Guardian Network Monitor (GNM)

Mr.K.V. Siva Prasad Reddy[1], V.Aravinda Chary[2], Y. Anush Raj[3]
[1]*Computer Science & Engineering-Cyber Security & IOT, Malla Reddy University, Hyderabad, India.*
[2,3] *Computer Science & Engineering-Cyber Security, Malla Reddy University, Hyderabad, India.*

***Abstract* — The Guardian Network Monitor (GNM) is a versatile, Python-based solution designed to strengthen network security. It automates the scanning and identification of all connected devices, leveraging algorithms such as ARP scanning for device discovery and IP-MAC mapping to provide users with essential details like IP and MAC addresses, device names, and estimated bandwidth usage. These features allow for effective network management and give insights into how each device interacts with the network.**

The tool includes parental controls, enabling time-based access restrictions on specific devices through schedule-based filtering algorithms, which are particularly beneficial for families managing children's internet usage. Its advanced ARP spoofing detection algorithms monitor for unauthorized connections, using pattern recognition to identify anomalies and protect the network from potential intrusions.

Real-time email alerts, triggered by event-driven monitoring algorithms, notify users whenever new devices connect or suspicious activity is detected, empowering them to take swift action. Optimized for Linux systems, the Guardian Network Monitor integrates with iptables, applying rule-based access control algorithms to manage device access and provide robust security against vulnerabilities.

Keywords: **Network Security, Python-based, Device Discovery, ARP Scanning, IP-MAC Mapping, Bandwidth Usage, Parental Controls, Time-based Access Restrictions, Schedule-based Filtering, ARP Spoofing Detection.**

I. INTRODUCTION

The Guardian Network Monitor (GNM) is a powerful Python-based network security tool designed to enhance network visibility and protection. It automates device discovery using ARP scanning and IP-MAC mapping, providing detailed insights into connected devices, including IP addresses, MAC addresses, and bandwidth usage. The tool features parental controls, allowing time-based access restrictions through schedule-based filtering, making it ideal for families managing children's internet usage. Advanced ARP spoofing detection safeguards against unauthorized access by identifying suspicious network activity using pattern recognition algorithms. Real-time email alerts notify users of new device connections and potential intrusions, enabling proactive security measures. Optimized for Linux systems, GNM seamlessly integrates with iptables, leveraging rule-based access control for robust network defense. This tool provides enhanced security, network management, and threat detection, making it a valuable asset for both home and business environments.

II. LITERATURE SURVEY

Network security has become a crucial concern with the increasing number of cyber threats and unauthorized access attempts. Various network monitoring tools have been developed to enhance security, each employing different techniques for device discovery, intrusion detection, and access control. Traditional methods such as Wireshark provide deep packet inspection but lack automated detection of unauthorized devices. Nmap, a popular network scanner, helps in host discovery but does not include real-time alerts or parental controls.

Research on ARP scanning and IP-MAC mapping highlights their effectiveness in identifying devices on a network, allowing for efficient monitoring and bandwidth estimation. Studies on ARP spoofing detection emphasize the need for pattern recognition techniques to identify anomalies and prevent Man-in-the-Middle (MITM) attacks. Security frameworks like Snort implement intrusion detection but require extensive manual configuration, making them less accessible to general users.

Parental control mechanisms have been explored in various network security solutions, with schedule-based filtering algorithms proving effective in enforcing time-based access restrictions. Real-time event-driven monitoring has been widely studied, demonstrating its ability to provide instant notifications about unauthorized network activity.

The integration of iptables in Linux-based systems has been found to offer robust rule-based access control, enhancing overall security.

The Guardian Network Monitor (GNM) builds upon these existing technologies by combining automated device discovery, intrusion detection, parental controls, and real-time alerts into a single, user-friendly solution. By leveraging advanced algorithms for threat detection and access control, GNM provides a comprehensive approach to network security for both home and business users.

III. SYSTEM ANALYSIS

The Guardian Network Monitor (GNM) is designed to address network security challenges by automating device discovery, intrusion detection, and access control. Existing network monitoring tools often lack real-time alerts, parental controls, or efficient anomaly detection, making them less effective for home users. GNM overcomes these limitations by integrating ARP scanning and IP-MAC mapping to identify and monitor connected devices accurately.

The system employs schedule-based filtering algorithms to enforce time-based access restrictions, ensuring better control over network usage. Advanced ARP spoofing detection mechanisms analyze network traffic patterns to identify potential intrusions and unauthorized connections. Real-time event-driven monitoring enables instant email alerts, allowing users to take immediate action against threats.

Optimized for Linux environments, GNM integrates with iptables to implement rule-based access control, enhancing overall security. By combining multiple security features into a single tool, GNM provides a comprehensive and user-friendly network security solution for both personal and enterprise use.

Advantages of Guardian Network Monitor (GNM)

Guardian Network Monitor offers several key advantages that enhance network security and management. It automatically identifies all devices connected to the network through ARP scanning and IP-MAC mapping, providing comprehensive visibility of the network. This eliminates the need for manual tracking and ensures that all devices, including unauthorized ones, are monitored efficiently. The tool also enhances network security by detecting unauthorized connections and intrusions using advanced ARP spoofing detection and pattern recognition techniques, protecting against threats like Man-in-the-Middle (MITM) attacks.

A notable feature is the parental controls, which allow for time-based access restrictions using schedule-based filtering algorithms. This helps parents control internet access for their children, set usage limits, and block access during inappropriate times. Additionally, GNM provides real-time email alerts, notifying users whenever new devices connect or suspicious activities are detected, allowing for quick action to secure the network.

Optimized for Linux systems, GNM integrates seamlessly with iptables to implement rule-based access control, providing an added layer of protection by managing device access based on predefined rules. It also offers bandwidth monitoring, giving users insights into network usage per device and enabling them to optimize resource allocation to avoid congestion. The user-friendly interface ensures that even non-technical users can easily manage network security without specialized expertise.

Moreover, GNM's proactive threat detection through event-driven monitoring identifies and addresses potential threats before they escalate. Despite its advanced capabilities, it remains lightweight and efficient, consuming minimal system resources, which makes it ideal for both home networks and business environments. The tool is versatile, providing a comprehensive security solution suitable for managing small home networks or securing large-scale business infrastructures.

IV. METHODOLOGY

A. Architecture

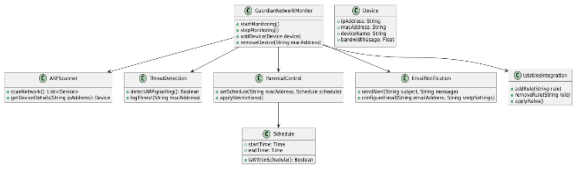

Figure 1: Architecture diagram

The architecture of the Guardian Network Monitor (GNM) is designed to offer an efficient, secure, and scalable network monitoring solution. It is based on several core modules, each responsible for different aspects of network management, security, and monitoring, and all of which work together seamlessly to provide a unified solution.

The Device Discovery Module is the foundation of the system. It uses ARP scanning and IP-MAC mapping techniques to detect all devices connected to the network. This module collects key information, such as IP addresses, MAC addresses, and device names, creating an inventory of active devices. The data collected is stored in a central database, making it easy to track and manage all devices in real time.

Next is the Intrusion Detection Module, which continuously monitors network traffic for any signs of suspicious or malicious activities, particularly unauthorized access or ARP spoofing attempts. Using pattern recognition algorithms, the system identifies anomalies and detects potential threats like Man-in-the-Middle (MITM) attacks. By scanning network traffic for unusual patterns, it ensures that any security breach is detected and addressed promptly.

The Parental Control Module focuses on providing time-based access restrictions for specific devices. By leveraging schedule-based filtering algorithms, it allows users to enforce internet usage policies, such as limiting online access during certain hours or blocking specific devices from connecting. This module is especially useful for families who need to manage their children's internet usage and ensure safer online experiences.

The Alerting and Notification Module works in conjunction with the intrusion detection and device discovery modules. It provides real-time email alerts whenever new devices connect or suspicious activities are detected. This event-driven monitoring system ensures that users are immediately informed about potential security risks, enabling quick responses to mitigate threats.

For controlling network access, the Access Control Module integrates with iptables on Linux systems to implement rule-based access controls. This module ensures that only authorized devices can connect to the network, enforcing access restrictions based on specific rules, such as IP or MAC addresses. By preventing unauthorized devices from gaining access, it strengthens overall network security.

The Bandwidth Monitoring Module allows users to monitor the network's bandwidth usage. It tracks the data consumption of each device connected to the network, helping users identify devices that are consuming excessive bandwidth. This information is crucial for optimizing network performance and ensuring that resources are allocated efficiently.

The User Interface Module is designed to be intuitive and user-friendly, allowing both technical and non-technical users to interact with the system. It presents all the collected data, security alerts, and device information in an easily readable format, making network monitoring and management accessible to everyone, regardless of technical expertise.

Finally, the Database Module stores all the data collected by GNM, including device information, security logs, bandwidth usage statistics, and user configurations. This centralized storage ensures that data is persistent and easily accessible for future reference, reporting, and analysis. The database also supports the generation of logs and reports to assist in effective network management.

Together, these modules form the backbone of the Guardian Network Monitor, creating a comprehensive, scalable, and modular system that ensures robust network security, efficient management, and effective monitoring.

B. Sequence Diagram

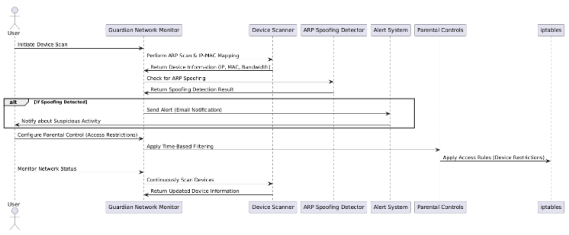

Figure 3: Sequence Diagram

The sequence diagram for the Guardian Network Monitor (GNM) illustrates the interactions between the user and various system components involved in network security monitoring and management.

The process begins when the User initiates a device scan through the Guardian Network Monitor (GNM). This prompts the Device Scanner to perform an ARP scan and generate a mapping of IP and MAC addresses for the connected devices. The scanner returns the relevant device information, such as IP, MAC addresses, and estimated bandwidth usage, to GNM.

Next, the Guardian Network Monitor sends the collected data to the ARP Spoofing Detector to check for any anomalies or unauthorized devices on the network. If any suspicious activity or ARP spoofing

is detected, the Alert System is triggered. The Alert System immediately sends an email notification to the User, informing them of the potential intrusion or abnormal behavior.

Simultaneously, the User may configure Parental Controls through the GNM interface, specifying time-based access restrictions on particular devices. The Parental Controls module applies these restrictions and communicates with iptables to enforce access rules on the devices, ensuring that only authorized users can access the network during the specified times.

In essence, the sequence diagram outlines how the components work together: the User interacts with the system to initiate scans and configure controls, the Device Scanner collects data, the ARP Spoofing Detector checks for security threats, the Alert System notifies the User of potential issues, and the Parental Controls manage device access with iptables enforcing security policies. The system continuously monitors the network, ensuring real-time protection against potential intrusions or unauthorized device access.

C. Activity Diagram

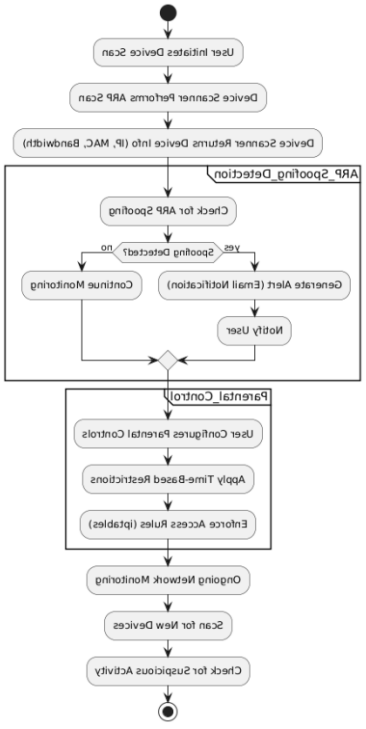

Figure 2: Activity Diagram

The Activity Diagram for the Guardian Network Monitor (GNM) represents the flow of actions that occur during network monitoring, device management, parental control configuration, and security checks.

The process begins when the User triggers a network scan through the Guardian Network Monitor (GNM). This action initiates the Device Scanner to perform ARP scanning, which discovers devices connected to the network. The system then gathers information such as device names, IP addresses, MAC addresses, and bandwidth usage.

Once the device scan is completed, the system checks for potential ARP spoofing attacks. If the ARP Spoofing Detector identifies suspicious activity or an unauthorized device, the system moves to the alerting phase. If no anomalies are detected, the system will continue monitoring the network.

If the system detects any unauthorized devices or ARP spoofing, the Alert System generates a real-time email alert to notify the User. The User is then informed of potential threats, and they may choose to take action to secure the network further.

In parallel, the User can configure Parental Controls through the GNM interface, setting time-based restrictions for specific devices. The system applies these settings and communicates with iptables to implement access control based on the defined schedules.

Iptables enforces the rules set by the Parental Controls, ensuring that devices can only access the network during allowed timeframes. Once the parental controls are set, the system continues to monitor the network, periodically scanning for new or modified devices.

The network is continuously monitored for new devices, changes in device status, or potential security threats. The system executes periodic scans and checks, providing constant oversight of the network's security status. If new devices are detected or if suspicious activity occurs, the appropriate actions are taken, such as alerting the user or updating security settings.

D. Process

I. Modules

Device Scanner (ARP Scanning Module): This module is responsible for detecting and mapping all devices connected to the network using ARP scanning. It retrieves essential information such as IP

addresses, MAC addresses, and estimated bandwidth usage, allowing administrators to have a clear overview of the network's connected devices.

ARP Spoofing Detector: The ARP Spoofing Detector monitors the network for any ARP spoofing attacks. It checks for discrepancies in ARP traffic and identifies unauthorized devices attempting to impersonate legitimate ones. This module helps protect the network from data interception or manipulation.

Alert System: The Alert System generates real-time notifications whenever critical events occur, such as detecting new devices or suspicious activity like ARP spoofing. These alerts are typically sent through email or SMS to notify the user immediately, empowering them to take quick actions if needed.

Parental Controls Module: This module allows users to configure time-based access restrictions for specific devices on the network. It helps in managing internet usage for children or specific devices by enabling access only during predefined times, thereby improving network control and safety.

Firewall Integration (iptables): This module integrates with the Linux-based firewall tool, iptables, to enforce access control rules on the network. It applies filtering policies based on user-configured rules, ensuring that only authorized devices can access the network and preventing unauthorized access.

Network Monitoring & Management Interface: This module provides a user interface for managing and configuring the Guardian Network Monitor. It allows users to initiate device scans, configure parental controls, view real-time network status, and receive alerts. The interface can be command-line or graphical, depending on the system configuration.

Continuous Monitoring & Scheduling Module: This module ensures the system runs continuous scans and checks for new devices or unusual activities. It automates regular network scans and updates, maintaining a proactive security posture by scheduling tasks and monitoring network status in real-time.

Log Management & Reporting: This module tracks and stores logs of all network activities, security alerts, and user actions. It helps in auditing the network and generating detailed reports to analyze network performance, security events, and the overall health of the network.

Machine Learning/Anomaly Detection (Optional): This module uses machine learning algorithms to detect anomalies in the network, such as unusual patterns in device behavior or traffic. It helps in identifying hidden threats or vulnerabilities that may not be immediately apparent through traditional detection methods.

V. RESULTS

Figure 1: Dashboard Page

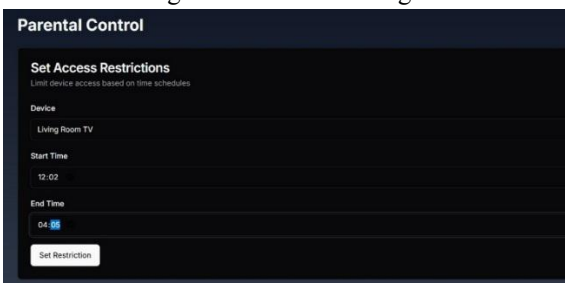

Figure 2: Parental Control Page

Figure 3: Alert Page.

Figure 4 : Settings page

III. CONCLUSION

The Guardian Network Monitor (GNM) provides a comprehensive, automated solution for network security and management. By leveraging advanced algorithms such as ARP scanning, IP-MAC mapping, and anomaly detection, it enables users to effectively monitor network activity, detect unauthorized devices, and mitigate potential security threats like ARP spoofing. The inclusion of parental control features allows for customizable, time-based device access restrictions, providing an added layer of control for families managing children's internet usage.

The integration with iptables ensures that access policies are enforced with robust firewall protection, while the alert system promptly notifies users of any suspicious activity or new device connections, enabling quick response actions. Additionally, the continuous monitoring feature ensures that the network remains secure at all times, detecting threats in real time.

The modular design of GNM, coupled with features like machine learning-based anomaly detection and log management, makes it a versatile and scalable solution for network administrators and home users alike. It offers both proactive security and convenient network management, ensuring a safe and well-monitored network environment.

IV. FUTURE SCOPE

The Guardian Network Monitor (GNM) has significant potential for future enhancements and expansions, which can further strengthen its capabilities in network security and management.

One key area for future scope is AI-driven threat detection, where integrating advanced artificial intelligence and machine learning models could improve threat detection accuracy. The system could learn from network traffic patterns and identify potential threats that may not be detectable by traditional methods, such as zero-day vulnerabilities or subtle data exfiltration attempts.

Another area is the integration with IoT devices, as the number of Internet of Things (IoT) devices continues to grow. GNM could be enhanced to specifically monitor IoT device security, detecting vulnerabilities unique to these devices and enforcing stricter security policies to prevent exploitation.

The device classification feature could also be expanded to include more granular classifications, such as detecting device types (e.g., smart TVs, cameras, etc.) and categorizing them for tailored monitoring or control policies.

Additionally, cloud integration and remote management could provide centralized network management across multiple locations. Cloud integration would also enable real-time monitoring from anywhere, allowing users to manage devices remotely using a web or mobile application.

Incorporating real-time bandwidth analysis would allow GNM to offer detailed insights into traffic patterns and usage, helping network administrators manage congestion, allocate bandwidth more efficiently, and detect bandwidth-hogging devices or suspicious activity.

The parental control features could be enhanced with content filtering, usage reporting, and more dynamic time-based restrictions, such as restrictions based on device activity or app usage, providing parents with more granular control over their children’s internet experience.

For enterprise-level security, GNM could be integrated with SIEM systems to contribute findings to a larger security infrastructure, providing more context for overall security operations and improving decision-making.

A more advanced feature could be the use of blockchain-based technologies for decentralized network security, offering enhanced transparency, data integrity, and user control over security data.

Finally, automated threat remediation could be introduced, where the system takes real-time remedial actions such as isolating compromised devices, updating firewall rules, or blocking malicious IPs when a threat is detected.

By exploring these avenues for improvement, Guardian Network Monitor can evolve into an even more sophisticated, comprehensive tool for network management and security, providing users with proactive and intelligent solutions for maintaining a secure network environment.

REFERENCES

[1] Here are some possible references related to the Guardian Network Monitor (GNM), which covers concepts and technologies discussed in the abstract:

[2] Scapy Documentation: Scapy is a powerful Python-based interactive packet manipulation tool that allows for ARP scanning and network

monitoring. It's frequently used for security assessments and network discovery.

[3] *Scapy: A Packet Manipulation Tool for Python*. https://scapy.readthedocs.io/en/latest/

[4] Python iptables Module: The iptables module allows interaction with the Linux firewall for managing network security and enforcing access rules. It's commonly used in server security and network administration.

[5] *Iptables Python Bindings*. https://github.com/axitil/iptables

[6] ARP Spoofing and Security Threats: ARP spoofing is a network attack where a malicious actor sends fake ARP messages to intercept network traffic. Understanding this threat is crucial for developing detection systems.

[7] *Understanding ARP Spoofing and How to Prevent It*. https://www.imperva.com/learn/application-security/arp-spoofing/

[8] Machine Learning for Network Anomaly Detection: Machine learning can be used to detect network anomalies and security breaches, providing intelligent threat detection capabilities.

[9] *A Survey of Machine Learning Algorithms for Network Intrusion Detection Systems*. https://arxiv.org/pdf/1910.06422.pdf

[10] Parental Control and Time-based Filtering: Parental control tools help regulate internet access for children and ensure safe online behavior. These systems often include time-based filtering mechanisms.

[11] *How Parental Control Works and Best Tools for Internet Safety*. https://www.kaspersky.com/resource-center/preemptive-safety/parental-control

[12] Linux Networking and Firewall Tools: Iptables is one of the most widely used firewall utilities on Linux. It helps to secure systems by applying custom rules to control the flow of network traffic.

[13] *Linux Iptables Firewall Configuration Guide*. https://www.digitalocean.com/community/tutorials/how-to-set-up-a-basic-firewall-with-iptables-on-ubuntu-20-04

[14] Real-time Network Monitoring: Real-time network monitoring tools allow administrators to visualize and track device activities, bandwidth usage, and traffic patterns on a network.

[15] *Best Network Monitoring Tools for 2025*. https://www.networkworld.com/article/3324969/the-best-network-monitoring-tools.html

[16] SIEM Integration for Network Security: Security Information and Event Management (SIEM) tools help aggregate and analyze security logs to improve incident detection and response.

[17] *What is SIEM? A Beginner's Guide to Security Information and Event Management*. https://www.varonis.com/blog/siem

[18] Blockchain for Network Security: Blockchain technology can enhance network security by decentralizing control, increasing transparency, and providing a more secure infrastructure.

[19] *Blockchain for Network Security: Opportunities and Challenges*. https://www.sans.org/reading-room/whitepapers/blockchain/blockchain-network-security-opportunities-challenges-38585

[20] Automated Threat Response Systems: Systems that automatically respond to threats help reduce the time between detection and remediation, minimizing potential damage to the network.

[21] *Automation and Orchestration in Cybersecurity: A Guide to Automated Incident Response*. https://www.csoonline.com/article/3259067/what-is-automation-and-orchestration-in-cybersecurity.html