International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 10 Issue: 03 | March - 2026 SJIF Rating: 8.659 ISSN: 2582-3930

ShieldNet: An Intelligent Network Security and Threat Detection System

Siddh Shah, Akshit Shriyan, Parth Singh, Pranav Prakash
Department of Computer Engineering
Atharva College of Engineering, University of Mumbai Mumbai, India

***Abstract*—ShieldNet is an integrated cybersecurity system designed to provide real-time network protection through continuous monitoring and threat detection. The project focuses on identifying malicious activities such as unauthorized access, open-port vulnerabilities, and malware threats within a network. The system combines multiple security mechanisms including intrusion detection, port scanning, and malware analysis into a unified framework. ShieldNet emphasizes proactive defense by alerting administrators to potential threats and enabling timely mitigation. The prototype demonstrates efficient threat monitoring and secure access control, with scope for future enhancements using intelligent detection techniques.**

***Index Terms*—Network Security, Cybersecurity, Intrusion Detection, Malware Analysis, Threat Monitoring**

I. Introduction

The exponential growth of digital infrastructure and internet-connected systems has significantly increased exposure to cyber threats. Organizations and individuals alike face risks such as data breaches, malware infections, denial-of-service attacks, and unauthorized access to sensitive resources. As networks grow in complexity, ensuring continuous protection and visibility has become a critical challenge.

Cybersecurity systems must not only detect known threats but also adapt to evolving attack patterns. Traditional security mechanisms, such as static firewalls and signature-based detection systems, often struggle to respond effectively to sophisticated and zero-day attacks. This has led to the development of intelligent, integrated security platforms capable of real-time monitoring and dynamic response.

ShieldNet addresses these challenges by providing a centralized cybersecurity platform that enables continuous network monitoring and real-time threat detection. By integrating intrusion detection, malware analysis, and vulnerability assessment into a single framework, the system improves situational awareness and strengthens overall network defense. The prototype demonstrates an efficient and scalable approach to protecting modern network environments.

By combining intrusion detection, malware analysis, and vulnerability assessment, the system enhances visibility and strengthens network defense. The proposed prototype demonstrates a practical and scalable approach to securing modern network environments.

II. Literature Review

Extensive research has been conducted in the field of network security and cyber threat detection. Existing studies emphasize the importance of intrusion detection systems (IDS), malware scanners, and vulnerability assessment tools in safeguarding digital assets. Traditional IDS solutions rely heavily on signature-based detection, which is effective for known threats but limited against novel attack vectors.

Recent research highlights the shift toward behavior-based and anomaly detection techniques, where network traffic patterns are continuously analyzed to identify deviations from normal behavior. These approaches improve detection accuracy but often require higher computational resources and efficient system design.

Other studies explore integrated security frameworks that combine multiple tools—such as port scanners, malware analyzers, and access control systems—into a unified architecture. Such integration improves threat correlation and simplifies security management. Cloud-based monitoring and logging systems further enhance scalability and remote observability but introduce concerns related to latency and data privacy.

Several studies also focus on vulnerability assessment techniques such as port scanning and service enumeration to identify potential entry points for attackers. These techniques help administrators detect misconfigured services and exposed ports before they are exploited. Other research emphasizes malware detection mechanisms that analyze file behavior and network traffic patterns to identify malicious activity.

Recent advancements highlight the need for centralized security platforms that integrate multiple security tools into a unified system. Such frameworks improve threat correlation, reduce response time, and simplify security management. ShieldNet aligns with these approaches by combining monitoring, detection, and analysis modules into a single prototype for effective network security.

This approach enables real-time network monitoring, threat diagnostics, and centralized security management through a unified security platform. Integrated monitoring systems reduce manual intervention and improve scalability, but also introduce challenges related to performance overhead, data privacy, and secure access control.

This project builds on existing literature by implementing a cost-effective network security prototype that combines intrusion detection, malware analysis, and vulnerability assessment. Instead of relying solely on traditional standalone security tools, ShieldNet employs a unified and lightweight monitoring framework for analyzing network activity and system behavior.

III. System Overview

A. Problem Statement

Modern networks face challenges such as unauthorized access, hidden vulnerabilities, and delayed threat detection. The absence of centralized monitoring increases the risk of security breaches. ShieldNet aims to provide a unified security system for real-time threat detection and network protection.

B. System Design

The system consists of interconnected security modules responsible for network monitoring, intrusion detection, malware scanning, and port analysis. A centralized interface displays alerts and system status. The modular design allows easy expansion and efficient monitoring of network security.

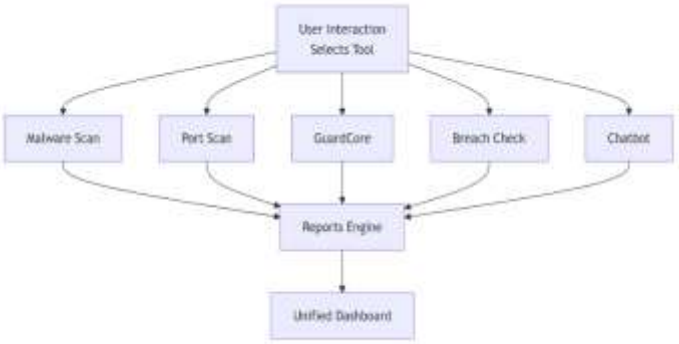

Fig. 1: System Architecture

C. Functional Scenarios

- **Malware Detection:** Uploaded files or URLs are analyzed using signature-based and heuristic techniques to identify malicious content.
- **Vulnerability Assessment:** Target IP addresses or domains are scanned to detect open ports and exposed services that may pose security risks.
- **Threat Monitoring and Alerting:** Detected threats, breaches, and suspicious activities are consolidated and reported to the user through a unified dashboard for timely response.

IV. Implementation

ShieldNet is implemented using backend services that monitor network traffic and analyze system activity. The intrusion detection module identifies suspicious behavior, while the port scanner detects open and vulnerable ports. Malware analysis examines files and data packets for malicious patterns.

The frontend interface provides real-time visualization of security alerts and system status. Secure authentication ensures controlled access to sensitive information.

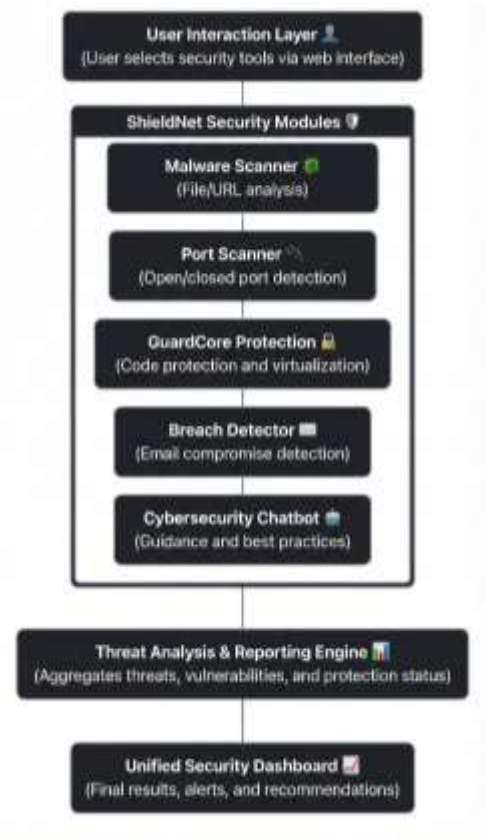

Fig. 2: Block Diagram

A. Cloud Integration

- Real-time security data upload to the centralized ShieldNet cloud platform for continuous monitoring.
- Security modules initiate operations only after successful cloud synchronization and authentication.

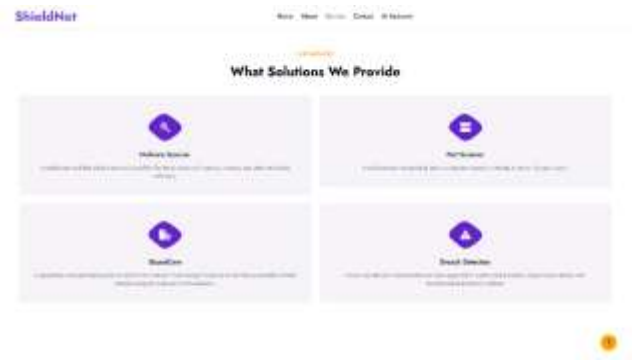

Fig. 4: Services

V. Results

- Successful detection of malicious files and suspicious network activity.
- Accurate identification of open ports and vulnerable services during scans.
- Real-time generation of security alerts without noticeable performance overhead.
- Centralized dashboard provided clear visualization of threats and system status.
- Stable and consistent operation observed during continuous monitoring scenarios.

VI. Conclusion

ShieldNet demonstrates an effective approach to network security by integrating multiple protection mechanisms into a single system. The prototype enhances visibility, improves response time, and provides a scalable foundation for advanced cybersecurity solutions.

VII. Future Work

- Integration of **machine learning techniques** for **intelligent threat detection**.
- Development of a **centralized web dashboard** for **multi-network monitoring**.
- Implementation of **automated incident response** and **alert mitigation** mechanisms.
- **Large-scale deployment and testing** in **real-world network environments**.

Acknowledgment

The authors would like to express their sincere gratitude to the Department of Computer Engineering, Atharva College of Engineering, for resources and support. Special thanks to Dr. Shweta Sharma for her guidance and encouragement throughout the project.

References

[1] R. Abu Bakar and B. Kijsirikul, "Enhancing Network Visibility and Security," *Sensors*, vol. 23, no. 17, Aug. 2023.
[2] Y. Ye, T. Zeng, Y. Duan, J. Han, G. Zhong, Z. Chen, and Y. Wang, "Obfuscated Malicious Traffic Detection Based on Data Enhancement," *Frontiers in Computer Science*, 2025.
[3] S. Swami, I. Singh, U. Singh, and C. P. Pant, "Adaptive Detection of Polymorphic Malware: Leveraging Mutation Engines and YARA Rules for Enhanced Security," *arXiv*, Nov. 2025.