Plug-and-Scan: A Lightweight Hardware-Based Physical Layer Security Device for Real-Time IoT Network Monitoring and Threat Detection

Mr. Zaid A. Maniyar[1], Mr. Saurabh Singh[2], Mr. Ashirwad Jenamani[3],
Mr. Himanshu Goswami[4], Dr. Jyoti Gangane[5]
[1,2,3,4]*Student, Vishwaniketan's Institute of Management Entrepreneurship and Engineering Technology (ViMEET), Khalapur*
[5]*Professor, EXTC Dept. Vishwaniketan's Institute of Management Entrepreneurship and Engineering Technology (ViMEET), Khalapur*

***Abstract*—The rapid growth of Internet of Things (IoT) devices has increased cybersecurity risks due to weak security measures such as default passwords, unencrypted communication, and lack of secure firmware updates, making networks vulnerable to attacks like Man-in-the-Middle (MitM), Distributed Denial of Service (DDoS), and data theft, while also highlighting a gap in practical hardware-based cybersecurity knowledge. To address these challenges, this paper presents the design and implementation of a Plug-and-Scan Physical Layer Security Device, a low-cost, portable, and plug-and-play hardware solution that can be easily integrated into existing networks without major configuration changes, operating at the physical and data link layers to monitor both wired and wireless traffic in real time. The device captures and analyzes network packets to detect abnormal behavior, unauthorized access, and potential threats using a custom lightweight Intrusion Detection System (IDS) built with suricata, while also performing scheduled vulnerability scanning using Nmap to identify open ports, weak configurations, and security loopholes, with all results displayed on a user-friendly Flask-based web dashboard. Unlike traditional expensive and complex security systems, this solution is affordable and suitable for smart homes, small offices, educational institutions, and research labs, while also serving as a practical learning platform for students and researchers to gain hands-on experience in embedded systems and cybersecurity. Overall, the project demonstrates that a hardware-based, integrated approach can effectively enhance network security, provide real-time threat detection, and bridge the gap between theoretical knowledge and real-world implementation, with future scope for AI-based detection, cloud integration, and expanded protocol support.**

***Index Terms*—Physical Layer Security, IoT Security, Intrusion Detection System, Raspberry Pi, Suricata, Network Monitoring, Transparent Bridge, Vulnerability Scanning.**

I. INTRODUCTION

The rapid advancement of Internet of Things (IoT) technologies has significantly transformed modern communication systems by enabling seamless connectivity between devices across domains such as smart homes, healthcare, and industrial automation. However, this widespread adoption has also introduced serious security challenges. Many IoT devices operate with weak security configurations, including default credentials, unencrypted communication, and lack of secure firmware updates, making them highly vulnerable to cyber threats such as Man-in-the-Middle (MitM) attacks, Distributed Denial of Service (DDoS) attacks, and unauthorized data access.

Traditional network security mechanisms primarily rely on software-based solutions such as firewalls and intrusion detection systems, which are often resource-intensive and require complex configurations. These limitations make them unsuitable for low-cost embedded systems and small-scale networks. Furthermore, existing solutions often fail to address vulnerabilities at the physical and data link layers, which are critical points of attack in IoT environments. To address these challenges, this paper proposes a Plug-and-Scan Physical Layer Security

Device, a hardware-based solution designed to provide real-time monitoring, intrusion detection, and vulnerability scanning. The device operates as a transparent bridge at Layer 2, allowing it to monitor network traffic without requiring any modifications to the existing network infrastructure. The system integrates lightweight intrusion detection using Suricata, scheduled vulnerability scanning using Nmap, and a web-based monitoring dashboard developed with Flask.

The main contribution of this work lies in developing a low-cost, plug-and-play security solution that bridges the gap between theoretical cybersecurity concepts and practical implementation in embedded systems. The proposed system is suitable for educational environments, small offices, and smart home setups where enterprise-level tools are not feasible.

II. LITERATURE REVIEW

Several research efforts have focused on improving IoT network security using embedded platforms and intrusion detection techniques.

Garalov and Elhajj (2023) proposed a Raspberry Pi-based Intrusion Detection System (IDS) for IoT environments that demonstrated effective real-time traffic monitoring and intrusion detection capabilities. However, the system lacked scalability and was not suitable for large-scale network deployments, limiting its practical applications [1].

Verma and Ranga (2020) developed a machine learning-based IDS for IoT applications that improved detection accuracy and enabled intelligent threat identification. Despite its effectiveness, the system required high computational resources, making it less suitable for implementation on resource-constrained embedded devices [2].

Al-Hawawreh et al. (2018) introduced a deep learning-based intrusion detection approach for Industrial IoT environments capable of detecting complex and unknown cyber threats. However, the system involved high complexity and computational requirements, making it unsuitable for lightweight and low-cost hardware platforms [3].

Soe et al. (2020) proposed a lightweight IDS optimized for IoT environments using feature selection techniques to improve efficiency. While the system reduced computational overhead, it involved trade-offs between accuracy and performance and showed limitations in detecting advanced attack patterns [4].

Amro (2020) presented a comprehensive study on IoT vulnerability scanning techniques, highlighting tools such as Nmap and Shodan for identifying network weaknesses. Although the study provided valuable insights, it lacked real-time implementation and practical deployment aspects.

Similarly, Al-Alami et al. (2017) demonstrated vulnerability scanning of IoT devices using Shodan, but the approach primarily focused on device discovery and visibility rather than providing an integrated intrusion detection solution [5], [6].

These studies indicate that although significant advancements have been made in IoT security, most existing systems focus on either intrusion detection or vulnerability scanning individually and require high computational resources or complex configurations. This creates a need for an integrated, lightweight, and hardware-based solution such as the proposed Plug-and-Scan Physical Layer Security Device.

III. SYSTEM DESIGN AND METHODOLOGY

A. Proposed System Architecture

The proposed Plug-and-Scan Physical Layer Security Device is designed as a hardware-based network security solution providing real-time monitoring, intrusion detection, and vulnerability scanning. The system follows a simple plug-and-play architecture where the device is connected between the router and network devices without requiring any modification to the existing network infrastructure.

The core component is a Raspberry Pi 3b+ (1GB RAM) acting as the central processing unit. The system captures network traffic through both wired (Ethernet) and wireless (Wi-Fi) interfaces. Captured data packets are then processed and analyzed using predefined rules and algorithms. The architecture follows a clear data flow model:

Input → Processing → Output, with the output displayed on a web-based Flask dashboard.

B. Block Diagram

The system comprises the following functional blocks:

(1) Power Supply — provides stable 5V/3A to all components;

(2) Raspberry Pi 3b+ — main processing and control unit;

(3) Network Interface (eth0 / USB-Ethernet) — captures wired and wireless traffic via transparent bridge br0;

(4) Custom Packet Sniffer & IDS (suricata) — performs real-time packet capture and rule-based threat detection;

(5) Vulnerability Scanner (Nmap) — executes scheduled network scans;

(6) SQLite Database — stores all logs, alerts, and scan results;

(7) Flask Web Dashboard — displays real-time monitoring data to the user.

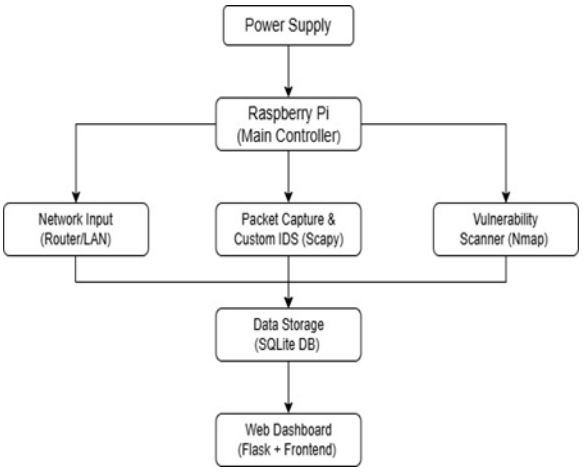

Figure 1: Functional Block Diagram of the Proposed System

C. Transparent Bridge Design

The device creates a transparent Layer 2 bridge (br0) by combining eth0 (connected to router) and eth1 (USB-to-Ethernet adapter connected to LAN). This setup allows all network traffic to pass through the Raspberry Pi without being assigned an IP address on the monitored interfaces, making the device invisible to the network while fully capturing all packets.

D. Methodology

The system methodology follows a sequential and scheduled execution model:

1) The device is connected between the router and LAN using plug-and-play setup.
2) System initializes all hardware and software modules including bridge interfaces and Flask server.
3) Custom packet sniffer (Suricata) starts capturing real-time packets from br0 interface.
4) Captured packets are analyzed using rule-based intrusion detection logic.
5) Detected threats are logged in SQLite database and alerts are pushed to the web dashboard.
6) At scheduled intervals, IDS is paused and Nmap vulnerability scan is executed.
7) Nmap scan results are parsed, stored, and IDS monitoring is resumed.
8) The process continues in a continuous loop until the device is powered off.

IV. IMPLEMENTATION

A. Hardware Setup

The system is implemented using a Raspberry Pi 3b+ (1GB RAM) running DietPi, a lightweight Debian-based Linux distribution optimized for minimal resource consumption. A USB-to-Ethernet adapter (USB 3.0) provides the second network interface (eth1). The bridge interface br0 is created by binding eth0 and eth1 using Linux bridge utilities. The device is powered via a 5V/3A USB-C adapter ensuring stable continuous operation.

B. Software Components

Python is used as the primary programming language for all system logic. The custom IDS is built using Suricata for packet capture and analysis. Nmap is integrated for vulnerability scanning through the python-nmap library. The web dashboard is developed using Flask with a frontend built on HTML, CSS, and JavaScript. All data is stored in an SQLite database for lightweight and fast access. System timers are used to schedule periodic vulnerability scans without interfering with the IDS.

C. Intrusion Detection Logic

The IDS implements rule-based detection for the following threats: SYN Flood — detected by

counting SYN packets from a single source exceeding a threshold within a time window; Port Scanning identified by multiple TCP connection attempts to different ports from a single IP; ARP Spoofing detected by monitoring ARP reply inconsistencies that may indicate a Man in the Middle attack attempt.

Asynchronous packet processing is achieved by running the sniffer in a dedicated thread that pushes packets into a queue, while a separate analysis thread processes packets. This separation ensures continuous high-speed capture without blocking.

D. Resource Optimization

Several optimizations are applied to ensure stable operation on 1GB RAM: packet filtering at the capture level to discard irrelevant traffic; non-concurrent execution of IDS and Nmap to prevent memory overload; kernel parameter tuning for network performance; and compressed swap space (zram) to handle memory pressure during peak activity.

V. RESULTS AND DISCUSSION

The proposed Plug-and-Scan Physical Layer Security Device was successfully implemented and tested in a real-time network environment. The system was evaluated based on its ability to monitor network traffic, detect intrusions, and perform vulnerability scanning using a Raspberry Pi 3B+ platform.

During testing, the system analyzed approximately 9,00,000 network packets, demonstrating its capability to handle high-throughput traffic efficiently. The integration of Suricata enabled accurate detection of suspicious activities, including TCP SYN scan attacks, which are commonly used during the reconnaissance phase of cyberattacks. A total of 256 alerts were generated, indicating the effectiveness of the intrusion detection mechanism.

The system also performed vulnerability scanning using Nmap, identifying open ports and assessing network security conditions. The calculated network risk score and severity distribution provided a clear understanding of the security status of the network. The Flask-based dashboard successfully visualized real-time data, including active devices, alerts, packet statistics, and risk metrics, making the system user-friendly and informative.

Figure 5.1: Dashboard Overview

Fig. 1 shows the main dashboard displaying active devices, network risk score, and vulnerability summary. The system detected multiple devices and indicated a low-risk network condition.

Figure 5.2: Scan Timeline and Alerts

Fig. 2 illustrates scan history and system performance metrics, including memory usage and device tracking. It demonstrates stable system operation over time.

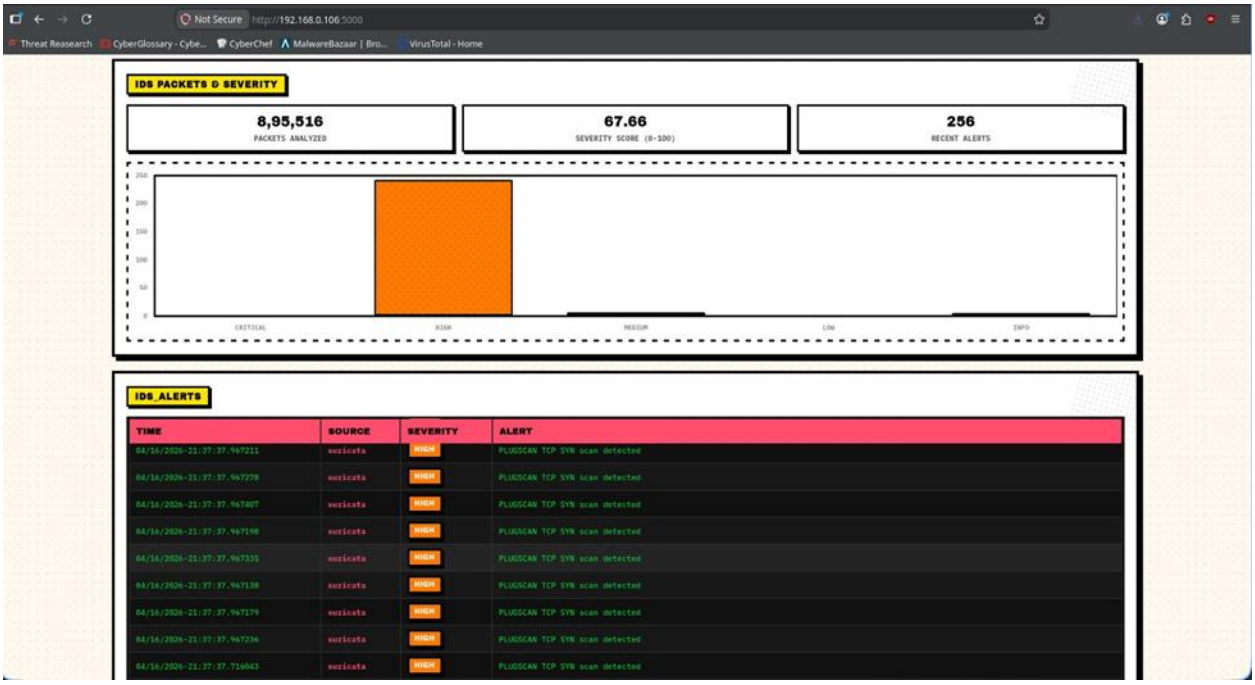

Figure 5.3: IDS Packets and Severity Analysis

Fig. 3 represents packet analysis and severity levels of detected threats. The system processed a large number of packets and classified alerts based on severity.

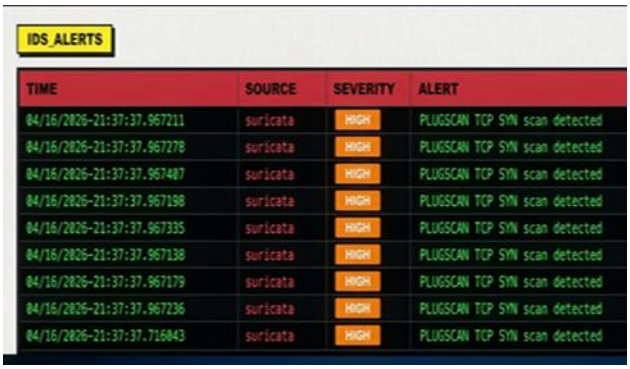

Figure 5.4: IDS Alerts Table

Fig. 4 shows detailed IDS alerts generated by Suricata, including timestamp, source, severity, and type of attack such as TCP SYN scans.

VI. CONCLUSION

The Plug-and-Scan Physical Layer Security Device presents an effective and practical solution for enhancing IoT network security using a lightweight, hardware-based approach. The system successfully integrates real-time packet monitoring, intrusion detection using Suricata, and vulnerability scanning using Nmap into a single compact device that can be easily deployed without modifying existing network infrastructure. Experimental results demonstrate that the system is capable of analyzing a large volume of network traffic, processing approximately 9,00,000 packets while maintaining stable performance on the Raspberry Pi 3B+ platform. The detection of high-severity events such as TCP SYN scan attacks confirms the effectiveness of the intrusion detection mechanism in identifying potential threats at an early stage. Additionally, the generation of multiple alerts and the visualization of network activity through a Flask-based dashboard enhance the usability and practical value of the system. The plug-and-play architecture ensures ease of deployment, making the solution suitable for smart homes, small offices, educational institutions, and research laboratories. Although the system is limited by hardware constraints and relies on signature-based detection, it provides a strong foundation for further improvements.

Overall, the proposed system successfully bridges the gap between theoretical cybersecurity concepts and real-world implementation by providing a cost-effective, portable, and user-friendly network security solution for IoT environments.

REFERENCES

[1] T. Garalov and M. Elhajj, “Enhancing IoT security: Design and evaluation of a Raspberry Pi-based intrusion detection system,” in Proc. IEEE Conf. on Security and Privacy, 2023.

[2] A. Verma and V. Ranga, “Machine learning based intrusion detection systems for IoT applications,” Wireless Personal Communications, vol. 111, pp. 2287–2310, 2020.

[3] M. Al-Hawawreh, N. Moustafa, and E. Sitnikova, “Identification of malicious activities in industrial Internet of Things based on deep learning models,” Journal of Information Security and Applications, vol. 41, pp. 1–11, 2018.

[4] Y. N. Soe, Y. Feng, P. I. Santosa, R. Hartanto, and K. Sakurai, “Towards a lightweight detection system for cyber-attacks in the IoT environment using corresponding features,” Electronics, vol. 9, no. 1, p. 144, 2020.

[5] A. Amro, “IoT vulnerability scanning: A state of the art,” in Computer Security, ESORICS Workshops, Lecture Notes in Computer Science, vol. 12501, Springer, 2020, pp. 57–75.

[6] H. Al-Alami, A. Hadi, and H. Al-Bahadili, “Vulnerability scanning of IoT devices in Jordan using Shodan,” in Proc. IT-DREPS Conf., 2017, pp. 1–6.