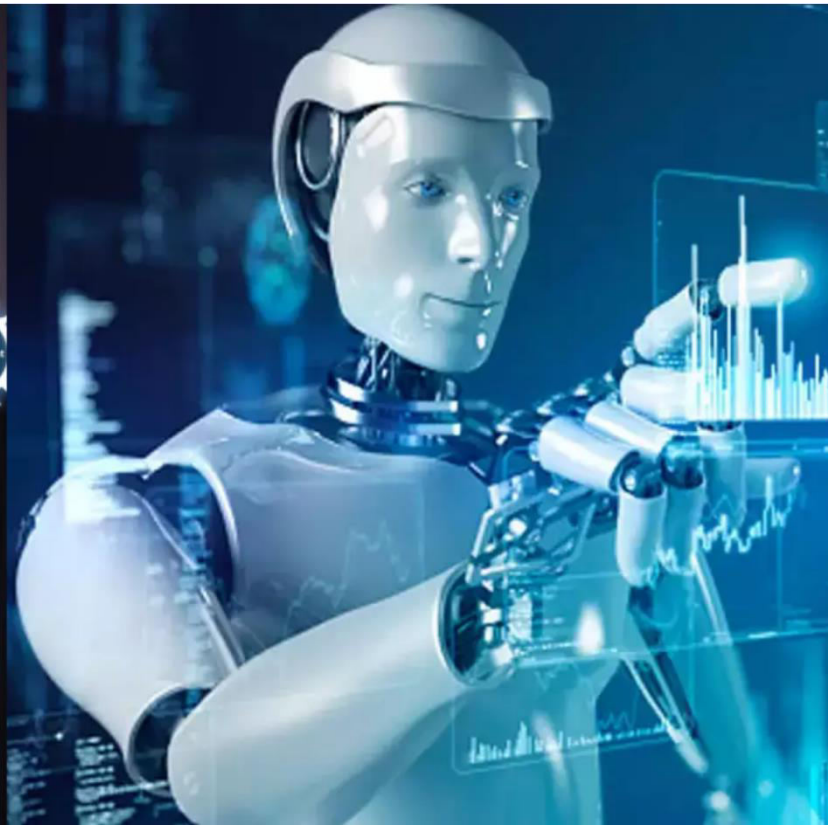
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

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 3, March 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 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503395|

Centralized Notification and Fraud Detection Dashboard

Sakshi Patil, Shreya Sakhare, Akash Salunkhe, Dr. Reeta Singh

U.G. Student, Department of Information Technology, K.C College of Engineering, Thane, Maharashtra, India

U.G. Student, Department of Information Technology, K.C College of Engineering, Thane, Maharashtra, India

U.G. Student, Department of Information Technology, K.C College of Engineering, Thane, Maharashtra, India

Associate Professor, Department of Information Technology, K.C College of Engineering, Thane, Maharashtra, India

ABSTRACT: As organizations increasingly adopt internal notification systems, attackers are shifting focus toward overlooked vectors like embedded URLs and QR codes to bypass traditional security filters. Unlike email-based threats, these internal alerts often bypass rigorous monitoring due to high employee trust. This paper proposes ARGUS, a centralized hybrid machine learning framework that analyzes notification content, hyperlinks, and QR code payloads in real time. By integrating text-based feature extraction and URL behavior analysis with a role-based alerting mechanism, the system ensures effective threat communication across the organization. Experimental evaluation on a simulated enterprise dataset demonstrates high detection accuracy and explainable results, confirming the system's readiness for real-world deployment.

KEYWORDS: Internal Notification Security, Phishing Detection, QR Code Analysis, Hybrid Machine Learning, Explainable AI (XAI), XGBoost, DistilBERT, FastAPI, Cybersecurity Dashboard.

I. INTRODUCTION

With the rapid growth of digital platforms, organizations today generate a huge amount of data through transactions, system logs, and internal communications. While this data helps improve efficiency and decision-making, it also opens the door to new types of security risks such as fraud, unauthorized access, and misuse of services. Most existing systems depend on separate tools or rule-based alerts to detect such issues. In many cases, these systems work independently, which makes it difficult to identify complex threats quickly. As a result, important warning signs may be missed or detected too late.

To address this problem, we developed a Centralized Notification and Fraud Detection Dashboard (ARGUS). The idea behind this system is simple: instead of handling alerts separately, everything is brought together into a single platform that continuously monitors activity and detects suspicious behavior in real time.

What makes this system different is its focus on internal notifications, which are often ignored in traditional security models. By combining real-time monitoring with machine learning and a centralized interface, ARGUS provides a more practical and efficient way to detect and respond to fraud within an organization.

II. LITERATURE SURVEY

Rapid development of e-commerce operations requires creating more advanced fraud prevention algorithms to overcome conventional security measures. This part provides a review of existing methods for fraud detection and notification systems as well as the gaps that need to be addressed by an intelligent, centralized and explainable algorithm.

2.1 Development of Alerting and Notification Paradigms

Current organizations employ automated notification systems to notify stakeholders about various processes via Email, SMS, Push Notifications and others. Although modern notification platforms ensure efficient delivery of relevant

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 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503395|

information, their scope is restricted to communication without involving intelligent decisions. Many studies proved that poor notification prioritization leads to alert fatigue experienced by administrators.

2.2 Comparative Evaluation of Detection Algorithms

The following table provides a comparative analysis of common detection methods in terms of advantages and drawbacks: Sr. No Method Type Main Characteristics Advantages Disadvantages

1 Rule-based systems Typical examples involve threshold rules and suspicious logins Quick detection and easy implementation Cannot identify emerging fraud techniques

2 Machine learning models Involves sophisticated mathematical calculations Ensures better accuracy and flexibility Lack of transparency; not incorporated in central interfaces

2.3 Latest Developments in Centralized Monitoring

- SIEM and multi-cloud systems: SIEM technology enables centralized monitoring and provides real-time alerting in various systems. At the same time, SIEM tools typically generate vast amounts of data that should be properly configured by experts.
- Streaming analytics: Technologies such as Kafka and Spark help perform real-time data processing and fraud detection. Nevertheless, these solutions are highly complicated for deployment.

2.4 Identified Research Gap

Despite providing useful visualizations and monitoring capabilities, most existing tools are not integrated with intelligent fraud detection algorithms. Such lack of coordination results in increased response time since many platforms should be used to prevent fraud. The proposed system (ARGUS) aims to address these gaps by integrating notification-based fraud detection, real-time alerting and central monitoring.

III. METHODOLOGY

The proposed ARGUS system serves as a centralized monitoring platform for the purposes of real-time alerting and fraud detection in the form of a dashboard. The dashboard becomes the central point from which all activities can be monitored.

A. System Architecture

The ARGUS solution employs a client-server architecture specifically optimized for quick threat detection and management:

- React-Based Web Dashboard: This web interface allows the users to monitor their notifications and discover potential fraudulent activities.
- Back-End Processing Server: It includes FastAPI-based back-end for processing data, performing machine learning tasks and authenticating users.
- Cloud-based Data Layer: This includes MongoDB as our choice for database storage of logs, notifications and other user-related information.

B. Alert Handling & Fraud Detection Flow

The flow of events in ARGUS includes several steps:

1. Event Generation: The event is triggered by applications or embedded content (URLs and QR codes).
2. Validation of Request: Back-End validates the request and keeps track of the event.
3. Hybrid Approach: A set of machine learning models analyzes the event based on patterns and behavior learned.
4. Classification of Threats: Based on the scores produced during analysis, the system classifies events as Safe, Suspicious or High-Risk events.
5. Verification by Humans: All suspicious events need to be manually verified by analysts through the use of dashboard.

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 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503395|

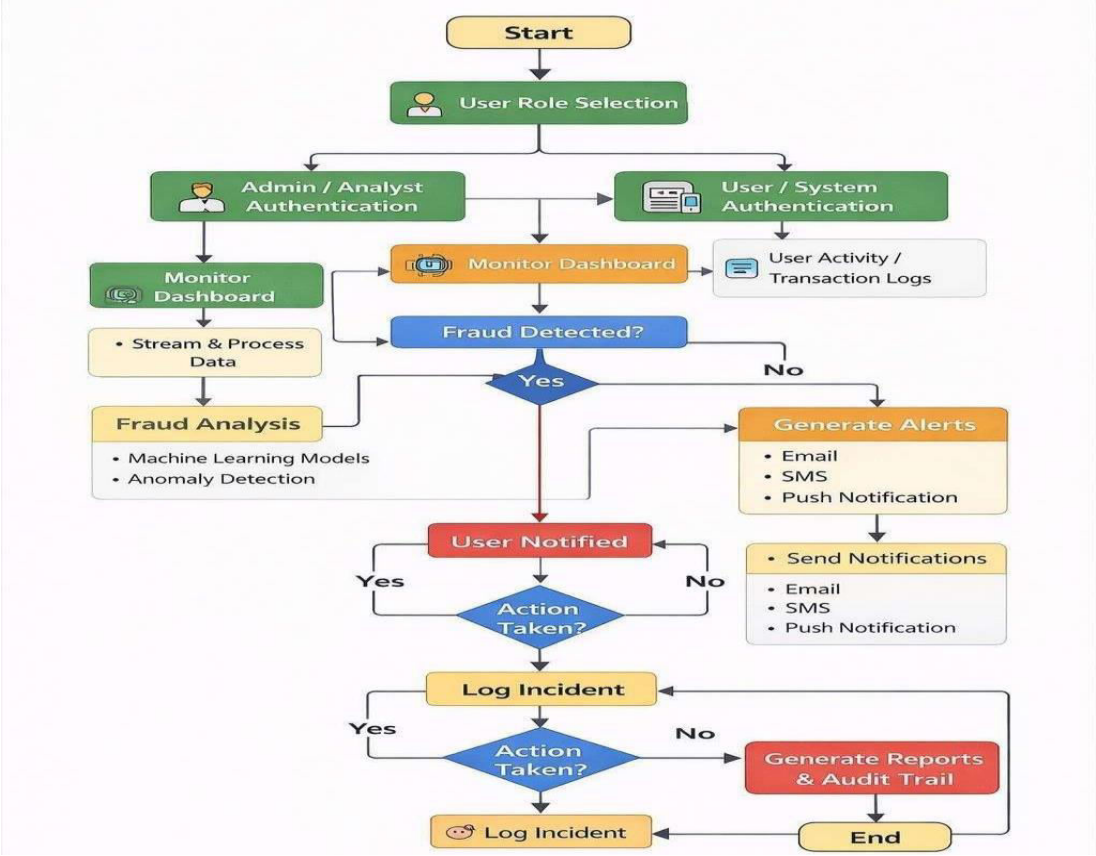


Fig 3.1 System Flowchart Diagram

The ARGUS system implements a multi-layered, role-based workflow to ensure a secure and transparent process for handling internal notifications and fraud detection.

A. Global System Workflow

The end-to-end processing of a notification follows a three-stage pipeline:

1. **Notification Generation**: Data originates from internal applications (Email, Slack), user transactions, or external integrations, potentially containing URLs, QR codes, or text-based payloads.
2. **Real-Time Processing**: The backend architecture extracts metadata and runs Machine Learning (ML) classifiers to assign a risk score, categorizing the event as Safe, Suspicious, or High-Risk.
3. **Dashboard Synchronization**: Classification results are pushed instantly to the relevant role-specific dashboards and queues for review or action.

B. Defined Organizational Roles

1. Administrator (Central Authority)

The Administrator maintains high-level oversight and system-wide control.

- Responsibilities: System health monitoring, role-based access management, and threat intelligence configuration.
- Workflow: Monitors aggregate metrics such as total alerts and model accuracy, manages user permissions, and executes system-wide responses like blocking malicious domains.

2. Fraud Analyst (Decision-Making Layer)

The Analyst acts as the primary validator, bridging the gap between automated AI decisions and human verification.

- Responsibilities: Investigating flagged high-risk notifications and validating the reasoning behind ML- generated alerts.
- Workflow: Reviews the "Review Queue" to analyze URL/QR scan results and AI-driven explanations (e.g., urgency patterns) before marking an incident as Safe, Malicious, or Escalated.

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 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503395|

3. Employee (First Line of Defense)

Employees are the primary users and potential targets of notification-based attacks.

- Responsibilities: Monitoring personal alerts and reporting suspicious activity.
- Workflow: Interacts with a "My Notifications" panel that displays risk levels and explanations; utilizes integrated tools like the URL and QR scanners to verify content before interaction.

4. Department Head (Operational Oversight)

Provides mid-level governance to ensure the safety of specific teams.

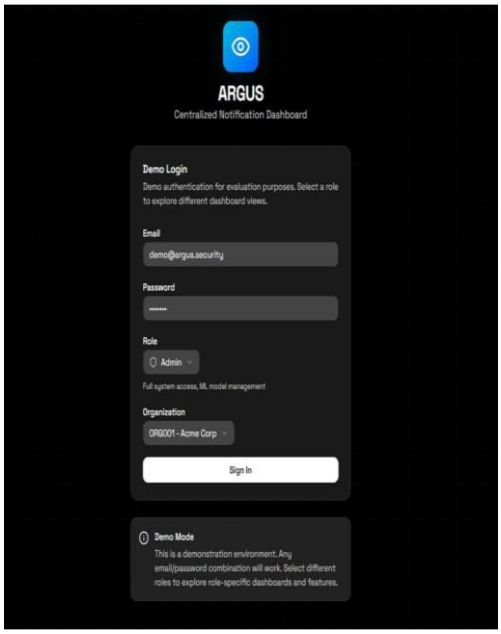
- Responsibilities: Monitoring department-specific risk trends and taking preventive measures.
- Workflow: Tracks notification volume and high-risk alerts within their department to identify emerging fraud patterns and alert relevant teams.

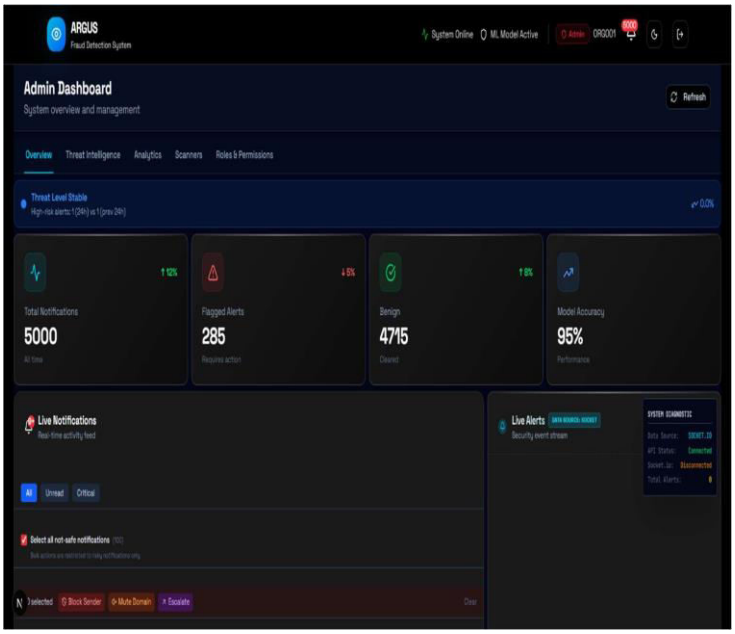
5. Auditor (Governance and Compliance)

The Auditor ensures the transparency and accountability of the entire security operation.

- Responsibilities: Compliance tracking and maintaining a transparent audit trail.
- Workflow: Accesses a read-only dashboard to review historical notification logs, analyst decisions, and system accountability metrics without the ability to modify data.

IV. EXPERIMENTAL RESULTS





The figures illustrate the ARGUS centralized notification and fraud detection dashboard system. The first screen shows a secure login interface where users select roles (e.g., Admin) and organization before accessing the system. The second screen presents the Admin Dashboard, displaying key metrics like total notifications, flagged alerts, benign events, and model accuracy. It also includes real-time alerts and notifications, enabling efficient monitoring and management of security events.

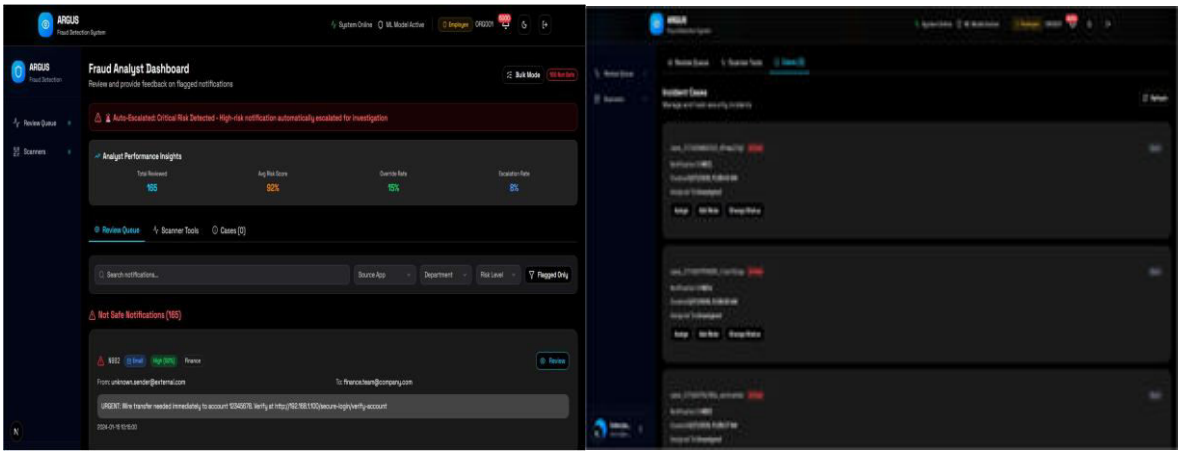
International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

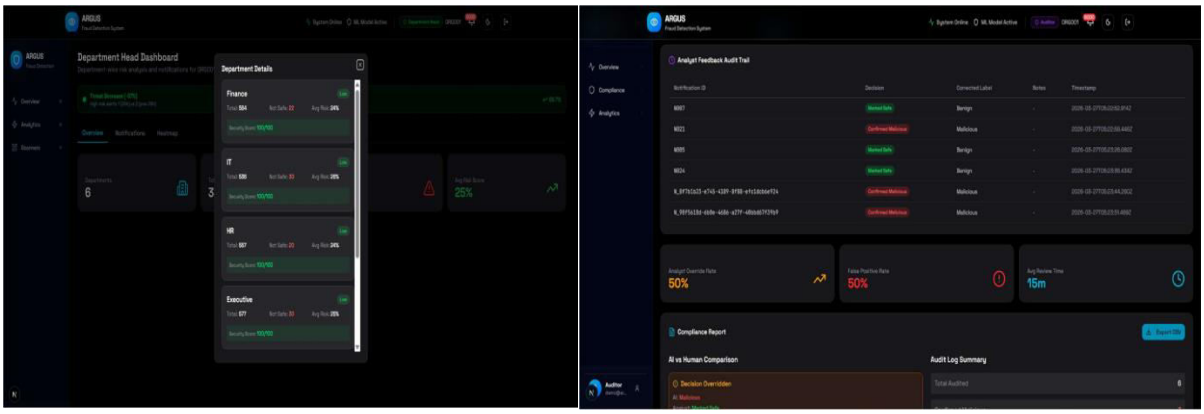
|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503395|



The figures represent the Fraud Analyst Dashboard of the ARGUS system, designed for reviewing and managing flagged notifications. It highlights auto-detected critical risks, performance insights (like accuracy and detection rate), and a queue of suspicious activities for investigation. The interface also provides tools for scanning and case management, enabling analysts to take actions such as reviewing, blocking, or escalating potential fraud cases efficiently.



The figures depict the Department Head Dashboard and Analytics Audit Panel of the ARGUS system. The first screen shows department-wise security insights, including risk levels and activity status, enabling department heads to monitor and manage alerts effectively. The second screen presents an audit trail with detection results, classification (benign/malicious), and performance metrics like detection rate and response time. Together, these interfaces support transparency, compliance tracking, and data-driven decision-making in fraud detection.

V. CONCLUSION

In this work, we designed and implemented a centralized dashboard that helps organizations monitor internal notifications and detect potential fraud in real time. By combining machine learning techniques with continuous data analysis and a unified interface, the system improves both detection capability and response time. From our implementation and testing, it is clear that the system can successfully identify suspicious activities and generate meaningful alerts. The ability to explain why a particular alert was triggered also makes it easier for analysts to take appropriate action. Overall, the proposed system is scalable and can be adapted to different organizational environments. In the future, the system can be further improved by integrating more advanced models, expanding data sources, and exploring technologies like deep learning and cloud-based deployment for better performance.

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 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503395|

REFERENCES

[1] T. Chen and C. Guestrin, "XGBoost: A Scalable Tree Boosting System," *Proceedings of the 22nd ACM SIGKDD International Conference*, 2024.
[2] S. M. Lundberg and S. I. Lee, "A Unified Approach to Interpreting Model Predictions (SHAP)," *Advances in Neural Information Processing Systems*, 2023.
[3] V. Sanh, et al., "DistilBERT, a distilled version of BERT: smaller, faster, cheaper and lighter," *arXiv preprint*, 2022.
[4] M. Stefen and L. Yang, "Explainable AI in Cybersecurity: A Survey of XAI Methods for Phishing Detection," *Journal of Cyber Security and Mobility*, 2024.
[5] R. Jain and A. Gupta, "Real-time Detection of Malicious QR Codes using Hybrid Deep Learning," *IEEE Access*, 2025.
[6] J. Ma, L. K. Saul, S. Savage, and G. M. Voelker, "Beyond blacklists: Learning to detect malicious web sites from suspicious URLs," *ACM SIGKDD*, 2009.
[7] K. Thomas et al., "Design and evaluation of a real-time URL spam filtering service," *IEEE Symposium on Security and Privacy*, 2011.
[8] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: A survey," *ACM Computing Surveys*, 2009.
[9] M. Ahmed, A. N. Mahmood, and J. Hu, "A survey of network anomaly detection techniques," *Journal of Network and Computer Applications*, 2016.
[10] Splunk Inc., "Security Information and Event Management (SIEM)," [Online]. Available: https://www.splunk.com.
[11] IBM Security, "IBM QRadar SIEM: Product Overview," [Online]. Available: https://www.ibm.com/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