ISSN: 2582 - 6379
IJISEA Publications
International Journal for Interdisciplinary Sciences and Engineering Applications
IJISEA - An International Peer- Reviewed Journal
2026, Volume 7 Issue 2
www.ijisea.org

Real-Time Network Security Monitoring and Auto Mitigating Firewall System Using Python and IP Tables

[1]K. Karthik, [2]K. Lokesh, [3]K. Naidu, [4]K. Geethasri, [5]K. Krishna
[1,2,3,4,5] B. Tech CSE Students, Dept. of CSE, Sir C R Reddy College of Engineering, Eluru.

ABSTRACT

As the internet-based services and online communication grow at an alarming pace, computer networks are becoming more susceptible to cybercrime, including Distributed Denial-of-Service (DDoS) attacks, unauthorized access attempts, and traffic surges. The conventional network security systems are majorly based on the use of fixed firewall settings and manual monitoring systems that tend to lead to a sluggish reaction to the changing threats. Consequently, companies need automated security systems that can identify and respond to malicious actions on a real-time basis. This study introduces the design/implementation of a Real-Time Network Security Monitoring and Auto-Mitigating Firewall System with Python and IPTables. The system is able to constantly scan network traffic, examine packet behavior, and automatically create firewall rules to block suspecting IP addresses without the intervention of the administrator. The developed solution has a low latency, low resources consumption, and stable operation in simulated attack conditions. The system offers an efficient and cost-effective solution to secure network within contemporary computing environment.
KEYWORDS: Network Security, Firewall Automation, IP Tables, Python, Real-Time Monitoring, Intrusion Detection, Cybersecurity

I. INTRODUCTION

The development of networked systems and the internet connection has had profound changes on how organizations deal with communication, data storage and online services. Even though these developments have enhanced productivity and accessibility, there is a greater risk of cyber threat to network infrastructure. Network systems are often vulnerable to attacks where attackers can use these vulnerabilities to disrupt the services, steal data or even gain unauthorized access to sensitive information.

The outdated security systems like the use of fixed firewalls and manual surveillance programs are no longer adequate to deal with the contemporary cyber threats. Such systems need human intervention to interpret logs and update firewall rules, adding delays between threat detection and mitigation. In this delay, attackers can cause serious harm to the network resources or destroy the integrity of the system.

To overcome these challenges, automated network security systems have been designed to inspect network traffic in real time and take action on threat in real time. The system suggested is a combination of real-time traffic monitoring, detection of threats, and automated firewall management. Using Python scripting and IPTables firewall mechanism, the system offers real-time security of the network against malicious network activity and efficient system performance.

II. RELATED WORK

The use of automated intrusion detection and firewall management systems to improve network security has been the subject of several studies. Snort and Suricata are signature-based intrusion detection systems, popular in identifying known attack patterns. These systems scan network packets and produce alerts in case

ISSN: 2582 - 6379
IJISEA Publications
International Journal for Interdisciplinary Sciences and Engineering Applications
IJISEA - An International Peer- Reviewed Journal
2026, Volume 7 Issue 2
www.ijisea.org

suspicious behavior is detected. They usually, however, use a set of signatures and they might not identify new or novel attack techniques.

Fail2Ban and other log-based security tools track system logs, and block IP addresses when they fail to log in multiple times. Although they are useful in preventing brute force attacks, such tools work mainly at the application level and they may be unable to detect network level threats in real time.

In recent studies, there has been interest in integrating traffic analysis with automated rule generation in firewalls to enhance response time and minimize human intervention. The security solutions written in Python have become more popular because of their flexibility, simplicity to develop and compatibility with network monitoring libraries. Although these have been developed, most of the current systems demand costly hardware or complicated infrastructure, which is restricting their implementation in resource-limited contexts.

The proposed system will be able to provide solutions to these limitations by offering a lightweight, low cost system that can run on Linux based systems and use the inherent firewall capabilities.

III. EXISTING SYSTEM

Current network security systems are often based on fixed firewall settings, and manualized log watch to identify potential threats. They are basic security measures that prevent unauthorized access but cannot dynamically react to the quickly evolving patterns of attacks. In most instances, administrators have to go through system logs manually and update firewall rules, which may take time to respond to security incidents. The other weakness of traditional systems is that they relied on fixed security policies that fail to automatically adapt to emerging threats. With the growing volume and complexity of network traffic, manual monitoring is inefficient and subject to human error. Also, commercial security systems can be expensive in terms of special hardware and licensing fees, not fitting the small organization or school.

These shortcomings underscore the necessity of an automated network security tool that can identify the presence of suspicious activity and implement security measures, without human intervention.

IV. PROPOSED SYSTEM

The suggested system is a Real-Time Network Security Monitoring and Auto-Mitigating Firewall System to identify and prevent malicious network traffic automatically. The system constantly monitors the network packets and compares the traffic characteristics to detect any abnormal behaviour like repeated connection attempts, high packet rate or suspicious protocol activity.

After a potential threat is identified, the system then creates firewall rules in real-time using IPTables in an attempt to block the offending IP address. The automated mitigation facility can be relied upon to prevent attacks as they occur, and minimize the chances of service disruption or loss of data integrity. Detailed logs of threats and mitigation measures detected by the system are also recorded allowing administrators to view network activity and analyse security incidents.

The proposed system is based on a modular architecture where individual components can be independent, which enhances the scalability and maintainability of the system. The system is compatible with different network security applications and can be deployed on personal computers or server or even a cloud based environment.

ISSN: 2582 - 6379
IJISEA Publications
International Journal for Interdisciplinary Sciences and Engineering Applications
IJISEA - An International Peer- Reviewed Journal
2026, Volume 7 Issue 2
www.ijisea.org

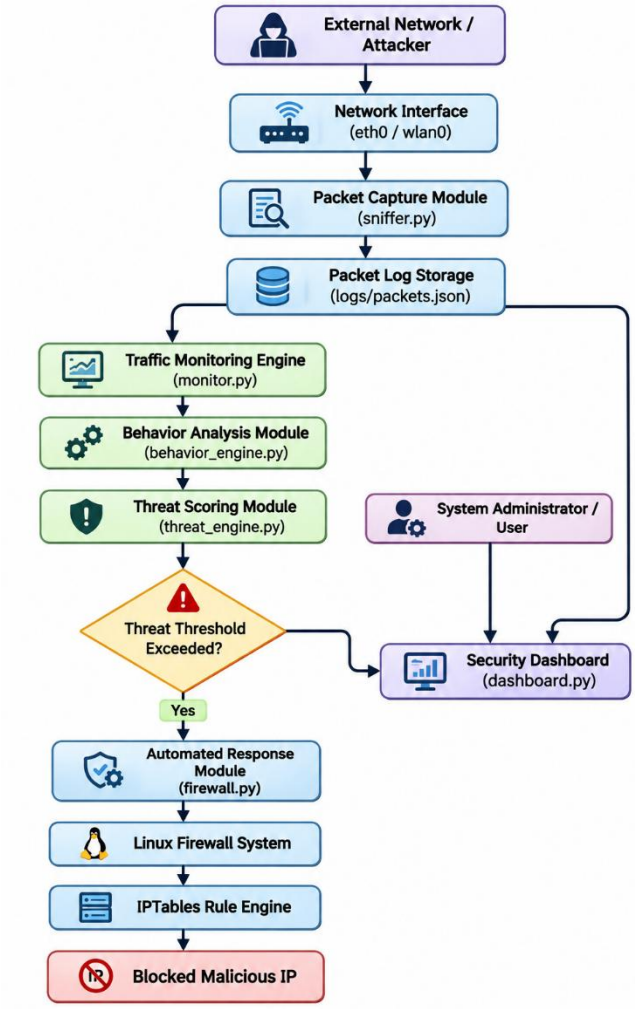


Fig 1: System Architecture of the Real-Time Network Security Monitoring System

The system architecture consists of a number of inter-linked modules, which work together to monitor network traffic and implement security policies. The Network Traffic Monitoring Module captures and logs packets sent or received over the network interface and captures critical details like the source IP address, destination IP address, protocol type, packet size and the time stamp. This data is logged in log files to be analyzed. Threat Detection Module processes the recorded traffic information that is used to analyze the packet behavior and compare the traffic patterns with predefined thresholds to detect suspicious or abnormal traffic. The system categorizes traffic into normal, suspicious, and attack-like traffic depending on the protocol features and frequency of packets.

In the case of abnormal behavior being identified, the Automated Mitigation Module activates the firewall mechanism to block the malicious source IP address. Firewall Module implements security policies based on IPTables firewall system to block additional rogue traffic to the network.

Lastly, the Logging and Reporting Module logs suspected threats and mitigation measures to log files, and displays real-time alerts and traffic data on a monitoring dashboard. Such logs will be audited, analyzed, and utilized later in incident response.

ISSN: 2582 - 6379
IJISEA Publications
International Journal for Interdisciplinary Sciences and Engineering Applications
IJISEA - An International Peer- Reviewed Journal
2026, Volume 7 Issue 2
www.ijisea.org

4.1 Methodology:
The Real-Time Network Security Monitoring and Auto-Mitigating Firewall System proposed is structured in a workflow that aims at providing efficient detection and mitigation of network threats. The methodology is divided into several stages that collaborate in ensuring continuous monitoring, proper threat detection, and automated action. Each stage has a certain task in the general security process to provide reliable and real-time security of the network infrastructure.

A. Data Collection
The initial stage of the methodology is the live network traffic data gathering of the network interface of the system. The monitoring module constantly monitors the packets that have been received and sent through packet sniffing. Some of the key packet data captured comprise the source IP address, destination IP address, protocol type, packet size and timestamp.

This step will provide the system with real time visibility into network activity so that abnormal behaviour can be detected immediately it is initiated.

B. Traffic Preprocessing
This stage involves processing and formatting the data taken off the network into a form that can be analyzed. The system screens out extraneous information and isolates pertinent packet attributes that are needed to identify threats. Statistical parameters like packet rate, connection frequency, and protocol distribution are estimated to develop a baseline of normal network operation.

This initial processing step enhances the accuracy of detection since only meaningful data is processed by the threat detection engine.

C. Threat Detection
Threat detection stage is in charge of detecting suspicious network traffic. The system will compare actual traffic statistics with the pre-programmed thresholds to identify the abnormal behavior. Such suspicious behaviors as an unusually large number of connection attempts by a single IP address, a high rate of packet transmission, and repeated failed attempts to communicate are examples of suspicious activity.

When the system identifies traffic patterns that are above the established thresholds, the relevant source IP address is defined as a possible threat. This stage guarantees that malicious activity is quickly detected and that there are fewer false positives.

D. Automated Mitigation
When a threat is established, the automated mitigation phase automatically acts to secure the network. The system is a dynamically generated system that creates firewall rules based on the IPTables framework in order to block or restrict traffic by the malicious IP address. It also has the advantage of automatic deployment of the mitigation process in response to security incidents without needing the intervention of the administrators, thereby responding quickly.

This step saves a lot of time between the detection of threats and mitigation, as the attackers will not be able to cause more damage to the network.

E. Recording and Reporting
The last step of the approach is to document all threats and mitigation measures identified. The system creates detailed log entries that include data on the timestamp, source IP address, type of attack, and firewall rule

ISSN: 2582 - 6379
IJISEA Publications
International Journal for Interdisciplinary Sciences and Engineering Applications
IJISEA - An International Peer- Reviewed Journal
2026, Volume 7 Issue 2
www.ijisea.org

utilized. These logs are very useful in analyzing the activity on the network and in assisting future analysis, troubleshooting and security audits.

The logging mechanism guarantees transparency and accountability in the functioning of the system as well as allowing administrators to monitor the overall network security performance.

4.2 Algorithm: Automated Network Threat Detection and Mitigation

Step 1: Start the network monitoring system.
Step 2: Intercept traffic in and out of the network interface.
Step 3: Get the packet attributes like the source IP address, destination IP address, protocol type, and packet size.\
Step 4: Compute traffic measures, such as packet rate and connection frequency.
Step 5: Compare the statistics calculated to some pre-determined threshold values.
Step 6: When the traffic value is lower than the threshold, then it is a normal traffic and proceed with monitoring.
Step 7: When the value of traffic is greater than the threshold then the source IP address will be classified as suspicious.
Step 8: Check the suspicious IP address with whitelist to avoid blocking trusted users.
Step 9: Create an IPTables firewall rule that will block or rate-limit the suspicious IP address.
Step 10: Dynamically apply the firewall rule to the system firewall.
Step 11: Log the detection of the event and the mitigation action into the system log.
Step 12: Keep on watching network traffic.
Step 13: End.

4.3 Implementation Architecture:

The system implementation algorithm determines the order of actions carried out to trace network traffic, identify an abnormal behavior, and automatically perform mitigation of possible security threats. The flow starts at the Packet Capture Module that constantly scans the network interface and records the packets going in and going out. Every packet that is captured is processed to extract pertinent attributes including; source IP address, destination IP address, protocol type, packet length and timestamp. This data is recorded in structured log files to be analysed further.

The Traffic Monitoring Module then reads the packet data stored and measures traffic patterns over a specified time frame. The system keeps a log of the number of packets sent by each source IP address and the comparison of the observed traffic rate with preset threshold values. When the packets of a certain IP address surpass the limit during a given period of time, the traffic is marked as abnormal, and it is analyzed. Behavior Classification Module then processes the packet characteristics to identify the type of traffic. Depending on the conditions that are based on rules, the system classifies traffic as a Normal, Suspicious, or Attack-like. As an example, ICMP packets, or abnormally small UDP packets can be considered suspicious, and unusually large packets or a high-frequency pattern of traffic can be recognized as attack-like behavior. After classifying the behavior, the Threat Scoring Module computes a numerical threat score of each source IP address. The system will place weight values on the various categories of behaviors and will add the weight values over time to identify the severity of the threat that may exist. When the risk score is computed to be higher than a predetermined threshold, the system will see the traffic as malicious activity that needs to be dealt with at once.

When malicious traffic is detected, the Automated Mitigation Module triggers a response, which calls the firewall control mechanism. The system will dynamically produce firewall rules to block the hit malicious IP address with the help of a packet filtering system of the operating system. This will stop any additional

ISSN: 2582 - 6379
IJISEA Publications
International Journal for Interdisciplinary Sciences and Engineering Applications
IJISEA - An International Peer- Reviewed Journal
2026, Volume 7 Issue 2
www.ijisea.org

destructive traffic that may be introduced into the network and guard against any possible attacks to the system resources.

Lastly, the Logging and Reporting Module logs all threats identified, system responses and mitigation measures in special log files. These logs are presented as a monitoring dashboard so that administrators can monitor network activity, security alerts, and analyze past events to use later. The whole process is a real time continuous operation that ensures that threats in the network are proactively detected and prevented.

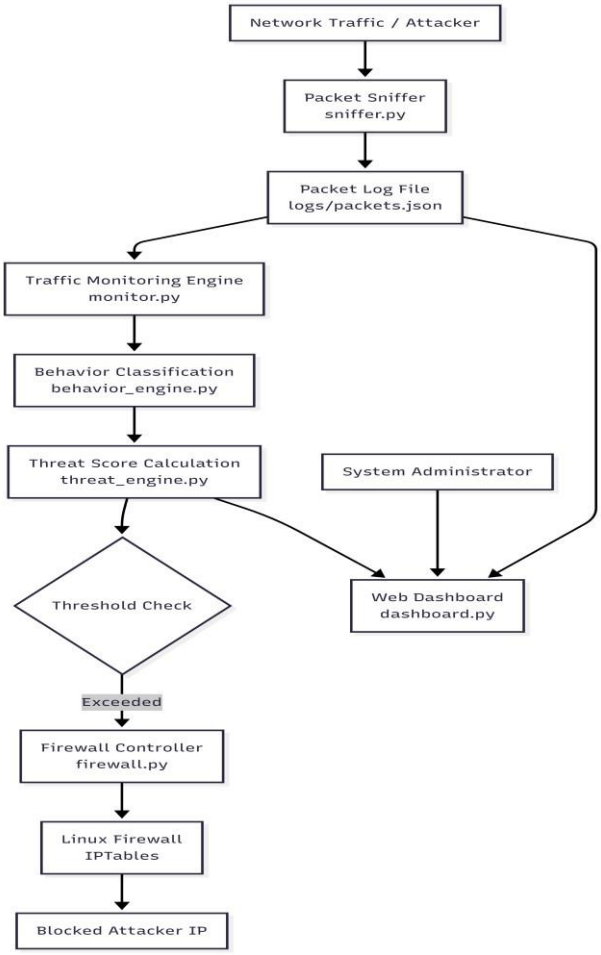


Fig. 2. Detailed implementation architecture illustrating real-time packet capture, traffic analysis, threat scoring, automated firewall mitigation, and security monitoring dashboard communication.

4.4 Sequence Diagram (Network Security Monitoring and Auto-Mitigating Firewall System):
The sequence diagram is the flow of interaction among the system components when monitoring the network and averting threats. The monitoring module captures and analyzes network packets, and the detection engine analyzes them. In case of normal traffic, the monitoring process goes on as usual. In case a malicious activity is detected, the mitigation module creates a firewall rule with the use of IPTables to prevent the attacker. This rule is applied immediately by the firewall and the logging module logs the mitigation. This chain guarantees automated and real time protection against network attacks.

ISSN: 2582 - 6379
IJISEA Publications
International Journal for Interdisciplinary Sciences and Engineering Applications
IJISEA - An International Peer- Reviewed Journal
2026, Volume 7 Issue 2
www.ijisea.org

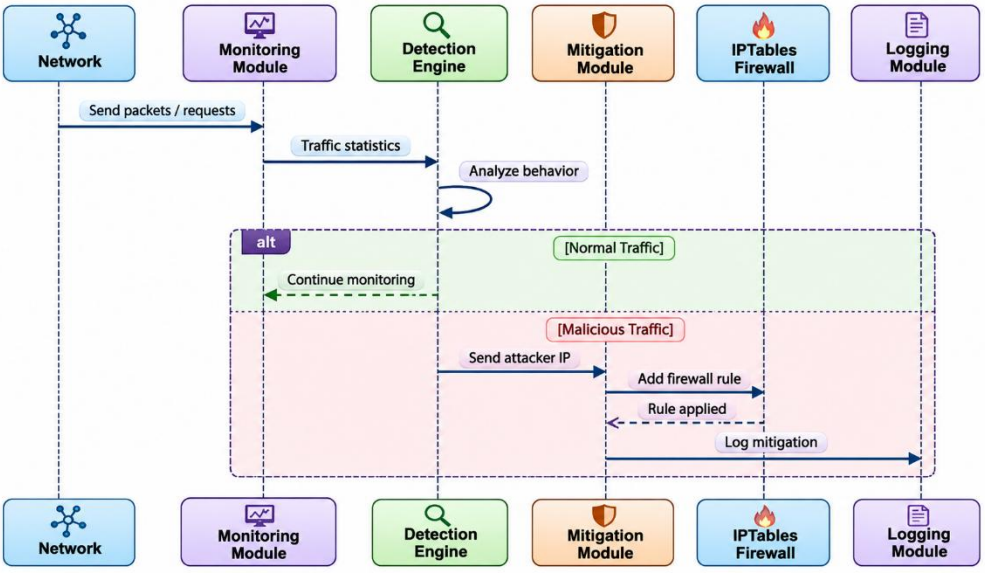


Fig. 3. System response sequence diagram demonstrating packet monitoring, behavior analysis, threat detection, firewall rule enforcement, and security event logging during network attack mitigation.

V. RESULTS & DISCUSSIONS

5.1 System Testing Overview

The proposed Real-time Network Security Monitoring and Auto-Mitigating Firewall System has been implemented and tested to test functionality, reliability and performance of the system in various conditions of the network. The testing procedure involved ensuring that the system can identify suspicious network operations, automatically create firewall rules and can maintain consistent performance throughout high availability.

The system was installed on a Linux-based platform and was linked to a simulated network whereby the normal and malicious traffic conditions were simulated using network testing tools. Real-time packet monitoring, threat detection accuracy, and automated mitigation response were evaluated using the testing environment.

The findings confirmed that the system was able to monitor network traffic, identify abnormal behavior, and block malicious IP addresses without the need to be manually handled. The system was stable during the test phase and tested to be reliable when operating with different network loads.

ISSN: 2582 - 6379
IJISEA Publications
International Journal for Interdisciplinary Sciences and Engineering Applications
IJISEA - An International Peer- Reviewed Journal
2026, Volume 7 Issue 2
www.ijisea.org

5.2 Live Traffic Monitoring Interface Result

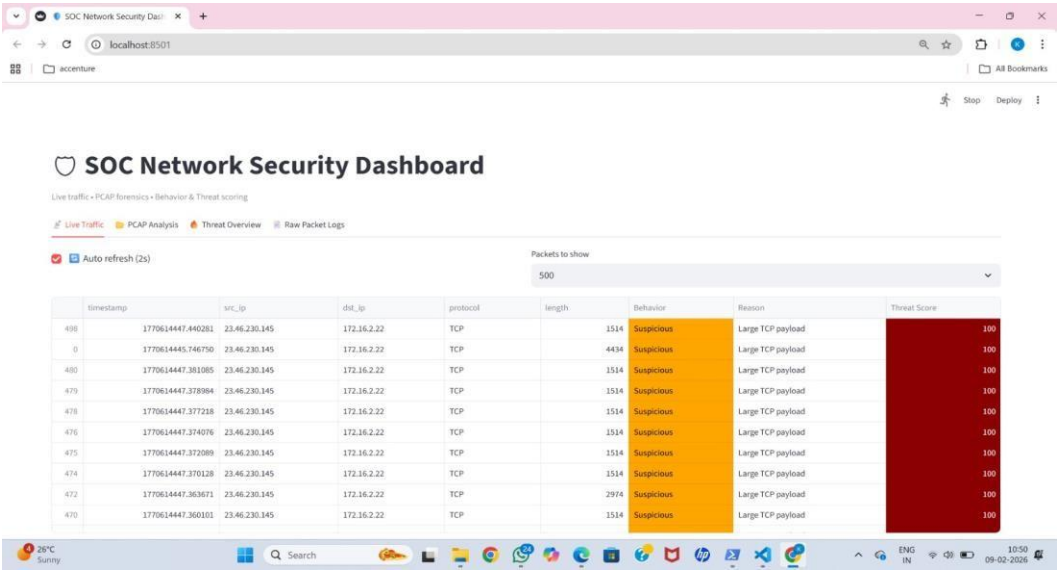


Fig. 4. Live Traffic Monitoring Dashboard Displaying Real-Time Network Activity

The system has a real-time dashboard interface as illustrated in Figure 4, which reports detailed information regarding network traffic measured by the monitoring module. The interface contains information on source IP address, destination IP address, protocol type, packet length and traffic classification status.

The dashboard will allow administrators to monitor network behavior in real-time and detect suspect activity promptly. The graphical view of real-time traffic data enhances situational awareness and makes it easier to make faster decisions regarding network security management.

5.3 Packet Analysis Overview Result

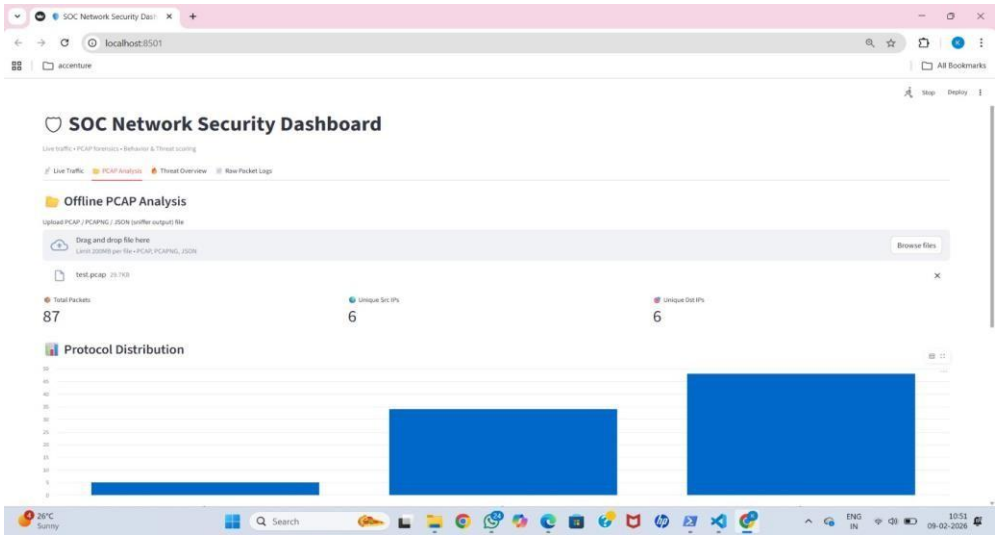


Fig. 5. Packet Analysis Overview Showing Traffic Statistics and Protocol Distribution

ISSN: 2582 - 6379
IJISEA Publications
International Journal for Interdisciplinary Sciences and Engineering Applications
IJISEA - An International Peer- Reviewed Journal
2026, Volume 7 Issue 2
www.ijisea.org

Figure 5 shows the overview of the packet analysis created by the system. This interface gives a summary of the network traffic statistics, such as the total packets captured, distinct source and destination IP addresses, and a breakdown of the different communication protocols used, such as TCP, UDP and ICMP.
The packet analysis overview can guide administrators in knowing the general patterns of network activities and detecting the abnormal traffic patterns. Real time traffic statistics analysis improves the system in identifying possible security threats at an early stage before they become serious.

5.4 System Performance and Functionality

The system was able to execute the main functionalities of garment selection, visualization, and virtual try-on simulation. The augmented reality component was able to show the chosen piece of clothing on the display interface without major delays. The user experience was responsive to user input, and the try-on experience was real time. These findings suggest that the given system can offer an interactive and effective virtual shopping experience.

5.5 Detailed Packet Inspection Result

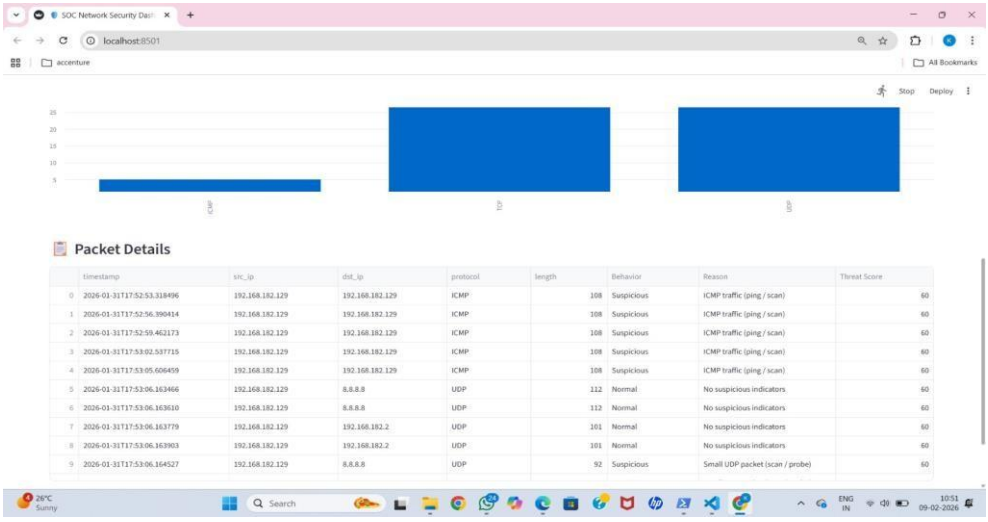


Figure 6: Detailed Packet Inspection Displaying Suspicious Traffic Behavior

Figure 6 shows the packet inspection view with a detailed view given by the monitoring system. This interface provides detailed data related to the individual network packets such as the timestamp, source IP address, destination IP address, protocol type, packet size and the reason of detection. The detailed inspection option allows administrators to examine suspicious traffic logs and establish the reason why the network was acting abnormally. This would be critical in detecting patterns of attacks and enhancing the security policies of the system.

ISSN: 2582 - 6379
IJISEA Publications
International Journal for Interdisciplinary Sciences and Engineering Applications
IJISEA - An International Peer- Reviewed Journal
2026, Volume 7 Issue 2
www.ijisea.org

5.6 Raw Packet Logs Result

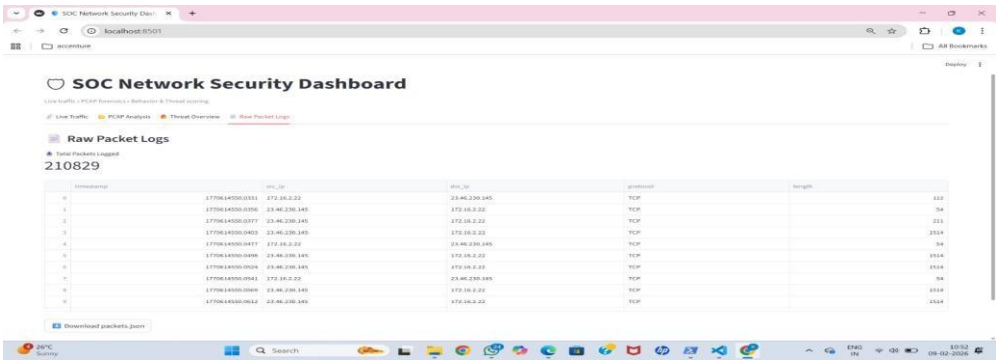


Figure 4: Raw Packet Logs Generated by the Monitoring System

The results of the network monitoring in terms of raw packet logs can be seen in Figure 4. These logs have chronological logs of packets and system events captured, such as detection alerts and firewall events.
The logging system is used to track network activity accurately and to find useful data to make troubleshoot and forensic analysis. Access to detailed logs enhance transparency in the system and facilitate incident response.

5.7 Top Threat Actors Result

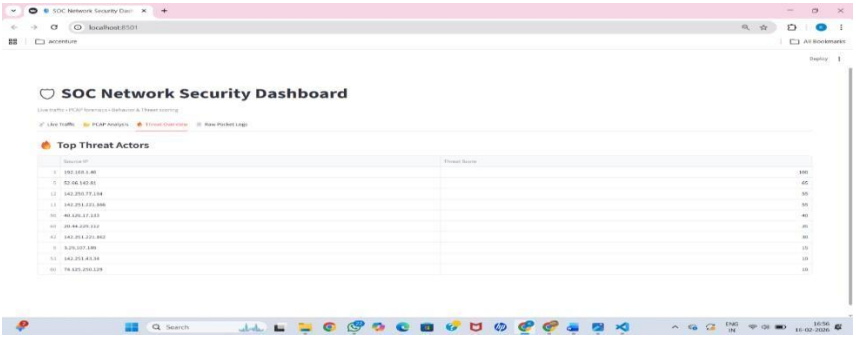


Figure 5: Top Threat Actors Ranked Based on Threat Score

The list of the leading threat actors detected by the system is shown in Figure 5. The interface prioritizes IP addresses according to the amount of suspicious activities that have been identified and gives a threat score to each source.

This ranking system assists administrators to receive top priority on security measures and concentrate on the most severe threats. The system helps to strengthen the network defense strategies by detecting high-risk sources promptly.

5.8 Performance Comparison Table:

Type	Representative Systems	Strengths	Limitations
Packet firewall	IPTables, nftables	Kernel speed, fine-grained control	Rule scale, rule management
IDS/IPS	Snort, Suricata	Known-signature detection	New/unknown attacks missed

ISSN: 2582 - 6379
IJISEA Publications
International Journal for Interdisciplinary Sciences and Engineering Applications
IJISEA - An International Peer- Reviewed Journal
2026, Volume 7 Issue 2
www.ijisea.org

Behavior-based ML	Research detectors	Novel attack detection	Requires baseline + retraining
Host auto-bans	fail2ban, OSSEC	Simple, effective for brute-force	Limited feature set
Cloud mitigation	Cloudflare, AWS Shield	Absorb volumetric attacks	Cost, vendor dependency
SIEM / SOAR	Splunk, QRadar	Central correlation, playbooks	Latency; not first-line mitigation

The table below shows the strengths and weaknesses of the available network security solutions against the proposed automated firewall system. All security mechanism types have a designated purpose in safeguarding network infrastructure, but they vary greatly in their ability to detect, respond to, function at scale, and complexity.

Packet-level firewalls, including IPTables and nftables, offer high-performance packet filtering on the kernel level and enable a fine-tuning of network traffic. Such systems are effective in implementing security policies and preventing unwarranted connections. Nevertheless, they might not perform well in the presence of a large number of dynamic rules and managing rules by hand may become complicated in large-scale network environments.

ids/IPS: IDS/IPS tools like Snort and Suricata are popular in the process of detecting known attack patterns using signature-based methods of detection. These systems provide a good chance of detection of threats that have been previously identified but cannot detect new or unknown types of attacks unless its signatures are updated. Due to that, they need constant maintenance and updating of rules to ensure that they are effective. Machine learning detection systems that operate based on behaviors offer the ability to detect new or unfamiliar patterns of attacks through deviation analysis of network behavior. Even though these systems enhance accuracy in detection, they need a lot of training data and occasional retraining to sustain the performance. Also, machine learning models can add increased computational complexity over conventional detection algorithms.

Host-based automatic banning systems like fail2ban and OSSEC provide an easy and efficient solution to prevent repeated unauthorized access attempts, especially when it comes to brute-force login attacks. These can be used to keep track of system logs and automatically enforce temporary firewall rules whenever suspicious activity is detected. Yet, they are usually confined to a set of attack types and might not be able to deliver protection against sophisticated network threats.

Mitigation services that are available on the cloud such as Cloudflare and AWS Shield offer volumetric protection of large scale by blocking malicious traffic before its entry to the target network. These services are very reliable and scalable and are usually characterized by repetitive operational expenses and reliance upon third-party providers. When using external mitigation services, organizations might also lose a sense of control with network security policies.

Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) Splunk and QRadar have a centralized log management, event correlation, and automated response processes. These systems enhance visibility and coordination of various security elements but are not usually designed to offer first-line mitigation because processing latency exists.

ISSN: 2582 - 6379
IJISEA Publications
International Journal for Interdisciplinary Sciences and Engineering Applications
IJISEA - An International Peer- Reviewed Journal
2026, Volume 7 Issue 2
www.ijisea.org

On the whole, the comparison indicates that current security mechanisms are useful to offer essential security in particular settings, yet they tend to be manually configured, necessitate extra infrastructure, or expert knowledge. The proposed Real-Time Network Security Monitoring and AutoMitigating Firewall System overcomes these constraints by integrating real time monitoring of traffic, automated threat detection and dynamically generated firewall rules into a single lightweight architecture. This integration will increase the speed of the response, lessen operational complexity and generate the effectiveness of the management of network security.

VI. CONCLUSION

The current research provided the creation of a Python and IPTables-based Real-Time Network Security Monitoring and Auto-Mitigating Firewall System. The system combines traffic monitoring, threat detection and automated firewall management into a single system that is able to react to cyber threats in real time.
The outcome of experiments proves that the system offers rapid detection, effective mitigation, and a minimum level of resources. The solution suggested provides a viable and scaled solution to enhancing network security within the contemporary computing landscape.

VII. FUTURE SCOPE

Additional improvements to the system in the future can be to incorporate machine learning algorithms to enhance the accuracy of threat detection and minimise false positives. Further enhancements might include upgrading to new firewall solutions that can support distributed network and work with larger rule sets. Further improvement of system scalability and usability will be achieved by the development of centralized monitoring dashboards and cloud-based deployment options.

REFERENCES

[1] *Automation* 2025 paper, *6*(3), 43; https://doi.org/10.3390/automation6030043
[2] IEEE - 'Intrusion Detection and Prevention Systems: A Survey' (2023)
[3] ACM Computing Surveys - 'Network Security Automation Techniques' (2024)
[4] Journal of Network Security - 'Real-Time Threat Mitigation Strategies' (2023)
[5] IPTables Official Manual - 'Linux Firewall Configuration Guide' (2023)
[6] OWASP Foundation, "OWASP Top 10 – Web Application Security Risks," 2023. [Online]. Available: https://owasp.org/www-project-top-ten/
[7] Cybersecurity Research - 'Behavioral Analysis in Network Security' (2024)
[8] C. Sanders and J. Smith, *Applied Network Security Monitoring: Collection, Detection, and Analysis*, Syngress, 2014.
[9] M. Rash, *Linux Firewalls: Attack Detection and Response with IPTables, PSAD, and fwsnort*, No Starch Press, 2007.
[10] SANS Institute - 'Automated Security Response Systems' (2023)
[11] Python Scapy Documentation - 'Packet Manipulation and Analysis' (2024)
[12] Netfilter Project, "IPTables / Netfilter Documentation," Available: https://www.netfilter.org/
[13] S. Northcutt and J. Novak, *Network Intrusion Detection*, New Riders Publishing, 2003.
[14] Nmap Security Scanner, "Nmap Reference Guide," Available: https://nmap.org/docs.html
[15] S. Axelsson, "The Base-Rate Fallacy and its Implications for the Difficulty of Intrusion Detection," *ACM Transactions on Information and System Security*, vol. 3, no. 3, pp. 186-205, 2000.