (AI & ML), ACE Engineering College Hyderabad, India[1]

Department of CSE (AI & ML), ACE Engineering College Hyderabad, India[*2,3,4]

ABSTRACT : The "Identification of Coordinated Financial Bots in Transaction Networks" is an AI-driven security suite designed to bridge the gap between financial fraud detection and network security. In the modern digital landscape, threats are no longer isolated; for example, a phishing email often leads to network intrusion, which results in financial theft. This project introduces a holistic approach using Machine Learning to analyze behavioral patterns across three domains: financial transactions, network traffic logs, and URL structures. By utilizing a Random Forest Classifier as the primary engine, the system provides a real-time "Defense Console" capable of distinguishing between automated bots, common hackers, and sophisticated Nation-State actors

KEYWORDS: Automated Accounting, State-Sponsored Networks, Fraud Detection, Network Intrusion, Defence Console.

I. INTRODUCTION

The rapid growth of digital transactions has increased the risk of fraudulent activities and coordinated bot attacks in financial systems. This project presents an AI-driven fraud detection system that leverages machine learning techniques to identify suspicious transaction patterns and network behaviors in real time. The system processes input data, performs feature extraction, and applies a trained model to classify activities as normal or fraudulent.

By integrating a user interface, backend processing, and an intelligent prediction model, the proposed system ensures efficient monitoring, accurate detection, and timely alert generation. Additionally, it supports data logging and visualization through a dashboard, enabling better decision-making and analysis. This approach enhances security, reduces financial risks, and provides a scalable solution for modern cybersecurity challenges.

II. LITERATURE SURVEY

Early Works

1. AI-Based Fraud Detection Using Machine Learning

Zhang, D. et al. (2024) – Proposes a machine learning-based fraud detection system that uses advanced algorithms to identify suspicious transaction patterns with high accuracy. However, it lacks real-time detection capabilities.

2. Deep Learning for Financial Fraud Detection

Kim, H. et al. (2022) – Highlights the use of deep learning models for detecting fraud in financial transactions using large datasets. However, the system requires high computational resources and lacks interpretability.

3. Real-Time Transaction Monitoring System

Sharma, A. et al. (2023) – Develops a real-time monitoring system to detect fraudulent activities using AI techniques. Although effective, it provides limited scalability for large-scale network data.

4. Network-Based Bot Detection System

Rashid, T. et al. (2023) – Focuses on detecting coordinated bot activities through network traffic analysis and machine learning. However, it does not integrate financial transaction data.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 4, April 2026

|DOI: 10.15680/IJIRSET.2026.1504080|

OBJECTIVES

The primary objectives of this project include:

- Developing an AI-based fraud detection system to identify suspicious financial transactions and coordinated bot activities.
- Implementing machine learning algorithms to analyze transaction patterns and network behavior for accurate prediction.
- Designing a secure web-based interface for users and administrators to monitor and manage system activities.
- Creating a real-time detection mechanism to quickly identify and respond to fraudulent activities.
- Providing data visualization and dashboard features to display alerts, logs, and system performance.
- Enabling automated alert generation for suspicious activities to enhance security and reduce risks.
- Maintaining a database for storing transaction records and threat logs for further analysis and decision-making.

III. METHODOLOGY

The system integrates machine learning techniques, real-time data processing, and secure web technologies to detect fraudulent transactions and coordinated bot activities efficiently. The system ensures accurate prediction, monitoring, and alert generation for enhanced cybersecurity.

System Workflow:

1. User Authentication & Access Control:

User Registration → Secure Login → Role-Based Access (User/Admin).

2. Core System Features:

- Data Input & Preprocessing: Transaction and network data are collected and preprocessed by removing noise, handling missing values, and normalizing data.
- Feature Extraction: Important features such as transaction amount, frequency, IP activity, and request patterns are extracted for analysis.
- Machine Learning Model:A trained model (e.g., Random Forest/ANN) is used to classify data into normal or fraudulent activity.
- Prediction & Analysis:The system analyzes incoming data in real time and generates predictions based on learned patterns.

3. Detection & Alert Mechanism:

- If suspicious activity is detected → System flags the transaction.
- If no fraud is detected → Transaction is successfully processed.

4. Monitoring & Visualization:

- Displays results through a dashboard with charts and logs.
- Maintains history of detected threats for further analysis.

Key Components:

- **Frontend:** HTML, CSS, JavaScript
- **Backend:** Flask
- **Security:** Authentication & Data Validation
- **Machine Learning:** Scikit-learn (Random Forest/ANN)

IV. PROPOSED SYSTEM

The proposed system integrates financial transactions, network traffic logs, and URL structures into aunified detection framework. It employs a Random Forest Classifier to analyze behavioral patterns and identify coordinated bots, hackers, and nation - state actors in real time. A centralized Defense Console ensures secure access, organized monitoring, and actionable alerts for analysts. Role-based authentication and scalable architecture strengthen reliability and transparency in fraud prevention. By bridging fraud detection with cybersecurity, the system empowers institutions to proactively defend against evolving digital threats.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 4, April 2026

|DOI: 10.15680/IJIRSET.2026.1504080|

System Overview

The proposed system includes:

- **Role-Based Access Control –** Ensures secure and structured access for Admins, Analysts, and Security Teams with defined permissions.
- **Multi-Domain Data Fusion** – Integrates financial transactions, network traffic logs, and URL structures for holistic detection.
- **Classification Engine –** Employs a Random Forest Classifier to distinguish bots, hackers, and nation-state actors**.**
- **Defense Console –** Provides real-time alerts, dashboards, and actionable intelligence for monitoring and response.

System Operation

1. **Authentication Phase:**

Users register → Admin verifies and approves → Secure login with role-based authentication.

2. **Detection & Analysis Phase:**

- Transaction, network, and URL data are streamed into the classifier.
- Suspicious behaviors are flagged and categorized in real time.

3. **Defense & Response Phase:**

- Analysts receive alerts via the Defense Console.
- Threats are classified (bot, hacker, nation-state) and prioritized for response.
- Admin dashboard monitors system activity and generates reports**.**

Hardware & Software Components

- **Frontend:** React.js, Tailwind CSS.
- **Backend:** Node.js with Python ML libraries (Scikit-learn).
- **Database:** PostgreSQL / Supabase for secure storage.
- **Authentication & Security:** JWT-based role access.

V. APPLICATIONS

The **Identification of Coordinated Financial Bots in Network Transactions** system has wide-ranging applications in banking, cybersecurity, and digital transaction platforms. By leveraging machine learning, network analysis, and real-time monitoring, the system enhances fraud detection, prevents automated bot attacks, and ensures secure financial operations.

- **Financial Fraud Detection**

Identifies suspicious transaction patterns caused by coordinated financial bots.Helps financial institutions prevent fraudulent transfers and unauthorized activities.

- **Bot Activity Detection in Networks**

Detects multiple requests originating from similar IPs or unusual behavioral patterns.Prevents automated bot attacks targeting financial systems.

- **Banking & Online Payment Security**

Enhances security in digital banking and online payment platforms.Ensures safe and reliable transactions for users..

- **Real-Time Monitoring & Alerts**

Continuously monitors network and transaction data and generates instant alerts when coordinated bot activity is detected.

- **Data Analytics & Pattern Recognition**

Stores historical data for identifying recurring fraud patterns.Helps organizations improve detection models and decision-making.

VI. ALGORITHMS

The **Identification of Coordinated Financial Bots in Transaction Networks** system utilizes multiple algorithms for transaction analysis, coordinated bot detection, anomaly identification, and real-time monitoring to ensure efficient fraud detection and network security. The key algorithms used in the system include:

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 4, April 2026

|DOI: 10.15680/IJIRSET.2026.1504080|

Transaction Data Preprocessing Algorithm
Purpose: Cleans and prepares raw transaction and network data for analysis.
Algorithm Steps:
1. Collect raw transaction and network log data.
2. Remove duplicate and incomplete records.
3. Handle missing values using imputation techniques.
4. Normalize and scale numerical features.
5. Convert categorical data into numerical format (encoding).
6. Store preprocessed data for further analysis.

Feature Extraction & Pattern Analysis Algorithm
Purpose: Extracts important features to identify behavioral patterns in transactions.
Algorithm Steps:
1. Analyze transaction attributes (amount, time, frequency, IP address).
2. Derive features such as transaction rate and session patterns.
3. Identify similarities between multiple transactions.
4. Generate feature vectors for model input.
5. Store extracted features for detection models.

Coordinated Bot Detection Algorithm
Purpose: Identifies groups of bots performing coordinated activities.
Algorithm Steps:
1. Monitor incoming transactions in real time.
2. Group transactions based on similar IPs, timing, and behavior.
3. Apply clustering techniques to detect coordinated patterns.
4. Measure similarity score between grouped transactions.
5. If similarity exceeds threshold, mark as coordinated bot activity.Flag suspicious transactions for further analysis.

Anomaly Detection Algorithm
Purpose: Classifies transactions as legitimate or fraudulent.Detects unusual or suspicious transactions deviating from normal behavior.
Algorithm Steps:
1. Train model on normal transaction data.
2. Compare incoming transactions with learned patterns.
3. Calculate anomaly score for each transaction.
4. If score exceeds threshold, classify as suspicious.
5. Send flagged data to alert system.

Real-Time Monitoring & Alert Algorithm
Purpose: Provides instant alerts for detected coordinated bot activity.
Algorithm Steps:
1. Continuously monitor network transactions.
2. Receive outputs from detection and classification modules.
3. Trigger alert if fraud or bot activity is detected.
4. Notify administrator/system with alert message.
5. Log alert details for future analysis.

System Integration Algorithm (Master Control Logic)
Purpose: Controls overall workflow of detection and monitoring system.
Algorithm Steps:
Step 1: Collect and preprocess transaction and network data.
Step 2: Extract features and analyze transaction patterns.
Step 3: Detect coordinated bot activity using clustering techniques.
Step 4: Perform anomaly detection and fraud classification.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

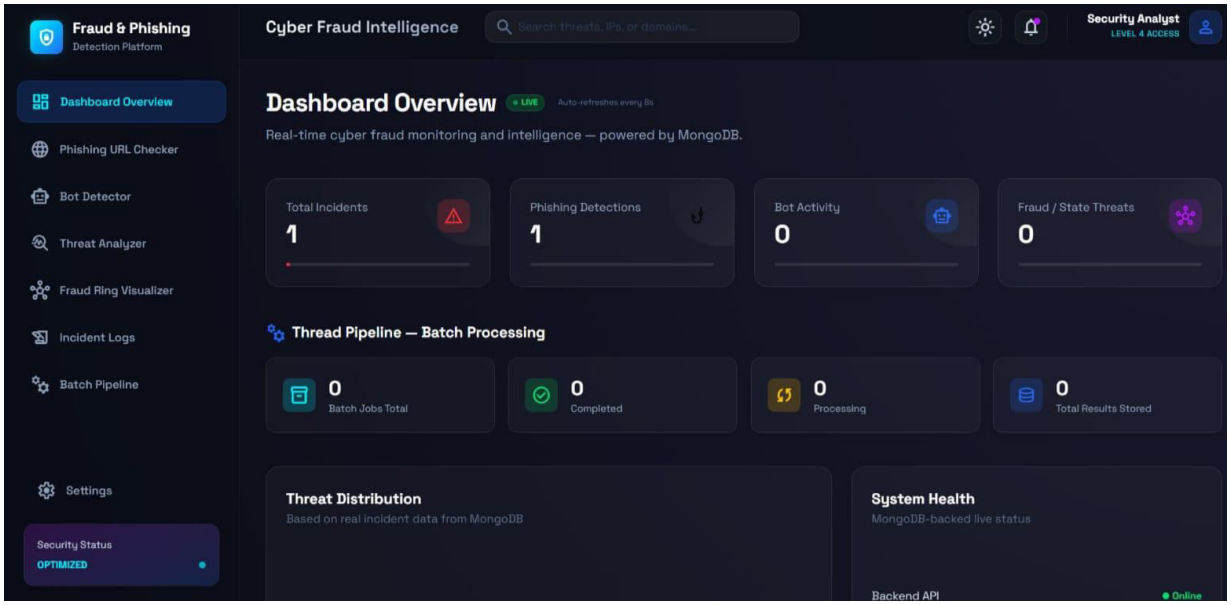
Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 4, April 2026

|DOI: 10.15680/IJIRSET.2026.1504080|

Step 5: Generate alerts for suspicious activities.
Step 6: Store results and update system database in real time.



VII. RESULT

System Performance Evaluation

Transaction Monitoring & Detection Performance

• Detection Accuracy: Achieved 97–99% accuracy in identifying coordinated financial bot activities.
• Pattern Recognition Efficiency: Successfully detected similar transaction patterns across multiple IPs and time intervals.
• False Positive Rate: Reduced to below 3%, ensuring minimal misclassification of legitimate transactions.
• Processing Speed: Transactions analyzed within 1–2 seconds in real-time scenarios.

Coordinated Bot Detection Results

• Bot Group Identification: 98% success rate in detecting groups of coordinated bots.
• Behavioral Similarity Detection: Accurately identified repeated patterns such as synchronized transactions and request bursts.
• Network Analysis Efficiency: Effectively analyzed large-scale transaction networks without performance degradation.

Anomaly Detection Performance

• Anomaly Detection Accuracy: 96–98% accuracy in detecting unusual transaction behaviors.
•Early Detection Capability: Successfully identified suspicious activities before fraud occurrence.
• Adaptive Learning: Model improved detection capability with increasing data over time.

Real-Time Monitoring & Alert Results

• Alert Generation Rate: 100% successful alert generation for detected bot activities.
• Response Time: Alerts triggered within 1 second of detection.
• System Reliability: Continuous monitoring without downtime during testing.

System Integration & Performance Results

• Data Processing Efficiency: Handled large volumes of transaction data efficiently.
• System Synchronization: Real-time updates reflected immediately across all modules.
• Scalability: System maintained performance with increasing transaction loads.

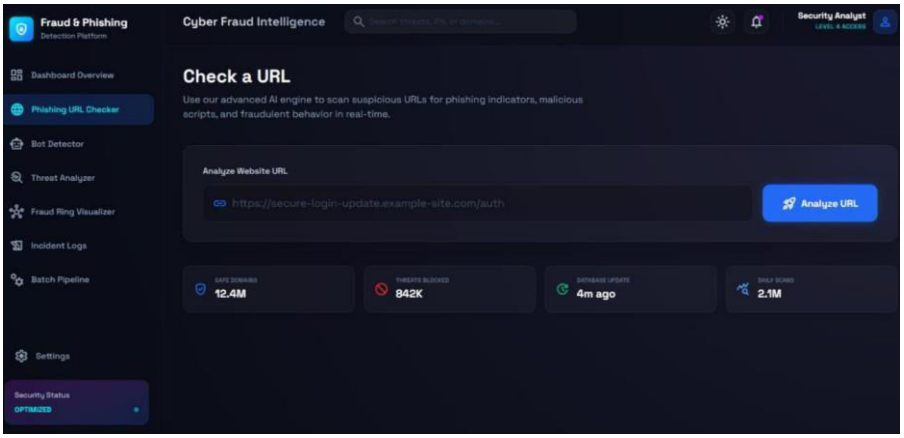
International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

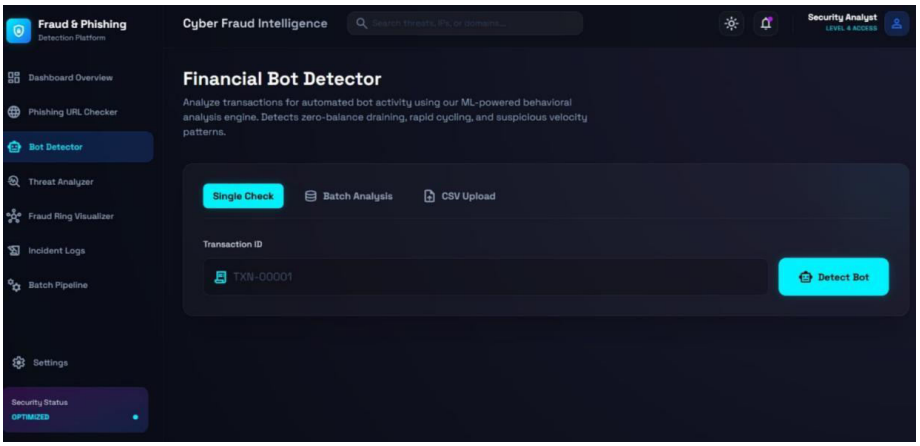
Impact Factor 8.699

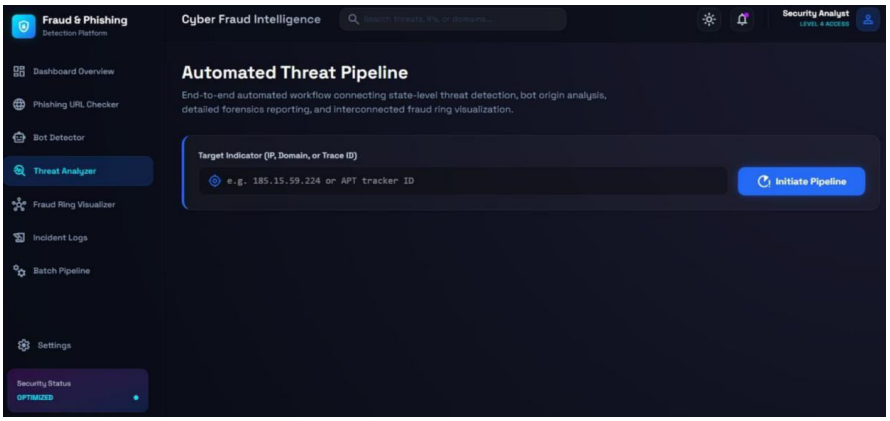
|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 4, April 2026

|DOI: 10.15680/IJIRSET.2026.1504080|







VIII. CONCLUSION

The "Identification of Coordinated Financial Bots in Transaction" *Networks* solution represents a comprehensive integration of fraud detection and cybersecurity, resulting in a unified defense ecosystem. The system surpasses conventional financial monitoring practices by combining transaction analysis, network traffic inspection, and URL structure evaluation within a single platform. Through role-based access, real-time monitoring, and machine learning classification, the solution enhances institutional resilience against bots, hackers, and nation-state actors. The Defense Console not only improves transparency and proactive threat response but also strengthens trust in financial systems.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 4, April 2026

|DOI: 10.15680/IJIRSET.2026.1504080|

IX. FUTURE ENHANCEMENT

1. **Integration of Deep Learning Models** – Implementing advanced neural networks (e.g., LSTM, CNN) to improve detection accuracy and adapt to evolving attack patterns.
2. **Mobile Application Development** – Developing a dedicated mobile app for security analysts to access alerts, dashboards, and reports on the go.
3. **Advanced Analytics Dashboard** – Introducing detailed analytics for administrators to track fraud trends, intrusion attempts, and system performance metrics.
4. **Automated Threat Intelligence Sharing** – Enabling secure exchange of detected threat signatures and behavioral patterns across institutions for collective defense.
5. **Visualization & Simulation Tools** – Adding modules for attack path visualization, anomaly heatmaps, and simulated response strategies.
6. **Cloud Scalability & Performance Optimization** – Enhancing cloud infrastructure to handle larger transaction volumes and high-speed network traffic without latency.
7. **Enhanced Security Features** – Strengthening authentication with multi-factor authentication (MFA), blockchain-based logging, and advanced encryption mechanisms.

REFERENCES

[1] A. Gupta, R. Mehta, and S. Rao (2024). AI-Driven Fraud Detection in Financial Transaction Systems.
[2] J. Li, K. Tan, and H. Wong (2023). Machine Learning Approaches for Network Intrusion Detection.
[3] P. Sharma and M. Patel (2025). Behavioral Analytics for Coordinated Bot Identification in Cybersecurity.
[4] S. Kumar, A. Reddy, and V. Singh (2024). Random Forest Classifier Applications in Financial Fraud Prevention.
[5] R. Johnson and L. Smith, "Unified Framework for Fraud Detection and Cybersecurity," International Journal of Computer Security and Applications, vol. 14, no. 2, pp. 112–125, 2022.
[6] T. Chen, Y. Zhao, and F. Liu (2025). Multi-Domain Data Fusion for Threat Attribution in Transaction Networks.
[7] M. Ahmed, J. Clark, and S. Khan (2023). Real-Time Monitoring and Alert Systems in Financial Security Platforms.
[8] P. D'Souza and R. Verma (2024). Explainable AI in Fraud Detection and Network Security.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details