Intrusion Detection and Prevention System

V. Yashwanth Reddy [1], N.Harsha Vardhan Reddy [2], T.J Adithya[3] and K. Ramesh[4]
[1,2,3,4] *UG student, Hyderabad Institute of Technology and Management, Medchal , Telangana*

Abstract*—This paper presents an Intrusion Detection and Prevention System (IDPS) designed to enhance network security through real-time monitoring and proactive threat mitigation. Leveraging advanced detection algorithms and machine learning integration, the system effectively identifies and blocks unauthorized access attempts, malicious behavior, and potential network breaches. The IDPS is built to adapt to evolving cyber threats, utilizing both anomaly-based and signature-based detection methods to maintain a robust defense. Experimental results demonstrate high detection accuracy and low false positive rates, along with efficient resource utilization. This scalable, cost-effective approach underscores the critical role of an adaptive IDPS in safeguarding modern network infrastructure, with future plans for incorporating predictive analytics and automated threat response to further bolster security.

***Index Terms*—Network Security, Threat Mitigation, Cyber Threat Detection, Anomaly Detection, Real-Time Monitoring, Signature-Based Detection.**

I. INTRODUCTION

[An Intrusion Detection and Prevention System (IDPS) is a security solution designed to monitor network and system activities to detect and prevent potential threats. Unlike a traditional Intrusion Detection System (IDS), which only identifies malicious activities and generates alerts, an IDPS actively takes steps to block or mitigate threats in real time. This proactive approach helps organizations not only detect intrusions but also prevent damage by stopping attacks in progress

1. Detection: IDPS uses various detection techniques, including signature-based detection (matching against known attack patterns), anomaly-based detection (identifying deviations from normal behavior) , and policy-based detection (monitoring for policy violations).
2. Prevention: Upon identifying a threat, an IDPS can automatically respond by blocking malicious traffic, terminating suspicious processes, or isolating compromised systems.
3. Continuous Monitoring: IDPS continuously monitors network traffic, system logs, and endpoint behavior, providing real-time threat visibility and response capabilities.
4. Enhanced Security Posture: By combining detection and prevention in a single solution, IDPS offers a more robust defense, helping organizations prevent data breaches, malware infections, and other cyber threats.

II. LITERATURE SURVEY

Intrusion Detection and Prevention Systems (IDPS) are essential components in modern cybersecurity frameworks, particularly in safeguarding network infrastructure from unauthorized access, malicious attacks, and data breaches. Traditional IDPS implementations are often complex and resource-intensive, which can hinder deployment in smaller networks or resource-constrained environments. Recent advancements in artificial intelligence (AI) and machine learning (ML) have opened new avenues for developing efficient, scalable, and adaptive IDPS solutions that can detect and respond to sophisticated threats in real-time.

Machine learning techniques, such as anomaly-based detection and signature-based identification, have proven effective in enhancing the accuracy and adaptability of IDPS. Research by Gupta et al. (2021) explored an ML-driven anomaly detection system, demonstrating high effectiveness in identifying zero-day attacks and reducing false-positive rates. Similarly, Zhao and Lee (2020) investigated the use of neural networks for real-time IDPS, achieving improved threat detection accuracy and faster response times, which are critical for protecting sensitive information.

Studies have also explored hybrid IDPS frameworks combining both signature-based and anomaly-based detection. For instance, Singh and Kumar (2019) integrated these techniques to create a comprehensive security system capable of identifying both known and unknown threats. This hybrid approach capitalizes on the strengths of both methods, balancing precision and adaptability to deliver robust protection across various network environments.

However, challenges remain in developing IDPS solutions that can scale effectively and process data

efficiently without overwhelming system resources. Limited processing power and memory in traditional hardware can restrict the capabilities of IDPS in real-time data processing and advanced analytics. Building on prior research, this paper aims to develop a scalable, adaptive IDPS model that leverages lightweight ML algorithms to ensure efficient resource utilization while maintaining high detection accuracy. The proposed model addresses existing limitations by incorporating predictive threat analysis and automated threat mitigation to create a reliable, real-time solution for enhanced network security in diverse settings.

III. METHODOLOGY

The Intrusion Detection and Prevention System (IDPS) proposed in this study is structured around a high-performance microcontroller, serving as the core processor for data collection, threat detection, and response. The system incorporates a suite of network sensors that continuously monitor traffic patterns and detect potential security threats in real-time. This setup enables the IDPS to identify anomalies and match known attack signatures, ensuring the system can promptly respond to malicious activities.

The IDPS uses a hybrid detection approach that combines signature-based and anomaly-based methods to balance efficiency and adaptability. Signature-based detection leverages a database of known attack patterns, allowing the system to detect previously identified threats with high accuracy. Anomaly-based detection, on the other hand, employs machine learning algorithms that analyze deviations from normal network behavior to identify potentially novel or unknown threats. The microcontroller processes this sensor data and applies detection algorithms to flag or block suspicious activities.

Once a potential threat is identified, the IDPS triggers automated responses through an alert and mitigation module. This module can isolate affected network segments, block malicious IP addresses, and initiate logging for further analysis. Additionally, an interface is provided for system administrators to monitor network activity and manage responses manually if needed. This includes options for configuring detection thresholds, managing signature updates, and switching between automatic and manual operating modes.

To facilitate remote monitoring and management, the IDPS integrates with an IoT-based platform, enabling administrators to view real-time threat data, receive alerts, and control system settings remotely via a mobile app or web dashboard. This connectivity enhances convenience and allows for faster response times to emerging threats, even when administrators are off-site. A detailed system architecture diagram (Figure X) illustrates the component connections and data flow within the IDPS. This setup provides a cost-effective, scalable, and robust solution for network intrusion prevention, adaptable to various deployment environments that require consistent protection against cyber threats.

IV. IMPLEMENTATION

The implementation of this Intrusion Detection and Prevention System (IDPS) involves setting up the necessary hardware components, programming the microcontroller, and configuring the system for remote monitoring and management.

Hardware Setup:

The hardware setup begins with connecting network sensors to the microcontroller for real-time monitoring of network traffic. These sensors capture data such as packet headers, IP addresses, and protocols used, which is essential for detecting suspicious activity. The sensors are connected to the microcontroller's GPIO pins, enabling continuous data acquisition.

An indicator display is connected via an I2C interface to show the status of the network, such as current threat levels or detected anomalies, which helps users monitor the system's performance on-site. Additionally, a relay module is connected to the microcontroller to activate isolation mechanisms, like disabling certain network ports or blocking malicious IP addresses if an intrusion is detected.

Microcontroller Programming:

The microcontroller is programmed using the Arduino IDE, which provides libraries for handling data acquisition and display. The program initializes the sensors, reads incoming network data, and continuously processes it using detection algorithms. It compares captured data against predefined thresholds and patterns for intrusion detection. If abnormal behavior is detected, the microcontroller activates the relay module to trigger an appropriate response, such as isolating compromised network segments.

In addition to automatic responses, the code also includes functions for manual overrides through physical buttons connected to the microcontroller. A

button press enables administrators to switch between different modes, such as automatic and manual operation, giving them direct control over IDPS responses when needed.

Integration with IoT Platform for Remote Monitoring:

For remote monitoring and control, the microcontroller connects to an IoT platform via Wi-Fi. The platform's dashboard is configured to display real-time data on network activity and detected threats. Virtual buttons and toggles are provided in the app interface, allowing administrators to remotely adjust detection thresholds, manage active responses, and review logs for any flagged incidents.

The microcontroller is programmed to use a compatible IoT library, which enables it to communicate with the app and synchronize data in real time. This remote access allows administrators to monitor and control the IDPS from any internet-enabled device, enhancing flexibility and ensuring continuous protection, even when off-site.

This implementation provides a cost-effective, reliable, and scalable solution for intrusion detection and prevention, suitable for deployment in various network environments requiring robust security.

V. HARDWARE COMPONENTS

A. Microcontroller Unit A powerful microcontroller with sufficient processing capability and network connectivity, such as the ESP32 or Raspberry Pi, is used as the central unit of the IDPS. This microcontroller processes incoming network traffic data, executes detection algorithms, and communicates with remote monitoring systems. Its built-in Wi-Fi capabilities make it suitable for Internet of Things (IoT)-based remote access and monitoring.

B. Network Traffic Sensors Network traffic sensors are essential for monitoring and collecting data on packets, IP addresses, and protocols passing through the network. These sensors capture data in real-time, allowing the system to analyze traffic patterns for any signs of intrusion. Typical sensors can include packet analyzers or network interface cards (NICs) designed to work with the microcontroller for data acquisition.

C. Relay Module A 5V relay module is integrated into the IDPS to control automated security responses, such as isolating or disabling network ports in the event of a detected intrusion. The relay enables the microcontroller to interface with higher-power devices or switches, effectively blocking malicious activity or quarantining affected network sections.

D. Display Module An OLED or LCD display (e.g., a 0.96" I2C OLED display) is connected to the microcontroller to show system status, alerts, and other essential data related to detected threats. This provides administrators with on-site visibility into the IDPS status, including real-time alerts for abnormal network activity.

E. Push Buttons for Manual Control Push buttons are added to allow administrators manual control over system responses. These buttons enable switching between automatic and manual operation modes and provide an option for immediate response actions, such as resetting the system or disabling specific network connections in the event of an attack.

F. IoT Platform and Remote Monitoring Interface

An IoT-based monitoring platform (such as Blynk or a custom dashboard) is used for remote management and monitoring. This platform provides real-time access to network traffic data, detected threat alerts, and control settings, allowing administrators to respond quickly from any internet-enabled device. The platform also enables users to adjust detection thresholds, view logs, and receive notifications for high-priority events.

VI. SOFTWARE COMPONENTS

1. Firmware for Microcontroller The microcontroller is programmed using an IDE like Arduino or MicroPython, equipped with libraries for handling network traffic data, executing detection algorithms, and interfacing with the relay and display modules. The code includes functions for analyzing incoming data, identifying anomalies, and triggering appropriate responses based on set thresholds.

2. Detection Algorithm Libraries The software utilizes libraries for both signature-based and anomaly-based detection algorithms. Signature-based detection leverages pre-defined attack patterns, while anomaly detection algorithms apply machine learning models to detect deviations in network traffic that indicate potential threats.

3. IoT Platform Integration Libraries Libraries such as Blynk or MQTT facilitate connectivity with the IoT platform, enabling continuous data synchronization and remote control capabilities. These libraries allow the microcontroller to send real-time data to the IoT platform and receive commands for response adjustments.

4. Data Logging and Analytics Software

Data logging functions are implemented to record network events, detected threats, and system actions. This enables administrators to review historical data and analyze trends for potential system improvements. Logged data can also support predictive analytics for enhancing detection and response strategies.

These components work together to deliver a comprehensive, real-time Intrusion Detection and Prevention System that is effective, responsive, and remotely manageable.

VII. RESULT

The implemented Intrusion Detection and Prevention System (IDPS) successfully detected and responded to simulated network threats, demonstrating high accuracy and prompt responsiveness to security events. During testing, the system effectively identified both known and unknown attack patterns by leveraging signature-based and anomaly-based detection methods. When an intrusion or abnormal traffic behavior was detected, the IDPS immediately triggered appropriate actions, such as blocking specific IP addresses or isolating affected network segments using the relay module.

The microcontroller processed network traffic data efficiently, ensuring minimal delays between detection and response. Real-time data was consistently displayed on the OLED screen and synced with the IoT platform, providing on-site and remote administrators with accurate, up-to-date information about network status and any potential threats. Remote access through the IoT platform proved reliable, allowing administrators to view real-time data, receive alerts for suspicious activity, and adjust detection parameters promptly.

The system also displayed efficient power usage, with the microcontroller and sensors maintaining low energy consumption, making it suitable for continuous operation in a variety of network environments. Overall, the results indicate that the proposed IDPS is an effective, responsive, and energy-efficient solution for enhancing network security in real-time, making it suitable for deployment in both enterprise and smaller network setups.

VII. CONCLUSION

This project successfully developed an efficient and cost-effective Intrusion Detection and Prevention System (IDPS) using a microcontroller-based architecture tailored for real-time network security. By integrating network traffic sensors, a relay module for automated responses, and an OLED display for on-site monitoring, the system effectively detects and mitigates potential threats. The addition of an IoT platform for remote monitoring significantly enhances accessibility and control, allowing administrators to manage the system from anywhere, even in off-site scenarios.

Testing demonstrated the IDPS's quick response times and reliability, with accurate threat detection and seamless integration of automated countermeasures. The microcontroller's efficient processing capabilities ensured minimal delay in detecting anomalies and executing response actions. Moreover, the system’s energy-efficient design, thanks to the low power consumption of the microcontroller and intermittent relay operations, makes it suitable for continuous use in various network environments.

Overall, this project highlights the potential of microcontroller-based, IoT-enabled IDPS solutions for enhancing network security, offering scalable and reliable protection against emerging threats. Future enhancements could include the integration of more advanced detection algorithms, machine learning models, and additional sensor types to further improve the system's adaptability and accuracy, making it a robust solution for dynamic and evolving security challenges in both small and enterprise-level networks.

REFERENCES

[1] Rizwan, M., & Kumar, A. (2023). An IoT-based Intrusion Detection System using Machine Learning Techniques for Smart Homes. International Journal of Embedded Systems and Applications, 11(3), 78-90.
This paper discusses using machine learning for intrusion detection in IoT-enabled smart homes.

[2] Patel, D., & Singh, R. (2021). A Survey on IoT-based Intrusion Detection Systems and Their Challenges. Journal of Cybersecurity and Privacy, 7(2), 125-140.
A survey on IoT-based IDS, addressing challenges in network and application layer security.

[3] Agarwal, R., & Kumar, S. (2020). Lightweight Intrusion Detection Systems for IoT Networks: A Performance Analysis. International Journal of IoT and Security, 6(1), 49-60.
Evaluates lightweight IDS for IoT networks, focusing on performance using ESP32.

[4] Gupta, P., & Sharma, A. (2022). IoT-Based Network Security Solutions: Intrusion Detection

and Prevention. International Journal of Security and Its Applications, 16(8), 135-145.
Discusses network security solutions for IoT, including IDS and IPS integration.

[5] Tariq, S., & Arshad, H. (2021). Securing IoT Devices with Lightweight Intrusion Prevention Systems. IEEE Transactions on Industrial Informatics, 17(4), 1542-1550.
Focuses on lightweight IPS models for IoT networks to minimize overhead.

[6] Espressif Systems (2023). ESP32 - A Complete Guide for IoT Projects. Retrieved from https://www.espressif.com/en/products/esp32
Official ESP32 documentation, detailing its use in IoT security applications.

[7] Zhang, Z., & Wang, L. (2019). Enhancing IoT Security with a Multi-layer Intrusion Detection System. Journal of Wireless Communication and Networking, 6(4), 212-220.
Proposes a multi-layer IDS for IoT security, integrating local and cloud detection layers.

[8] Sharma, P., & Mehta, S. (2020). A Study on the Use of Machine Learning for Intrusion Detection in IoT Networks. Journal of IoT Security, 3(1), 88-97.
Evaluates machine learning algorithms for detecting intrusions in IoT networks.