REVA UNIVERSITY

SCHOOL OF COMPUTING AND INFORMATION TECHNOLOGY

Bachelor of Technology
in
CSIT

Major Project Phase-I Synopsis

Real-Time Cyber Threat Intelligence and Incident Monitoring System for India

By

SL. No.	Student Name	Department	SRN
1	Rabi Rahul	BTech CSIT	R22EJ117
2	T Mukesh	BTech CSIT	R22EJ143
3	Nezil Nasar	BTech CSIT	R22EJ170

Under the supervision of
Prof. Vijayalaxmi C Handaragall

School of Computing and Information Technology

Rukmini Knowledge Park, Kattigenahalli, Yelahanka, Bengaluru-560064
www.reva.edu.in

November 2025

1: Introduction (Background):

India's rapid digital transformation has also made it one of the fastest growing targets for cyberattacks. Sectors such as banking, healthcare, education, critical infrastructure, e-commerce, transportation, and government services are increasingly exposed to cyber threats. Attackers often exploit newly discovered vulnerabilities in operating systems, network devices, and web applications before organizations apply necessary security patches.

Additionally, phishing scams, fraudulent URLs, UPI payment frauds, and data breaches are increasingly affecting citizens and organizations. In many cases, actionable threat information reaches users too late, leading to financial losses, operational disruption, and data compromise.

Therefore, there is a strong need for a real-time, India-focused cyber threat intelligence system that provides early warnings, enhances cybersecurity awareness, and enables proactive defense across Indian cyberspace.

2: Problem Statement:

Although India has national cybersecurity agencies such as CERT-In, NCIIPC, I4C, and Cyber Swachhta Kendra for threat monitoring and response, there is no publicly accessible unified platform that delivers real-time cyber threat feeds combining critical information such as:

- Newly published software/hardware vulnerabilities,
- Active Phishing or scam links,
- Ongoing cyberattacks,
- India-specific cybercrime incidents, and
- Public reporting of suspicious activities.

This gap results in delayed response and reduces cyber readiness for users who are not directly connected to government agencies or dedicated cybersecurity centers.

2.1 Significance of the Problem

- Enables faster response to cyber incidents.
- Helps prevent large-scale data breaches, operational disruption, and fraud.
- Improves cyber awareness among citizens and small organizations that lack dedicated cybersecurity teams.
- Enhances national security by enabling early detection of threats to critical infrastructure.

2.2 Who is Affected?

- Citizens: victims of scams, phishing, fraud, identity theft.
- Organizations: particularly those without internal SOC teams.
- Critical Infrastructure Operators: hospitals, banks, telecom, energy, transport, etc.
- Law Enforcement and Cyber Cells: who rely on public reporting and data aggregation.

3: Scope and Objectives:

3.1 Scope of the Project

This project focuses on developing a real-time cyber threat intelligence platform tailored for India. It provides early warning information about vulnerabilities, malicious URLs, fraud activities, and cybercrime incidents from multiple sources and allows public participation in threat reporting.

3.2 Primary Objective

To design and implement a real-time cyber threat awareness system that delivers actionable incident information specific to Indian cyberspace.

3.3 Secondary Objectives

- To scrape and aggregate vulnerability advisories directly from OEM websites (e.g., Cisco, Microsoft, Fortinet).
- To detect malicious or phishing URLs using an integrated link-scanning tool.
- To collect and classify India-focused cybercrime news and alerts.
- To provide a public reporting module for suspicious links, fraud attempts, or cyber incidents.
- To visualize threat trends and attack analytics relevant to Indian users.

3.4 Social / National Impact

- Enhances cybersecurity awareness among citizens.
- Reduces the chances of fraud, ransomware, and data theft.
- Supports cyber hygiene and preparedness in small and medium-scale organizations.
- Strengthens national security by improving early detection of cyber threats.

4: Target User:

4.1 Citizens

- Individuals can check suspicious links, avoid online scams, and report fraud attempts such as phishing, UPI scams, fake job links, and malicious websites.
- The platform promotes cyber awareness and safer digital practices for everyday users.

4.2 Small and Medium Enterprises (SMEs)

- SMEs without dedicated cybersecurity teams can receive timely vulnerability alerts and threat feeds.
- This allows them to apply essential security patches early and avoid costly data breaches or ransomware attacks.

4.3 Critical Infrastructure Organizations

- Sectors such as banking, healthcare, telecom, power, and transportation can monitor high-severity vulnerabilities relevant to their systems.
- Early alerts allow faster mitigation, reducing operational disruption and risk to public services.

4.4 Cyber Cells and Law Enforcement Agencies

- Cybercrime investigation agencies can use crowd-reported data to track new scams, malicious trends, and targeted attacks.
- Data analytics from the platform can support case tracing, public awareness drives, and faster response.

4.5 Students, Cybersecurity Researchers, and Academic Institutions

- The platform provides valuable datasets on cyber incidents, scam patterns, and vulnerability trends.
- It supports academic research, education, skill-building, and development of innovative security solutions.

5: References

- CERT-In (2024). *Computer Emergency Response Team India – Advisories & Alerts.* Ministry of Electronics and Information Technology, Government of India. Retrieved from https://www.cert-in.org.in

- NCIIPC (2024). *National Critical Information Infrastructure Protection Centre – Threat Reports & Guidance.* Government of India. Retrieved from https://www.nciipc.gov.in
- Indian Cybercrime Coordination Centre (I4C). (2024). *National Cybercrime Reporting Portal.* Ministry of Home Affairs, Government of India. Retrieved from https://cybercrime.gov.in
- Cyber Swachhta Kendra. (2024). *Botnet Cleaning and Malware Analysis Centre.* Retrieved from https://www.cyberswachhtakendra.gov.in
- National Vulnerability Database (NVD). (2024). *Common Vulnerabilities and Exposures (CVE) Reports.* Retrieved from https://nvd.nist.gov
- MITRE Corporation. (2024). *MITRE ATT&CK Framework.* Retrieved from https://attack.mitre.org
- Cyble Research. (2024). *India Threat Landscape Report 2024.* Retrieved from https://cyble.com/resources/research-reports/india-threat-landscape-report-2024
- Press Information Bureau (PIB). (2024). *Government Releases Cybersecurity Guidelines and Alerts.* Government of India. Retrieved from https://pib.gov.in