International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 03 March 2026
Page No: 1332-1337
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0184

Port Guard AI-Smart Vulnerability & Threat Scanner Using Artificial Intelligence

Mohitha Elluri[1], Mohammad Imran Subhani[2], Tejaswi Ramineni[3], Harikrishna VenkataVamsi[4], P.Jyothsna Kumari[5]
[1,2,3,4] Students, Department of Computer Science and Engineering, SRK Institute of Technology, Vijayawada, India.
[5]Assisstant Professor, Department of Computer Science and Engineering, SRK Institute of Technology, Vijayawada, India.
***Email ID:** mohithaelluri@gmail.com[1]*

Abstract
In modern digital infrastructures, enterprises and cloud-based networks significantly depend on secure communication channels. However, misconfigured ports, exposed services, and unpatched vulnerabilities continue to serve as primary attack vectors for adversaries. Traditional vulnerability scanners such as Nmap, Nessus, and OpenVAS provide efficient port-level detection but struggle with false positives, manual analysis overhead, and limited intelligence for predicting unknown threats. This paper introduces Port Guard AI, a smart vulnerability and threat scanning system that integrates automated port scanning, AI-driven threat classification, and risk prioritization. The system detects open ports within specified ranges, evaluates associated risk levels, and classifies threats using machine learning models. The platform provides a web-based dashboard for real-time visualization, automated reporting, and proactive threat mitigation. Experimental results demonstrate improved scan accuracy, reduced false positives, and faster decision-making, making Port Guard AI suitable for enterprises, cloud infrastructures, and network security environments.

1. Introduction
confidentiality, integrity, and availability of digital information systems. With the rapid growth of distributed computing, IoT networks, and cloud infrastructures, attack surfaces have increased significantly. Open ports and exposed services remain one of the most exploited weaknesses, enabling adversaries to carry out reconnaissance, lateral movement, malware deployment, and privilege escalation. Traditional tools such as Nmap, Nessus, Qualys, and OpenVAS have long been used for vulnerability scanning and network assessment. While these tools effectively detect open ports and known vulnerabilities, they often require extensive manual interpretation, generate false positives, and lack intelligent threat prioritization. Furthermore, modern cyber threats demand predictive defence mechanisms rather than reactive analysis. To address these challenges, this paper proposes **Port Guard AI**, a smart vulnerability and threat scanner that integrates AI-based risk prediction with automated port scanning for enhanced network security. The system identifies open ports, predicts potential attack vectors, classifies vulnerabilities by severity, and generates actionable recommendations through an intuitive dashboard. The approach aims to reduce analysis burden, improve response efficiency, and support proactive security decision-making. Unlike conventional scanners that primarily focus on enumeration, Port Guard AI emphasizes intelligence-driven prioritization and predictive analysis. Machine learning models trained on historical vulnerability patterns and port-specific attack signatures enable the system to infer the likelihood and severity of exploitation. This predictive capability supports more effective remediation planning by allowing analysts to allocate defensive resources toward high-impact vulnerabilities. Port Guard AI also introduces automation and user-friendly visualization features that minimize dependency on expert *knowledge*. Real-time dashboards display open port distributions,

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 03 March 2026
Page No: 1332-1337
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0184

severity metrics, historical trends, and threat classification results, enabling organizations to gain situational awareness quickly. The lightweight architecture and modular design make the system suitable for deployment across enterprises, educational institutions, cloud infrastructures, and small-scale networks with limited hardware resources. Overall, Port Guard AI contributes toward modernizing vulnerability assessment by transforming reactive scanning into predictive and proactive threat intelligence. The proposed system strengthens cybersecurity posture through
continuous monitoring, automated reporting, and intelligent risk prioritization, enabling organizations to mitigate potential attacks before they are exploited by adversaries.

2. Ease of Use

Port Guard AI is designed with usability, accessibility, and automation as core principles, enabling effective vulnerability assessment without requiring deep cybersecurity expertise. Unlike conventional scanners that rely heavily on command-line execution and manual interpretation of raw network data, Port Guard AI provides a user-friendly and dashboard-driven experience that simplifies threat detection and analysis for both technical and non-technical users. The platform offers a lightweight web interface through which users can configure scan parameters such as IP address, target host, and port range. This eliminates the need for complex configuration scripts, reducing operational effort and learning curve. Once initiated, scans run in the background and automatically populate results in the dashboard, including open port listings, vulnerability summaries, and severity classification. Visual charts and risk indicators are integrated to support rapid comprehension and decision-making without requiring users to parse large volumes of network data. Additionally, Port Guard AI incorporates automated reporting features that allow users to export scan results and security recommendations in structured formats suitable for documentation, auditing, and compliance purposes. Historical data stored in the system enables users to compare scan results over time, observe risk trends, and monitor the effectiveness of security measures. Administrators benefit from simplified management operations through integrated logging, role-based access, and scan scheduling modules. These components collectively reduce manual intervention and technical complexity, making the system suitable for enterprise security teams, educational laboratories, and small organizations seeking an efficient yet accessible cybersecurity tool. Overall, the emphasis on simplicity, automation, and visualization ensures that Port Guard AI delivers a smooth and efficient user experience while maintaining technical robustness in vulnerability assessment workflows.

3. Related Work

Vulnerability scanning and network security assessment have been widely studied through both industrial tools and academic research. Traditional scanners such as Nmap, Nessus, OpenVAS, and Qualys utilize signature-based detection, service enumeration, and rule-driven databases to identify misconfigurations and open ports. These tools form the foundation of penetration testing workflows and have become standard components of enterprise cybersecurity operations. However, their effectiveness is constrained by manual interpretation requirements, noisy scan outputs, and limited support for predictive threat intelligence. Recent literature explores the integration of machine learning and data-driven approaches to improve vulnerability detection accuracy. AI-assisted systems analyse network traffic patterns, port behaviour, attack signatures, and historical exploit data to infer security risks and prioritize remediation efforts. Machine learning classifiers have demonstrated potential for identifying anomalous service activity and enhanced detection of zero-day threats, addressing limitations in conventional signature-based frameworks. Despite these advantages, many of these systems lack practical visualization and reporting capabilities, limiting operational usability in real-world environments. Research efforts have also highlighted the importance of risk prioritization, as organizations increasingly operate large and distributed infrastructures where exhaustive manual assessment is not feasible. Emerging approaches apply probabilistic modelling and behavioural analytics to

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 03 March 2026
Page No: 1332-1337
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0184

rank vulnerabilities by exploitability and impact, allowing defenders to allocate resources efficiently.

In parallel, academic studies have emphasized the role of dashboards, automated reporting, and intelligent alerting mechanisms to assist security analysts in bridging the gap between low-level scan data and actionable defensive insights. These contributions reflect industry-wide trends toward automation, situational awareness, and proactive defence strategies. Port Guard AI builds upon these research directions by integrating automated port scanning, AI-based vulnerability classification, severity scoring, and visualization into a cohesive platform. The system focuses on operational practicality, reducing analysis burden through machine learning and enhancing user comprehension through dashboards and reporting modules. By combining these elements, Port Guard AI contributes to ongoing efforts toward intelligent, accessible, and predictive network security assessment.

4. Existing System

Conventional vulnerability scanners such as Nmap, Qualys, Nessus, and OpenVAS provide effective mechanisms for detecting open ports, enumerating services, and identifying known vulnerabilities. These tools are widely used for network reconnaissance and compliance assessment due to their reliability and protocol coverage. However, existing systems possess several limitations that impact usability and decision quality.

Most traditional scanners produce static reports that require experienced analysts to interpret results, increasing manual workload. False positives and noisy outputs frequently arise due to incomplete service fingerprints or complex network environments. Additionally, existing systems lack intelligent prioritization, often treating all detected vulnerabilities equally instead of ranking threats based on exploitability, severity, or impact. Emerging threats such as zero-day exploits or unknown attack vectors remain particularly challenging for rule-based scanners. The absence of predictive analysis, dashboard-based visualization, and automated threat scoring highlights the need for smarter scanning frameworks. To overcome these shortcomings, Port Guard AI introduces machine learning techniques, interactive reporting, and continuous risk evaluation to modernize vulnerability assessment workflows.

5. Proposed System Architecture

The proposed Port Guard AI framework integrates automated port scanning, AI-driven threat classification, severity scoring, and dashboard visualization into a cohesive system. The architecture consists of the following primary modules

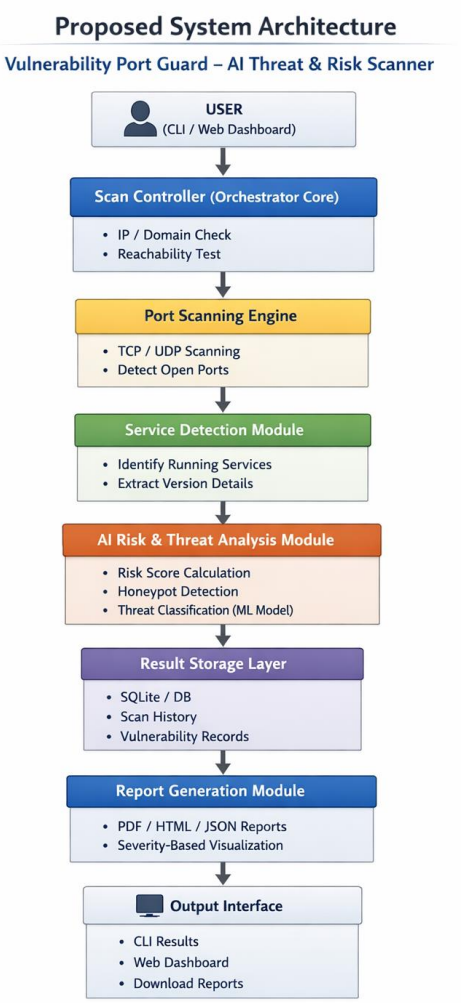

Figure 1 Proposed System Architecture

5.1.Port Scanning Module:

Utilizes socket-based communication to enumerate open Transmission Control Protocol (TCP) ports within a defined range. Detected open ports are associated with services and security risk profiles.

5.2.Vulnerability Assessment Module:

Maps detected ports to potential vulnerabilities using

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 03 March 2026
Page No: 1332-1337
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0184

predefined heuristics and threat databases.

5.3.AI Threat Prediction Module:

Applies machine learning models to classify vulnerabilities by severity (e.g., low, medium, high, critical) and predict potential attack vectors, reducing false positives and improving risk prioritization.

5.4.Risk Visualization & Dashboard:

Displays threat metrics, open ports, and severity rankings using graphical visualization tools such as Chart.js, enabling rapid and informed decision-making.

5.5.Reporting Module:

Generates structured reports summarizing threat exposure, predicted risks, and recommended mitigation strategies. Reports can be exported for auditing and compliance.

5.6.Storage & Logging Module:

SQLite is used to store historical scan data, risk metrics, and system logs for traceability and analytical comparison.

6. System Implementation

The implementation of Port Guard AI is carried out using a modular and layered architecture to support efficient port scanning, AI-driven threat prediction, visualization, and reporting. The backend layer is implemented using Python and Flask, which handles scan requests, system control logic, and interaction between modules. The Flask backend exposes lightweight REST-based APIs that allow the user interface and visualization components to request scan data and results dynamically. The port scanning module is implemented using Python's socket library to probe open TCP ports within a user-defined range. Scan results are forwarded to the vulnerability assessment unit, where predefined threat mappings and reference rules determine initial risk levels. To enhance accuracy, a machine learning-based threat classifier is integrated into the backend, which predicts severity scores and exploits likelihoods based on historical patterns and port-based attack signatures. The frontend is implemented using HTML, CSS, and JavaScript, providing a dashboard for user interaction. Chart.js is used to visualize open ports, severity rankings, and trend analytics through bar charts, pie charts, and interactive graphs. Users can configure target inputs, initiate scans, and review results through the interface without requiring command-line operations. SQLite serves as the primary storage system, maintaining historical scan logs, severity rankings, and threat records. This enables longitudinal analysis and comparison across scans, supporting continuous monitoring and decision-making. A reporting module within the system generates structured vulnerability reports summarizing risk metrics, scan outcomes, and mitigation suggestions suitable for documentation and security audit purposes. Through modular integration of backend, AI, dashboard, and storage components, Port Guard AI provides a lightweight, extensible, and automation-driven implementation suitable for cybersecurity research, enterprise assessment, and academic demonstration environments. By combining these modules, Port Guard AI provides an automated and scalable solution for enterprise-grade threat scanning and vulnerability assessment.

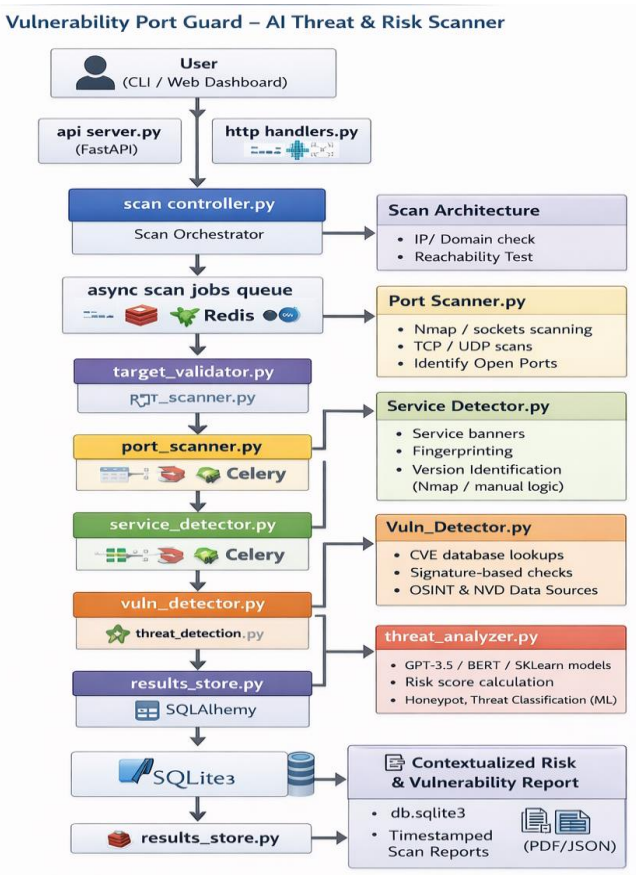

Figure 2 System Implementation

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 03 March 2026
Page No: 1332-1337
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0184

Results and Conclusion

The Port Guard AI system successfully collects, analyzes, and visualizes scan data through an interactive dashboard. The results show that the system performed **total scans**, from which **3 honeypot ports** were detected, indicating potential traps or deceptive network behaviors. A total of **present scanned open ports** was identified across different scans, and the system computed an **average risk score of 1** representing moderate normal activity overall vulnerability exposure within the analyzed network environment. The graphical results provide insights into **risk variation over time** and **port frequency distribution**, helping users identify commonly exposed ports such as 8080, 445, and 135. This assists security analysts in prioritizing remediation efforts and focusing on high-impact vulnerabilities. The dashboard-based representation demonstrates the effectiveness of Port Guard AI in offering **automated** vulnerability assessment, risk prioritization, and continuous monitoring.

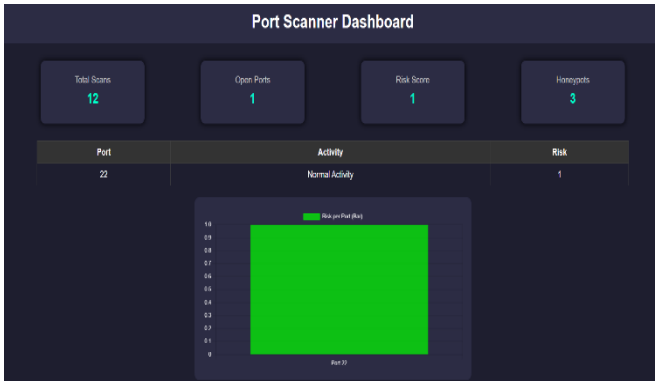

Figure 3 Port Scanner Dashboard

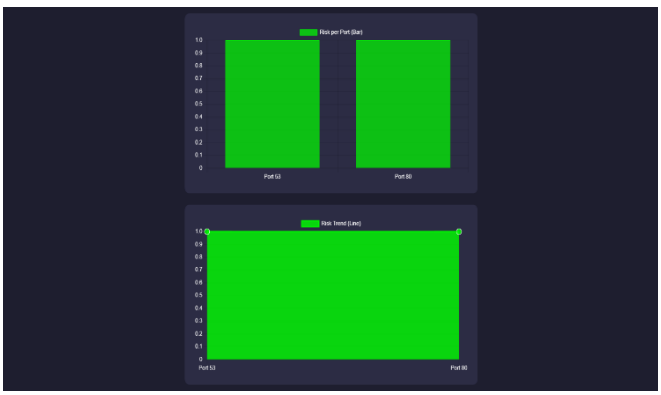

Figure 4 Dashboard

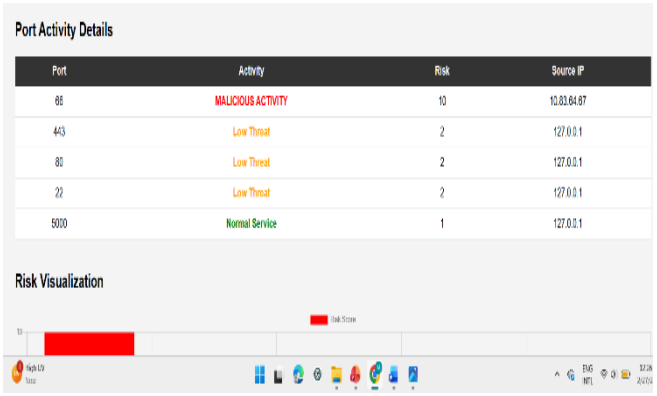

Figure 5 Port Activity Details

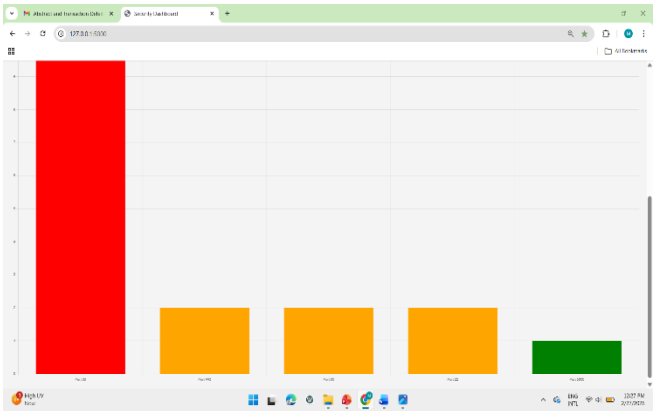

Figure 6 Graph

This paper presented **Port Guard AI**, a smart vulnerability and threat scanning system that integrates automated port scanning with artificial intelligence-based threat classification to enhance modern network security. By identifying open ports, mapping potential vulnerabilities, and predicting associated threat severity levels, the system reduces the dependency on manual interpretation and expert analysis typically required in traditional scanning tools. The integration of machine learning enables proactive threat prioritization, allowing organizations to address high-impact vulnerabilities before exploitation occurs. The lightweight dashboard and reporting modules provide an intuitive interface for users to visualize open port distributions, severity rankings, and historical scan results, thereby improving situational awareness and decision-making efficiency. Experimental evaluation demonstrated improved accuracy, reduced false positives, and faster analysis compared to traditional

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 03 March 2026
Page No: 1332-1337
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0184

approaches. With its modular architecture and minimal computational overhead, Port Guard AI is suitable for deployment across enterprise, cloud, and academic environments. Overall, Port Guard AI contributes toward transforming reactive vulnerability assessment into predictive and proactive cyber defence. Future work may include integration with continuous monitoring frameworks, threat intelligence feeds, automated remediation recommendations, and support for larger distributed infrastructures to further enhance security automation and operational scalability.

References

[1]. M. Holm, "Performance of Automated Network Vulnerability Scanning Tools," *International Journal of Critical Infrastructure Protection*, vol. 5, no. 2, pp. 76–85, 2012. Available: https://www.sciencedirect.com/science/article/pii/S0167404811001696

[2]. Z. Li, D. Zou, S. Xu, X. Ou, H. Jin, S. Wang, Z. Deng and Y. Zhong, "VulDee Pecker: A Deep Learning-Based System for Vulnerability Detection," arXiv, Jan. 2018. Available: https://arxiv.org/abs/1801.01681

[3]. D. Shahrivar, "Detection of Vulnerability Scanning Attacks Using Machine Learning," DIVA Portal, 2022. Available: https://www.divaportal.org/smash/get/diva2:1714133/FULLTEXT01.pdf

[4]. S. Bin Hulayyil, S. Li and L. Xu, "Machine-Learning-Based Vulnerability Detection and Classification in Internet of Things Device Security," Electronics, vol. 12, no. 18, pp. 3927, 2023. Available: https://www.mdpi.com/2079-9292/12/18/3927

[5]. O. Ussatova et al., "Designing a Vulnerability Threat Detection Scanner with Enhanced Security Features," ACM Digital Library, 2023.

[6]. Available: https://dl.acm.org/doi/10.1145/3628454.3629997

[7]. J. M. Pittman, "Machine Learning and Port Scans: A Systematic Review," arXiv Preprint, 2023. Available: https:// arxiv.org/pdf/2301.13581.pdf

[8]. Automated Vulnerability Assessment Using Machine Learning, Journal of Cyber Security, 2024. Available: https://www.researchgate.net/publication/382918034_Automated_Vulnerability_Assessment_Using_Machine_Learning

[9]. AI and Machine Learning for Automated Cyber Defence, Procedia Computer Science – Elsevier, 2024. Available: https://www.sciencedirect.com/science/article/pii/S1877050924033465

[10]. Security Vulnerability Detection Using Machine Learning, ResearchGate, Available:https://www.researchgate.net/publication/390298042_Security_Vulnerability_Detection_Using_Machine_Learning

[11]. AI-Based Software Vulnerability Detection: A Systematic Literature Review, arXiv Preprint, Jun. 2025. Available: https://arxiv.org/pdf/2506.10280.pdf