ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue IV, April 2026

# Design and Development of a Public Cyber Alert and Reporting System for Cyber Crime Incidents in India

**Kolusu Hemachandra Mouli[1], P. Indraja[2], Dr Arjunarao Rajanala[2]**

**[1]PG Student in Dept of CSE, Sree Vahini Institute of Science and Technology, AP, India**

**[2]Assistant Professor in Dept of CSE, Sree Vahini Institute of Science and Technology, India**

**DOI: https://doi.org/10.51583/IJLTEMAS.2026.150400053**

**Received: 11 April 2026; Accepted: 16 April 2026; Published: 07 May 2026**

## ABSTRACT

Cyber crime incidents in India have escalated in frequency and complexity, impacting individuals, organizations, and critical infrastructure. Despite existing law enforcement mechanisms and reporting platforms, gaps remain in public awareness, real-time alerts, and consolidated reporting.

This research proposes the design and development of a Public Cyber Alert and Reporting System (PCARS) tailored for India's cyber security landscape. The system integrates real-time threat alerts, user-centric reporting interfaces, automated categorization using machine learning, and seamless communication with law enforcement agencies. Evaluation shows increased reporting efficiency, improved user engagement, and enhanced situational awareness at national and grassroots levels.

**Keywords:** Automated Threat Classification, Cyber Crime, Cyber Crime Reporting, Cyber Security, Digital Forensics, India, Law Enforcement Integration, Machine Learning, Public Awareness, Real-Time Threat Alerts, Situational Awareness

## INTRODUCTION

With rapid digitalization in India, cyber crimes such as phishing, identity theft, ransomware, and financial fraud have grown exponentially. Existing reporting platforms are centralized and lack proactive alert dissemination. The public often remains unaware of emerging cyber threats, leading to repeated victimization and under-reporting. The objective of this research is to design and develop a user-friendly cyber crime reporting interface, enable real-time threat alerts, integrate machine learning-based automated classification, facilitate coordination with law enforcement, and evaluate system effectiveness.

## LITERATURE REVIEW

India has witnessed a sharp rise in cyber crime cases, financial frauds, and digital exploitation. Complaints via national portals have increased significantly. Global frameworks such as centralized reporting systems demonstrate the importance of multichannel reporting, automated analytics, dashboards, and law enforcement integration. However, gaps persist including technical complexity, delayed alerts, lack of regional customization, and minimal victim feedback.

### System Design

The proposed PCARS consists of frontend web and mobile interfaces, backend API servers with centralized database, analytics engine using machine learning, real-time alert engine, and secure law enforcement integration module. The system ensures modularity, scalability, interoperability, and secure data handling.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue IV, April 2026

### Implementation

The technology stack includes React.js/Flutter frontend, Node.js/Python backend, PostgreSQL database, and machine learning models such as Naïve Bayes, Random Forest, SVM, and LSTM. Security measures include SSL encryption, token-based authentication, data anonymization, and consent-based data collection.

### Machine Learning Classification

Supervised learning models were trained on labeled cyber incident datasets. Random Forest achieved 87% accuracy, SVM 83%, and LSTM 91% accuracy, demonstrating superior contextual understanding for textual incident reports.

| Model | Data Type | Accuracy (%) |
|---|---|---|
| Random Forest | Structured features | 87 |
| SVM | Structured features | 83 |
| LSTM | Textual incident reports | 91 |

### Evaluation

User testing with 200 participants from urban and rural regions showed 4.5/5 ease of use, 2.3 minutes average reporting time, and 4.3/5 satisfaction with alerts. The results indicate improved usability, faster reporting, and enhanced engagement.

| Evaluation Metric | Value | Description |
|---|---|---|
| Number of Participants | 200 | Users from both urban and rural regions |
| Ease of Use Rating | 4.5 / 5 | High usability across diverse user groups |
| Average Reporting Time | 2.3 minutes | Faster incident submission compared to traditional methods |
| Alert Satisfaction Rating | 4.3 / 5 | Positive user perception of alert effectiveness |

## DISCUSSION

The system increases reporting participation, enables faster detection of attack trends, and delivers customized alerts. Challenges include ensuring data privacy, integrating with diverse law enforcement IT systems, and managing false positives.

The proposed system significantly increases cyber incident reporting participation by simplifying the reporting process and improving user accessibility across urban and rural populations. Faster data aggregation and analysis enable earlier detection of emerging attack trends, allowing stakeholders to respond proactively. Additionally, the delivery of customized alerts enhances user awareness and engagement by providing timely, context-relevant notifications.Despite these advantages, several challenges remain. Ensuring data privacy is critical, particularly given the sensitive nature of cyber incident information. Integration with heterogeneous law enforcement information systems presents technical and organizational difficulties, requiring standardized interfaces and interoperability frameworks. Furthermore, managing false positives generated by automated classification models is essential to prevent alert fatigue and maintain user trust.
Overall, addressing these challenges will be key to achieving scalable, secure, and reliable deployment of the system in real-world environments.

## CONCLUSION

The proposed Public Cyber Alert and Reporting System significantly enhances cyber incident reporting efficiency, improves public awareness, and enables more coordinated response mechanisms across India. Its modular and citizen-centric design supports scalability, inclusivity, and adaptability to evolving cyber threats. By strengthening collaboration between citizens and authorities, the system contributes meaningfully to national cyber resilience and proactive cyber defense capabilities.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue IV, April 2026

**Future Work**

Future enhancements to the system will focus on incorporating advanced natural language understanding techniques to improve the accuracy and depth of cyber incident analysis. Integration with financial institutions is envisioned to enable rapid fraud detection and mitigation, thereby reducing response time and financial losses. Additionally, expanding regional language support will promote inclusive access, ensuring broader participation and usability across diverse linguistic communities.

## REFERENCES

1. Indian Computer Emergency Response Team (CERT-In), Cyber Security Reports and Advisories.
2. National Crime Records Bureau (NCRB), Crime in India Report.
3. National Cyber Crime Reporting Portal, Government of India.
4. Internet Crime Complaint Center (IC3), 2023 Internet Crime Report.
5. Action Fraud, UK National Reporting Centre for Fraud and Cyber Crime.
6. S. Gupta, P. Verma, Machine Learning Techniques for Cyber Crime Classification, 2021.
7. M. Singh, N. Patel, Design of Secure Web-Based Cyber Crime Reporting Platforms, 2020.
8. I. Goodfellow, Y. Bengio, A. Courville, Deep Learning, MIT Press, 2016.