2026 Volume: 02 Issue: 08 www.ijrpa.com ISSN 2456-9995 Review Article

International Journal Research Publication Analysis

Page: 01-11

DESIGN AND DEVELOPMENT OF AN AI-BASED CYBER DEVICE REGISTRATION AND EARLY WARNING SYSTEM FOR PROACTIVE CYBER THREAT DETECTION

***Dr. Arjunarao Rajanala**

Principal, Nrupatunga Institute of Technology and Management, Hyderabad, India.

Article Received: 10 July 2026
Article Revised: 30 July 2026
Published on: 19 August 2026

***Corresponding Author: Dr. Arjunarao Rajanala**
Principal, Nrupatunga Institute of Technology and Management, Hyderabad, India.

DOI: https://doi-doi.org/101555/ijrpa.8588

ABSTRACT

The rapid growth of smartphones, laptops, tablets, and IoT devices has significantly increased the attack surface for cybercriminals. Existing cybersecurity solutions primarily focus on antivirus software and enterprise-level Security Operations Centers (SOCs), leaving many individual users without proactive protection. This paper proposes an AI-Based Cyber Device Registration and Early Warning System (CDREWS) that enables citizens to voluntarily register their devices through a secure web portal. The system continuously evaluates cybersecurity risks using artificial intelligence and generates real-time alerts regarding phishing attacks, malware, unauthorized logins, suspicious network activity, SIM swap risks, and data breaches. The proposed architecture integrates device fingerprinting, behavioral analytics, machine learning, and threat intelligence feeds to provide an intelligent cyber warning service. The framework aims to enhance cyber resilience while preserving user privacy through encryption, consent-based monitoring, and secure data management.

KEYWORDS: Cyber Security, Artificial Intelligence, Threat Intelligence, Device Registration, Phishing Detection, Malware Detection, Machine Learning, Early Warning System, Cyber Awareness.

1. INTRODUCTION

Digital transformation has made smartphones and connected devices essential for communication, banking, healthcare, education, and governance. However, cyber threats such as phishing, ransomware, malware, credential theft, SIM swap attacks, and identity theft are increasing rapidly [7].

Current cybersecurity solutions mainly protect organizations rather than individual citizens. Most users receive warnings only after becoming victims. Therefore, there is a need for a proactive cybersecurity platform capable of identifying threats before significant damage occurs [1], [7].

This research proposes an AI-powered national cyber device registration framework capable of continuously assessing cyber risk and notifying users immediately when suspicious activities are detected.

2. Problem Statement

The rapid growth of Internet-connected devices, IoT systems, mobile devices, cloud services, and smart computing environments has significantly increased the cyber-attack surface. Organizations and individuals continuously connect new devices to networks, but many devices remain improperly registered, inadequately monitored, outdated, or vulnerable to known and emerging cyber threats. Traditional device registration and cybersecurity monitoring mechanisms are often fragmented, reactive, and dependent on manual processes, making it difficult to identify unauthorized or compromised devices at an early stage.

Existing cybersecurity systems generally focus on detecting attacks after suspicious activities have already occurred. They may not provide an integrated mechanism for device registration[3], continuous security assessment, vulnerability identification, behavioral monitoring, and early warning within a single framework. Consequently, unauthorized devices, abnormal network behavior, vulnerable configurations, malware infections, and potential cyber incidents may remain undetected until they cause significant damage.

Another major challenge is the increasing volume and complexity of cybersecurity data generated by network devices, applications, logs, and security tools. Conventional rule-based detection techniques may have limitations in identifying previously unknown attack patterns, zero-day-like behaviors, and evolving cyber threats. There is therefore a need for an intelligent system capable of analyzing heterogeneous cybersecurity data and identifying potential threats proactively.

The proposed research, “Design and Development of an AI-Based Cyber Device Registration and Early Warning System for Proactive Cyber Threat Detection,” aims to address these limitations by developing an AI-enabled framework that securely registers and maintains device identities, continuously monitors device and network behavior, analyzes security-

related data, detects anomalies and potential threats, assesses risk levels, and generates timely early warnings.

3. Objectives

The proposed research aims to develop an AI-based Cyber Device Registration and Early Warning System that can proactively identify cyber threats and provide timely warnings. The objectives are explained below:

Develop a Secure Cyber Device Registration Portal: To design and develop a secure web-based portal through which individuals, organizations, and institutions can register their computers, mobile phones, IoT devices, and other cyber-enabled devices. The portal will maintain essential device information and provide controlled access to authorized users.

Generate Unique Digital Identities for Registered Devices:To assign a unique digital identity to every registered device. This identity will help the system distinguish between authorized and unauthorized devices and support device tracking, authentication, security monitoring, and incident investigation.

Monitor Cyber Threats Using AI Algorithms: To integrate Artificial Intelligence and Machine Learning techniques for continuously analyzing device activity, network traffic, logs, and security-related events. AI models will be used to identify patterns associated with potential cyber threats and improve detection accuracy.

Detect Phishing, Malware, Suspicious Logins, and Unusual Device Behavior:To develop intelligent detection mechanisms capable of identifying common and emerging cyber threats, including phishing attempts, malware activities, repeated or suspicious login attempts, unauthorized access, abnormal network behavior, and unusual changes in device activity.

Provide Instant Security Alerts and Early Warnings: To develop a multi-channel notification mechanism that can immediately inform users or authorized security personnel when a potential threat is detected. Alerts may be delivered through SMS, Email, WhatsApp, and mobile applications, depending on the severity and nature of the detected threat.

Improve Cybersecurity Awareness Among Citizens:To improve public awareness about cyber threats by providing users with understandable security alerts, preventive recommendations, awareness messages, and guidance on safe digital practices. The system will help users recognize potential threats and take appropriate action before significant damage occurs.

4. Architecture Overview

The proposed system consists of the following major layers:

1. User & Device Registration Layer: Users access a secure web/mobile portal to register their cyber devices. Information such as device type, operating system, device identifier, owner/organization details, and security configuration can be recorded.

2. Digital Device Identity Layer: After successful registration, the system generates a unique digital identity for each device. This identity can be used for authentication, device tracking, monitoring, and security-event correlation [3[.

3. Data Collection & Monitoring Layer: The system continuously collects relevant security information from registered devices and network environments, such as:

4.1. Login and Authentication Events

These records show who is trying to access a device, account, or system and whether the access is successful.

Examples:The AI-based cybersecurity system continuously monitors successful login attempts, failed login attempts, multiple password failures, logins from new devices, unusual locations or times, password changes, and multi-factor authentication (MFA) failures to identify abnormal user behavior. For example, if a user normally logs in from Hyderabad during daytime hours but suddenly generates 20 failed login attempts followed by a successful login at 3:00 AM from an unfamiliar location, the AI system can recognize this unusual pattern as suspicious behavior. It can then assign a higher risk score and generate an early warning or security alert for further investigation.4.2. Network Activity[6]: Network activity represents the communication between a device and other systems over a network or the Internet [3].

The system can examine: The AI-based cybersecurity system monitors IP addresses, ports, protocols, incoming and outgoing connections, data transfer patterns, connection frequency, and unusual destinations to identify abnormal network behavior. For example, if a computer normally communicates with a few trusted servers but suddenly starts making hundreds of connections to unknown external IP addresses, the AI system may detect this as an unusual network pattern. It can analyze the behavior, assign a risk score, and generate an anomaly warning or security alert for further investigation.

Device Behavior: Device behavior refers to how a registered device normally operates and whether its activities suddenly change from the established pattern. The AI-based cybersecurity system can monitor CPU and memory usage, running processes, newly

installed applications, file changes, USB or external device connections, network connections, and system configuration changes. For example, a student's laptop may normally run web browsers and educational applications, but if an unknown process suddenly starts running continuously and creates numerous network connections, the AI system can identify this activity as abnormal device behavior, assign an appropriate risk score, and generate a security alert for further investigation.

System Logs: System logs are records automatically generated by the operating system and system services that provide important information about system activities and security events. The AI-based cybersecurity system can analyze login and logout records, system errors, service activity, security events, file access, configuration changes, software installations, and system startup or shutdown activities. For example, repeated attempts to access a protected system file may be recorded in the system logs[4]. The AI system can correlate these events with other indicators, identify unusual patterns, and determine whether the activity may represent potentially malicious behavior, enabling timely alerts and further investigation.

Application Activity: Application activity describes the actions and behavior of software applications running on a device. The AI-based cybersecurity system can monitor application execution, login attempts, file access, API activity, unusual application behavior, browser activity, and application errors to identify potential security threats. For example, if an application that normally does not access network resources suddenly begins sending large amounts of data to an unknown external server, the AI system can identify this as suspicious or potentially compromised application behavior. By correlating this activity with other security indicators, the system can assess the risk and generate an appropriate security alert.

Application Activity: Application activity refers to the actions and behavior of applications running on a device. The AI-based cybersecurity system monitors application execution, application login attempts, file access, API activity, browser activity, application errors, and other unusual application behavior to detect potential security threats. For example, if an application that normally does not access network resources suddenly starts sending a large amount of data to an unknown external server, the AI system can identify this as suspicious or potentially compromised application behavior. By analyzing such activities and comparing them with normal behavior, the system can detect anomalies, assign a risk score, and generate an appropriate security alert.

Security Events: Security events are activities that have direct relevance to the security of an organization's systems, devices, and networks. The AI-based cybersecurity system can

monitor antivirus detections, firewall blocks, unauthorized access attempts, account lockouts, privilege escalation events, intrusion detection alerts, and suspicious file activities. For example, if a firewall repeatedly blocks connections from a suspicious external IP address while the same device is experiencing unusual login attempts, the AI system can correlate these events and identify a potential coordinated attack. Based on the combined indicators, the system can assign a higher risk score and generate an early security alert for further investigation and response.

Suspicious URLs or Domains: The AI-based cybersecurity system can analyze URLs and domain names to determine whether they may be associated with phishing, malware, fraud, or other malicious activities. It examines characteristics such as newly registered domains, known malicious domains, suspicious URL structures, domain reputation, HTTPS and certificate information, redirect behavior, and threat-intelligence indicators. For example, if a user receives an email containing a suspicious URL such as example-login-security [.]Com, the system can compare its domain characteristics and URL patterns with known phishing indicators and threat-intelligence data. If the URL is identified as potentially malicious, the system can generate a phishing warning and alert the user before the link is accessed.

Malware-Related Indicators: Malware-related indicators are pieces of information that may suggest that a device has been infected with malware or is communicating with malicious infrastructure. The AI-based cybersecurity system can monitor suspicious executable files, known malware hashes, unexpected processes, malicious IP addresses, command-and-control connections, unusual file modifications, suspicious persistence mechanisms, and antivirus/EDR detections. For example, if a registered device suddenly communicates with an IP address associated with known malicious activity while simultaneously launching an unusual process, the AI system can correlate these indicators with other security events and classify the device as potentially compromised. This helps the system generate an appropriate risk score and early warning for further investigation and response.

Threat Intelligence & Rule Engine: The AI engine can be supplemented with threat-intelligence feeds, known indicators of compromise, signatures, security rules, and vulnerability information. Combining AI-based detection with established security rules can improve detection coverage.

The Risk Assessment Layer evaluates each detected security event to determine its potential impact and likelihood of representing a genuine threat. The AI-based cybersecurity system considers factors such as threat type, severity, probability, device importance, frequency of suspicious activity, and historical behavior. By combining these factors, the system calculates

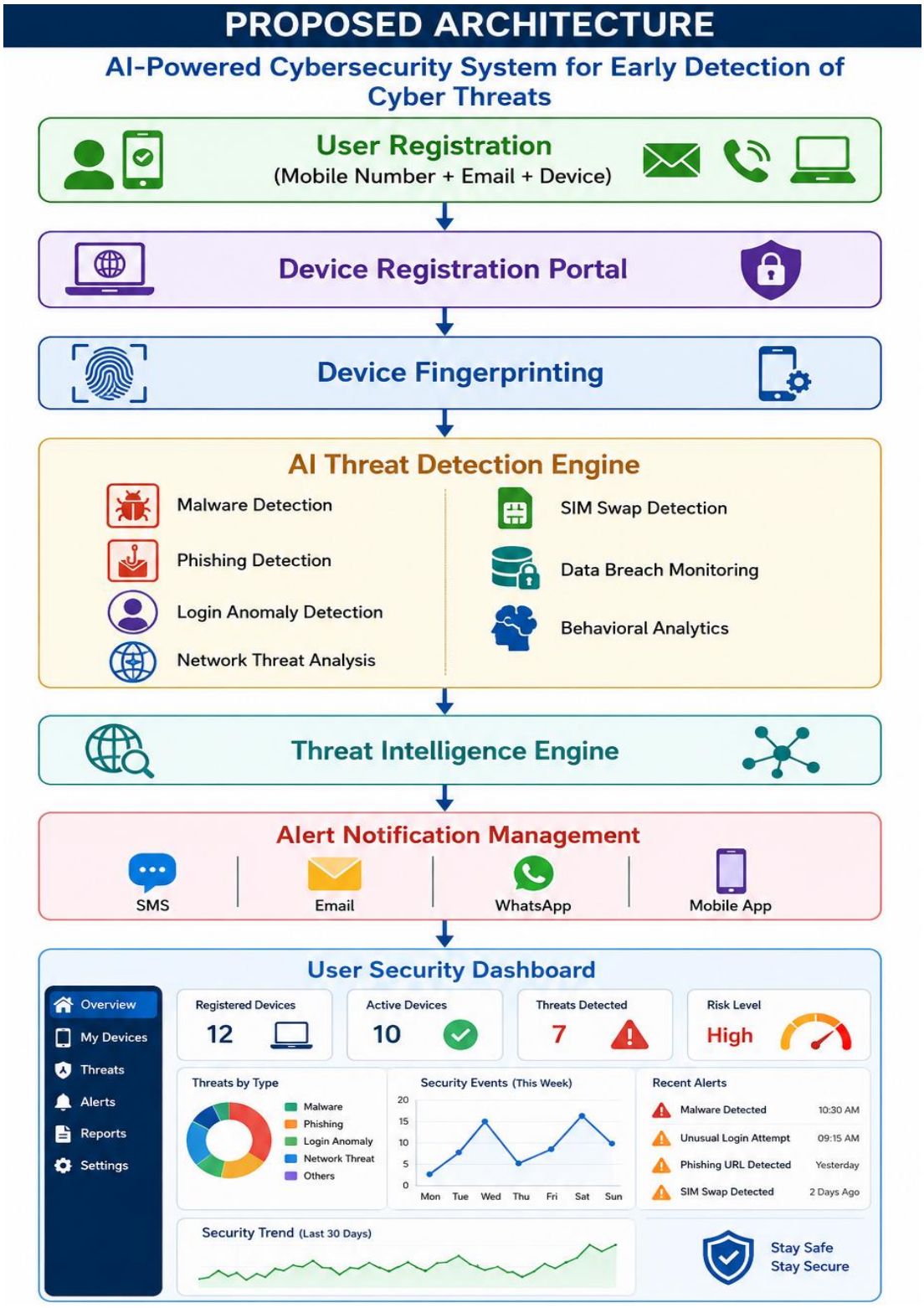
an appropriate risk score and classifies the event into different risk levels, such as Low, Medium, High, or Critical. This risk-based approach helps security teams prioritize serious threats, reduce false alarms, and take appropriate preventive or corrective actions in a timely manner.

Early Warning & Alert Layer: When the system identifies a significant threat, it generates an early warning. Depending on the risk level, notifications can be delivered through:

Security Dashboard & Management Layer: The Security Dashboard and Management Layer provides authorized administrators with a centralized platform to monitor and manage the overall security status of devices and users. The dashboard displays important information such as registered devices, device status, security events, detected threats, risk levels, alert history, device activity, incident reports, and security trends. By presenting this information in a clear and organized manner, the system enables administrators to quickly identify potential threats, track suspicious activities, review security incidents, and monitor changes in security conditions. This centralized approach supports effective decision-making, timely threat response, and continuous security monitoring.

Secure Database & Audit Layer:The Secure Database and Audit Layer provides secure storage and management of device registrations, digital identities, security events, alerts, risk scores, and audit records. The system applies strong security mechanisms such as access controls, data encryption, user authentication, authorization, and audit logging to protect sensitive information from unauthorized access or modification. All important activities can be recorded in audit logs, enabling administrators to track user actions, security events, and system changes. This layer ensures data confidentiality, integrity, accountability, and secure access while supporting reliable security monitoring and forensic investigation.

5. Proposed Architecture



6. How AI Uses All These Data Together

The important point for your research is that **the AI system should not necessarily depend on one indicator alone**. It can combine multiple signals to improve detection.

For example:

Failed logins

↓

Unusual login location

↓

Abnormal network connection

↓

Unknown process starts

↓

Suspicious domain contacted

↓

AI Risk Analysis

7. Proposed architecture

These eight data categories can be grouped into a **Cybersecurity Data Collection Layer**:

Devices → Data Collection → Data Preprocessing → Feature Extraction → AI/ML Detection → Risk Scoring → Early Warning → Alert/Response

AI-Based Cybersecurity System – Each Stage in 3 Lines

1. Devices: Devices such as computers, laptops, mobiles, servers, and IoT devices are registered in the system.Each device receives a unique digital identity.The system continuously monitors the security status of registered devices.

2. Data Collection: The system collects login, network, system, application, and security-related information. It also collects suspicious URLs, malware indicators, and device activity. This data provides the foundation for cybersecurity analysis.

3. Data Preprocessing: Collected data is cleaned, organized, and converted into a standard format.Duplicate, incomplete, and irrelevant information is removed.The prepared data is then provided to the AI/ML model.

4. Feature Extraction: Important security characteristics are extracted from the processed data.Examples include failed logins, unusual IP addresses, network traffic, and abnormal behavior.These features are used as inputs for AI-based threat detection.

5. AI/ML Detection:AI/ML algorithms analyze the extracted features to identify suspicious patterns.The system can detect phishing, malware, unauthorized access, and abnormal behavior.It classifies activities as normal, suspicious, or potentially malicious.

6. Risk Scoring: The detected threat is evaluated based on severity, probability, and device importance.The system assigns a numerical risk score and security level.Threats can be categorized as Low, Medium, High, or Critical.

7. Early Warning: When a threat crosses a predefined risk threshold, the system generates an early warning.The warning provides information about the affected device and detected threat.This enables users or administrators to take action before major damage occurs[1][5].

8. Alert / Response: Security alerts can be delivered through SMS, Email, WhatsApp, mobile apps, or dashboards.The system can recommend actions such as verification, password change, or device isolation.This enables a faster and more effective cybersecurity response.

8. CONCLUSION

The proposed **AI-Based Cyber Device Registration and Early Warning System** offers a proactive cybersecurity framework that enables citizens to receive timely alerts about cyber threats affecting their registered devices. By combining AI, machine learning, behavioral analytics, and threat intelligence[6][7], the framework enhances cyber resilience while emphasizing user consent, privacy, and secure data handling. The architecture has potential applications in smart cities, educational institutions, enterprises, and government cyber awareness initiatives.

REFERENCES

1. Pascoe, C., Quinn, S., & Scarfone, K. (2024). The NIST Cybersecurity Framework (CSF) 2.0. NIST Cybersecurity White Paper, NIST CSWP 29. National Institute of Standards and Technology.
2. Tabassi, E. (2023). Artificial Intelligence Risk Management Framework (AI RMF 1.0). NIST AI 100-1. National Institute of Standards and Technology.
3. Temoshok, D., Choong, Y.-Y., Galluzzo, R., LaSalle, M., Regenscheid, A., Proud-Madruga, D., Gupta, S., & Lefkovitz, N. (2025). NIST SP 800-63-4: Digital Identity Guidelines. National Institute of Standards and Technology.
4. Kent, K., & Souppaya, M. (2006). Guide to Computer Security Log Management. NIST Special Publication 800-92. National Institute of Standards and Technology.
5. Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). Computer Security Incident Handling Guide. NIST Special Publication 800-61 Rev. 2. National Institute of Standards and Technology.

6. MITRE. (n.d.). MITRE ATT&CK®: Knowledge Base of Adversary Tactics and Techniques. MITRE Corporation.
7. European Union Agency for Cybersecurity (ENISA). (2025). ENISA Threat Landscape 2025. ENISA.
8. Anderson, H. S., & Roth, P. (2018). EMBER: An Open Dataset for Training Static PE Malware Machine Learning Models. arXiv:1804.04637.