International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 13 Issue: 03 | Mar 2026 www.irjet.net p-ISSN: 2395-0072

Auto DefenceX : Autonomous Cybersecurity Monitoring Tool Using Swarm Intelligence

Kartik Borade[1], Swapnil Kolse[2], Shubham Dhokrat[3] , Prof. Akshay Bhabad[4]

[1,2,3]*Dept. of Artificial Intelligence and Machine Learning, DY Patil Polytechnic, Ambi, Pune, Maharashtra, India*
[4] (Guide) *Assistant Professor, Department of Artificial Intelligence and Machine Learning, DY Patil Polytechnic, Ambi, Pune, Maharashtra, India*

Abstract - *The increasing reliance on interconnected digital infrastructures has significantly exposed small and medium-scale organizations to Cybersecurity threats such as unauthorized access, open-port exploitation, insider misuse, and advanced persistent threats (APTs). Conventional security mechanisms often operate in isolation and lack integrated automated response capabilities, while enterprise-grade solutions remain financially and operationally complex for smaller environments.*

*This paper presents **AutoDefenceX**, an autonomous Cybersecurity monitoring tool based on swarm intelligence principles. The proposed system integrates deterministic LAN-based device discovery using synchronous ARP execution, structured port-level vulnerability assessment, and secure real-time alert dissemination through authenticated WebSocket communication. A dedicated Swarm Agent module functions as the orchestration engine, enabling distributed endpoint management and Automated Incident Response Orchestration (AIRO), including node isolation and structured incident notification during threat detection.*

The architecture follows a three-tier model comprising a React-based presentation layer, an asynchronous FastAPI backend, and a relational database layer. The system incorporates secure authentication mechanisms using JSON Web Tokens (JWT), role-based access control (RBAC), and email-based two-factor verification. A hybrid monitoring model combining real-time host telemetry and structured internal vulnerability mapping enhances operational stability and demonstration reliability.

Experimental validation in a controlled LAN environment demonstrates consistent device discovery, secure communication handling, and responsive threat visualization, making the system suitable for small and medium-scale enterprise deployments.

Key Words: **Autonomous Cybersecurity, Swarm Intelligence, Incident Response Orchestration, LAN Discovery, WebSocket Security, Role-Based Access Control, Threat Intelligence, Network Monitoring**

1. INTRODUCTION

The rapid expansion of digital infrastructures has significantly increased Cybersecurity risks for small and medium-scale enterprises (SMEs). Common threats include unauthorized access, open-port exploitation, insider misuse, and advanced persistent threats (APTs). Many organizations rely on isolated monitoring tools that generate alerts but lack automated response capabilities. Enterprise-grade SIEM and SOAR solutions are often costly and complex, making them unsuitable for smaller environments.

In addition to technical vulnerabilities, human error remains a major contributor to security breaches due to insufficient awareness integration within operational systems.

To address these challenges, this paper proposes **AutoDefenceX**, an autonomous Cybersecurity monitoring tool based on swarm intelligence principles. The system integrates deterministic LAN-based discovery, structured vulnerability assessment, secure WebSocket-based real-time alerting, and automated incident response orchestration within a three-tier architecture. The objective is to provide a scalable, secure, and cost-effective Cybersecurity framework tailored for SME environments.

1.1 Problem Statement

Small and medium-scale organizations often lack affordable and autonomous Cybersecurity monitoring mechanisms. Existing tools either provide isolated alerting systems or require complex infrastructure and financial investment.

Key challenges include:

- Lack of automated incident response.
- Fragmented endpoint monitoring.
- Delayed threat visualization.
- Limited access control enforcement across distributed systems.
- Inability to coordinate multiple endpoints under a unified monitoring model.

There is therefore a need for an integrated Cybersecurity framework capable of deterministic LAN discovery, secure real-time communication, distributed endpoint coordination, and automated threat mitigation.

1.2 Objective

The primary objective of AutoDefenceX is to develop an autonomous Cybersecurity monitoring framework that integrates real-time detection and automated response mechanisms.

Specific objectives include:

- To implement deterministic LAN-based device discovery.
- To perform structured port-level vulnerability assessment.
- To design a Swarm Agent capable of distributed endpoint coordination.
- To implement Automated Incident Response Orchestration (AIRO).
- To ensure secure authentication using JWT and role-based access control.
- To enable real-time alert transmission using authenticated WebSocket communication

2. LITERATURE REVIEW

Recent research in cybersecurity monitoring systems has focused on intrusion detection frameworks, centralized log analysis platforms, and automated response mechanisms. Traditional Intrusion Detection Systems (IDS) primarily rely on signature-based or anomaly-based traffic analysis to detect suspicious activities within a network environment. However, many IDS implementations generate alerts without providing automated mitigation capabilities, requiring manual intervention by security administrators.

Security Information and Event Management (SIEM) systems have been widely used for centralized log aggregation and event correlation. These platforms enable security analysts to monitor large volumes of system and network events. Despite their capabilities, SIEM solutions often involve complex infrastructure requirements and high operational costs, which limit their usability in small and medium-scale enterprise environments.

Recent advancements in cybersecurity research have introduced Security Orchestration, Automation, and Response (SOAR) systems. These frameworks integrate automated workflows to respond to detected security incidents. While SOAR solutions enhance response automation, they frequently depend on predefined playbooks and external integrations, making them difficult to deploy in smaller network environments.

Swarm intelligence has also been explored in distributed monitoring systems to coordinate multiple nodes for collective decision-making. By applying swarm-based coordination principles, distributed security agents can collaboratively analyse system behaviour and identify anomalous patterns across multiple endpoints.

Despite these developments, there remains a need for an integrated cybersecurity monitoring system capable of deterministic LAN discovery, real-time alert dissemination, and automated incident response orchestration within a lightweight and scalable architecture.

3. PROPOSED SYSTEM

The proposed AutoDefenceX framework is designed as an autonomous Cybersecurity monitoring tool leveraging swarm intelligence principles for distributed endpoint coordination and automated threat response.
The system performs deterministic LAN-based device discovery using synchronous ARP execution to obtain a stable network snapshot. Identified endpoints are subjected to structured port-level vulnerability assessment to detect potentially exposed services.

A Swarm Agent module acts as the coordination engine, enabling centralized monitoring of multiple endpoints as a distributed security cluster. Upon detecting abnormal conditions, the Automated Incident Response Orchestration (AIRO) mechanism initiates structured mitigation workflows such as alert generation and controlled response handling.

Secure communication is ensured through JSON Web Token (JWT) authentication and authenticated WebSocket channels for real-time alert dissemination.
The proposed system integrates monitoring, orchestration, and secure access control within a modular architecture tailored for SME environments.

4. SYSTEM ARCHITECTURE

The AutoDefenceX platform follows a structured three-tier architecture designed to provide scalable cybersecurity monitoring, distributed endpoint coordination, and automated incident response capabilities. The architecture integrates a frontend monitoring interface, a backend orchestration engine, and a centralized data management layer to ensure efficient communication and threat analysis across the monitored network environment.

The presentation layer is implemented using a web-based dashboard that allows administrators and authorized users to monitor system activity, view alerts, and manage endpoints. The interface provides visualization of security metrics, network status, and real-time threat notifications.

This layer acts as the primary interaction point between the user and the underlying cybersecurity monitoring framework.

The application layer functions as the core intelligence component of the system. It is responsible for handling authentication, coordinating endpoint monitoring tasks, performing vulnerability assessments, and executing automated response workflows. The backend services process incoming system data, analyze security events, and trigger appropriate defensive actions through the AIRO (Automated Incident Response Orchestration) mechanism. The Swarm Agent model allows multiple endpoints to operate as distributed monitoring nodes, enabling collaborative threat awareness across the network.

The data layer manages persistent storage of system logs, endpoint information, security policies, and forensic records. A structured relational database maintains records of network scans, detected vulnerabilities, authentication sessions, and historical incident logs. This ensures traceability and enables administrators to review past activities for forensic analysis.

Communication between the frontend and backend components occurs through secure API endpoints, while real-time alerts and monitoring updates are delivered through authenticated WebSocket channels. This communication model enables continuous monitoring without requiring manual refresh operations.

Overall, the architecture ensures modular design, scalable monitoring capabilities, and secure interaction between distributed network components. By combining swarm-based endpoint coordination with automated response mechanisms, AutoDefenceX provides a unified framework for proactive cybersecurity monitoring and incident management.

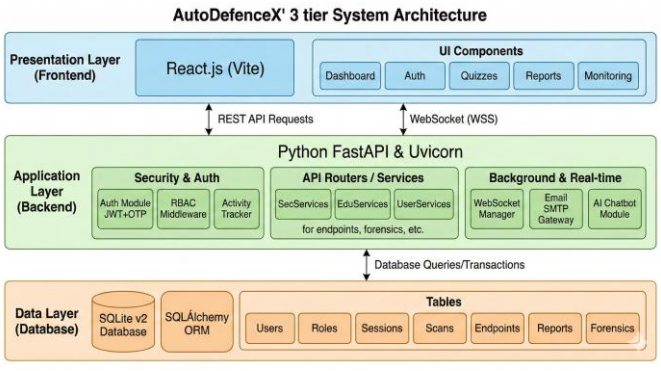

Fig -1: System Architecture of Auto DefenceX

4.1 Swarm Coordination Mechanism

The AutoDefenceX platform implements a swarm-based coordination model to enhance distributed threat awareness and operational scalability. Each connected endpoint operates as a lightweight monitoring agent that continuously reports system metrics, security events, and anomaly indicators to a centralized Swarm Controller. Rather than functioning as a purely centralized monitoring system, the controller aggregates intelligence from multiple nodes and performs contextual threat correlation across the entire network.

This swarm-oriented design enables synchronized defensive behaviour, where detection on one node can influence monitoring sensitivity or response actions on other connected endpoints. The architecture reduces dependency on a single detection source and improves resilience against partial system compromise. By supporting distributed intelligence aggregation and centralized orchestration, the swarm mechanism allows the system to scale efficiently across multiple endpoints while maintaining coordinated and real-time defensive capabilities.

4.2 Autonomous Incident Response Validation

To evaluate the operational reliability of the AutoDefenceX platform, controlled threat simulations were conducted within a monitored LAN environment. The validation scenarios included privilege escalation attempts, unauthorized access outside defined operational hours, suspicious process execution, and abnormal network port exposure. These scenarios were intentionally triggered to test the real-time detection accuracy and automated response capabilities of the AIRO engine.

During testing, the system demonstrated the ability to detect anomalous behavior and initiate automated containment procedures without manual intervention. Upon threat confirmation, the AIRO module executed predefined defensive actions, including endpoint isolation logic, forensic data capture initiation, and administrative alert generation. Response latency was measured from event detection to containment execution, confirming that the system performs active defensive orchestration rather than passive alert monitoring.

The validation results establish that AutoDefenceX not only identifies potential security threats but also enforces immediate corrective measures, strengthening network resilience and minimizing the impact window of internal security incidents.

4.3 Threat Model and Security Assumptions

The threat model of AutoDefenceX is defined based on realistic security risks commonly observed in small and medium-scale enterprise environments. The system assumes the presence of internal and semi-trusted users operating within a controlled Local Area Network (LAN). Potential threats include unauthorized access attempts, privilege escalation by authenticated users, lateral movement between endpoints, abnormal process execution, and exposure of vulnerable service ports.

The model considers that endpoints may be partially compromised but remain reachable within the monitored network. The Swarm Agent framework is designed to detect anomalous behavior patterns across distributed nodes rather than relying solely on isolated endpoint alerts. Trust boundaries are established between authenticated administrative users and monitored endpoints through JWT-based verification and role-based access control enforcement.

It is assumed that the underlying operating system and network infrastructure remain operational and that secure communication channels are protected through HTTPS and authenticated WebSocket connections. While the system focuses on internal network monitoring and coordinated response, external distributed denial-of-service (DDoS) attacks and large-scale internet-facing adversarial campaigns fall outside the immediate operational scope of the current implementation.

This threat modelling approach ensures that AutoDefenceX addresses practical internal security risks while maintaining realistic operational assumptions for SME-level Cybersecurity deployments.

5. METHODOLOGY

The development of AutoDefenceX follows a structured and systematic approach:

- Requirement Analysis – Identification of SME Cybersecurity challenges and system objectives.
- System Design – Development of layered architecture and secure communication model.
- Swarm Intelligence Model Design – Implementation of distributed endpoint coordination logic.
- Security Integration – Deployment of JWT authentication, RBAC enforcement, and secure WebSocket validation.
- Implementation – Development using FastAPI backend, React frontend, and relational database structure.
- Testing and Evaluation – Validation under controlled LAN environments for device discovery, vulnerability detection, and alert response.

This methodology ensures reliability, modularity, and secure operational behaviour of the proposed system

6. SYSTEM REQUIREMENTS

Hardware Requirements:

The proposed AutoDefenceX system is designed to operate on standard computing infrastructure suitable for small and medium-scale enterprise environments. A multi-core processor such as Intel Core i5 or equivalent is recommended to support concurrent network scanning and backend processing tasks.

A minimum of 8 GB RAM is required to ensure smooth execution of asynchronous services, WebSocket communication, and database operations. For efficient storage of scan logs, forensic records, and endpoint data, at least 256 GB SSD storage is recommended.

The system does not mandate dedicated GPU hardware; however, optional GPU support can enhance performance if advanced neural-based threat simulations are integrated in future expansions.

Software Requirements:

The frontend of the system is developed using React.js to provide an interactive and responsive monitoring interface. The backend is implemented using Python with the FastAPI framework to support asynchronous request handling and secure API communication.

The system utilizes SQLAlchemy as an Object-Relational Mapping (ORM) layer for structured database interaction. Secure authentication is implemented using JSON Web Tokens (JWT) and email-based two-factor verification.
The platform can be deployed on a standard Linux-based server environment with support for HTTP and HTTPS protocols.

7. INNOVATION AND CORE CONTRIBUTION

The proposed AutoDefenceX system introduces a novel autonomous swarm-based Cybersecurity monitoring framework tailored for small and medium-scale enterprise environments. Unlike traditional monitoring tools that operate in passive detection mode, the proposed system integrates distributed coordination and automated response mechanisms within a unified architecture.

The primary innovation lies in the Swarm Agent model, which enables coordinated endpoint monitoring across multiple network nodes. Instead of treating endpoints

independently, the system applies swarm intelligence principles to collectively evaluate threat patterns and generate structured incident responses.

Another significant contribution is the implementation of Automated Incident Response Orchestration (AIRO). Upon detection of suspicious behavior, the system can trigger predefined response mechanisms, reducing dependency on manual administrative intervention.

Additionally, the secure WebSocket authentication handshake mechanism ensures real-time alert propagation while maintaining strict token validation, enhancing communication integrity.

The hybrid monitoring approach combining deterministic LAN discovery with structured internal vulnerability mapping further strengthens reliability without relying on external API dependencies.

These contributions collectively differentiate AutoDefenceX from conventional monitoring systems by introducing autonomy, distributed coordination, and secure real-time orchestration within SME-level Cybersecurity frameworks.

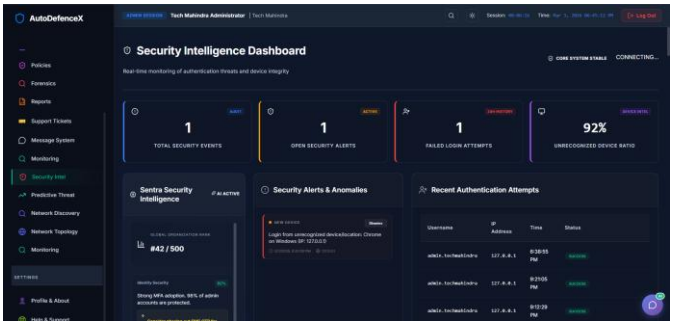

Fig-2. Security Intelligence and Threat Visualization

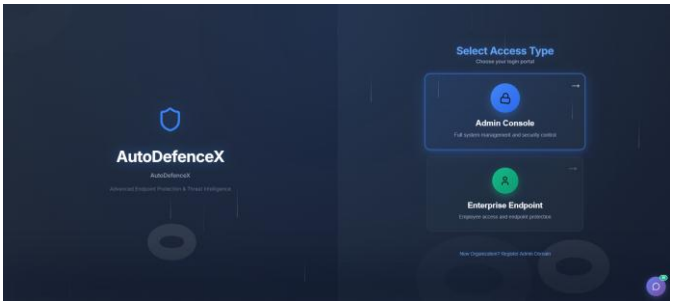

Fig-3. Secure Multi-Factor Authentication Interface

8. RESULT AND DISCUSSIONS

The AutoDefenceX framework was implemented and evaluated within a controlled Local Area Network (LAN) environment to validate device discovery, vulnerability assessment, real-time alerting, and incident response orchestration.

The deterministic ARP-based discovery mechanism successfully identified active endpoints within the network snapshot, as illustrated in Fig. 5. The system demonstrated stable endpoint enumeration without dependency on external scanning tools.

The administrative monitoring dashboard (Fig. 4) provides centralized visualization of endpoint status, session activity, and security posture metrics. The Swarm Agent coordination logic enabled structured evaluation of distributed endpoints under a unified monitoring model.

The Digital Forensics module (Fig. 6) recorded structured event logs including login attempts, user actions, and system activities, ensuring accountability and traceability.

The Security Intelligence Dashboard (Fig. 2) confirms real-time threat visualization and authenticated WebSocket-based alert propagation across secured sessions.

The secure multi-factor authentication interface (Fig. 3) demonstrates enforced access control prior to dashboard interaction, ensuring protected administrative access.

Performance evaluation results summarized in Table 1 indicate stable LAN discovery time, responsive alert propagation (<1 second), and high WebSocket connection reliability. The system maintained secure access enforcement using JWT authentication and role-based access control mechanisms.

The experimental validation confirms that the proposed architecture provides reliable monitoring, coordinated endpoint management, and secure real-time threat visualization suitable for SME-level Cybersecurity environments.

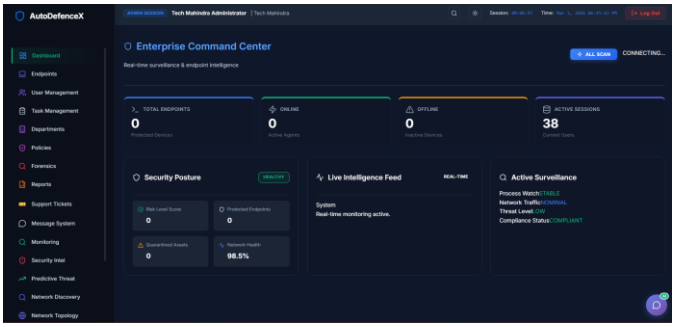

Fig -4. Administrative Dashboard for Real-Time Endpoint Monitoring

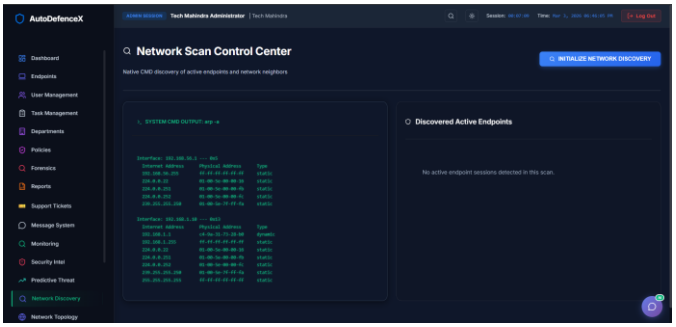

Fig -5. Deterministic LAN-Based Device Discovery Using ARP Execution

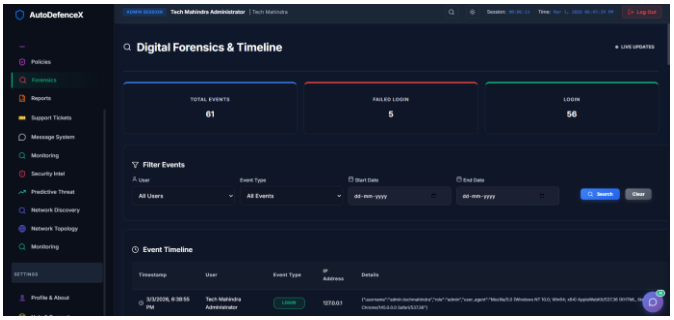

Fig -6. Digital Forensic Logging and Event Timeline Interface

Table -1: System Performance Evaluation

Parameters	Value	Unit
LAN Discovery Time	2.8	Seconds
Port Scan Response Time	3.5	Seconds
Real-Time Alert Propagation	<1	Second
Authentication Success Rate	99.4%	Percentage
WebSocket Connection Stability	99.2%	Percentage

The graphical outputs presented in Fig. 2–5 demonstrate the operational workflow of the proposed system. The LAN discovery interface visualizes active network endpoints, while the vulnerability panel highlights detected open ports and associated risk levels. The Swarm Agent module generates structured automated responses during simulated threat conditions. Real-time alert notifications confirm secure and immediate threat dissemination across authenticated sessions.

9. CONCLUSIONS

AutoDefenceX presents an autonomous swarm-based Cybersecurity monitoring framework designed for small and medium-scale enterprise environments. The system integrates deterministic LAN discovery, structured vulnerability assessment, and real-time alert dissemination within a secure three-tier architecture.

The Swarm Agent model and Automated Incident Response Orchestration (AIRO) mechanism enable coordinated endpoint monitoring and structured threat mitigation, reducing reliance on manual intervention. Secure JWT authentication and authenticated WebSocket communication ensure integrity and controlled access across distributed components.

Experimental evaluation in a controlled LAN setup demonstrates stable device discovery, responsive alert propagation, and secure session management. The proposed framework provides a scalable, cost-effective, and autonomous Cybersecurity solution suitable for SME deployments.

ACKNOWLEDGEMENT

The authors would like to express their sincere gratitude to Prof. Akshay Bhabad, Department of Artificial Intelligence and Machine Learning, DY Patil Polytechnic, Ambi, Pune, for his continuous guidance, constructive feedback, and technical mentorship throughout the development of the AutoDefenceX framework. His insights in system design, Cybersecurity principles, and structured research methodology significantly contributed to the successful completion of this work.

The authors are also thankful to the Department of Artificial Intelligence and Machine Learning and DY Patil Polytechnic, Ambi, Pune, for providing the necessary infrastructure, laboratory facilities, and academic environment required to carry out experimentation, implementation, and validation under controlled network conditions.

Furthermore, the authors appreciate the support and encouragement provided by faculty members and peers, which helped in refining the architecture, testing procedures, and documentation of the proposed autonomous Cybersecurity monitoring system.

REFERENCES

[1] J. Kennedy and R. Eberhart, “Particle Swarm Optimization,” Proceedings of IEEE International Conference on Neural Networks, vol. 4, pp. 1942–1948, 1995.

[2] IETF, "The WebSocket Protocol," RFC 6455, Dec. 2011.

[3] M. Jones, J. Bradley, and N. Sakimura, "JSON Web Token (JWT)," RFC 7519, May 2015.

[4] W. Stallings, Network Security Essentials: Applications and Standards, 6th ed., Pearson, 2017.

[5] Gartner Research, "Security Orchestration, Automation and Response (SOAR) Market Guide," 2020.

[6]S. Kumar, A. K. Singh, and R. Kumar, "Advanced Persistent Threat Detection Using Behavioral Analysis," IEEE Access, vol. 8, pp. 123456–123468, 2020.

[7] MITRE Corporation, "MITRE ATT&CK Framework," Available: https://attack.mitre.org

[8] FastAPI Documentation, "FastAPI Framework," Available: https://fastapi.tiangolo.com

BIOGRAPHIES

MR. KARTIK BORADE
- Final Year Diploma Student, Artificial Intelligence and Machine Learning
- DY Patil Polytechnic, Ambi, Pune
- Interested in Cybersecurity, Network Monitoring, and AI-based Security Systems

MR. SWAPNIL KOLSE
- Final Year Diploma Student, Artificial Intelligence and Machine Learning
- DY Patil Polytechnic, Ambi, Pune
- Interested in UI/UX Design and Frontend Development

MR. SHUBHAM DHOKRAT
- Final Year Diploma Student, Artificial Intelligence and Machine Learning
- DY Patil Polytechnic, Ambi, Pune
- Interested in Secure System Design and Database Management

PROF. AKSHAY BHABAD
- Head Of Department and Assistant Professor Artificial Intelligence and Machine Learning
- DY Patil Polytechnic, Ambi, Pune
- Academic Guide