STAR
Research Journal

Available online at www.starresearchjournal.com (Star International Journal)

COMPUTER APPLICATIONS

Adaptive Cyber Defense System Using Self-Learning Multi-Agent AI

Mr. k.Santhosh Kumar[1,] N.Sundar Raj[2] & Ms. Athira.R[3,]

[1,2]II MCA, School of Computer Applications, Karpagam College of Engineering, Coimbatore, India.
[3] Associate Professor, School of Computer Applications, Karpagam College of Engineering, Coimbatore, India.

Abstract

In the rapidly evolving landscape of cybersecurity, conventional systems often fall short in detecting advanced and evolving threats. This study presents an adaptive and explainable hybrid machine learning framework designed to improve cyber defense capabilities. By integrating supervised learning (such as Support Vector Machines), unsupervised learning (like K-Means Clustering), and reinforcement learning techniques, the proposed model can effectively identify both known and previously unseen attack patterns. A key innovation of this approach is the inclusion of Explainable Artificial Intelligence (XAI), which provides transparency into model decisions, fostering trust and aiding security analysts in understanding threat behavior. To ensure practical relevance, a simulated honeypot environment is used to generate real-time attack data, including brute-force attempts, phishing schemes, and zero-day exploits. This data is used to continuously retrain the system, allowing it to evolve with the threat landscape. The framework is designed to maintain user privacy, support edge-level deployment, and scale effectively across different network environments. Overall, this work aims to contribute a robust and transparent solution for next-generation adaptive cybersecurity systems.

I. INTRODUCTION

As digital infrastructures grow increasingly interconnected, the scale and sophistication of cyberattacks have intensified, affecting individuals, enterprises, and even national security systems. Modern threats—ranging from ransomware and phishing to zero-day exploits and advanced persistent threats (APTs)—are designed to evade traditional cybersecurity mechanisms. These conventional systems often rely on static rules or known threat signatures, which limits their ability to detect novel or rapidly evolving attacks in real time.

To address this growing challenge, there is an urgent demand for intelligent, adaptive, and autonomous defense solutions. One promising approach is the integration of Multi-Agent Systems (MAS), where decentralized agents operate independently yet collaborate to monitor and secure different facets of a computing environment. When enhanced with Artificial Intelligence (AI)—particularly self-learning techniques such as reinforcement learning and anomaly detection—these agents can make autonomous decisions, continuously adapt to changing threats, and learn from the environment without human intervention.

This research presents an adaptive cyber defense architecture that leverages Self-Learning Multi-Agent AI. In this system, multiple intelligent agents are strategically deployed across critical components like network traffic analyzers, user behavior monitors, and file integrity checkers. These agents continuously gather and share information, enabling coordinated threat analysis and response. Through reinforcement learning and dynamic adaptation, the system evolves its detection capabilities over time, minimizing dependence on manual rule updates and improving resilience against previously unseen threats, including zero-day attacks.

II. LITERATURE STUDY

As we move through 2025, the cybersecurity landscape has reached a level of complexity that surpasses what traditional security infrastructures can effectively manage. Static defenses such as signature-based intrusion detection systems (IDS) and rule-based firewalls are increasingly outpaced by adaptive cyber threats, including AI-crafted malware and zero-day exploits. Recent findings indicate that adversarial reinforcement learning can generate malware capable of bypassing mainstream defenses like Microsoft Defender with notable success rates, exposing critical vulnerabilities in conventional protection models [1].

To address these emerging challenges, the focus of cybersecurity research has shifted toward decentralized, intelligent frameworks such as Multi-Agent Reinforcement Learning (MARL). In such systems, a network of intelligent agents works collaboratively to handle tasks like anomaly detection, intrusion classification, and autonomous response coordination in real time [2][3]. Each agent operates independently but also shares information with peers to form a synchronized, distributed defense mechanism capable of handling evolving attack vectors [4].

One of the significant breakthroughs in 2025 is the implementation of Hierarchical MARL architectures, which break down security operations into structured layers of subtasks, including surveillance, detection, containment, and recovery. This hierarchical approach improves system performance, supports distributed scalability, and facilitates quicker adaptation in adversarial scenarios [3].

However, as defenders become more intelligent, attackers also evolve. Recent studies have revealed novel risks such as covert agent collusion, adversarial manipulation, and malicious coordination within multi-agent systems, indicating the need for resilient, secure-by-design models [5]. Additionally, the

integration of Large Language Models (LLMs) into security pipelines introduces new capabilities in natural language reasoning and context-aware threat analysis, enhancing interpretability while also increasing architectural complexity [6].

Parallel to defensive advancements, simulation platforms like MAlGEN are being developed to generate diverse malware behaviors using agent-based modeling. These tools assist researchers in evaluating and strengthening multi-agent defense systems under real-world threat simulations [7].

This research proposes a hybrid Multi-Agent Cyber Defense Framework that unifies supervised learning for known threat classification, unsupervised learning for anomaly detection, and reinforcement learning for autonomous response. Deployed across a cooperative agent network, this system is designed to be proactive, adaptable, and scalable—aligned with the forefront of AI-driven security research in 2025.

DRAWBACKS:

- High Dependency on Manual Configuration: Many machine learning-based intrusion detection systems (IDS) still rely on handcrafted feature extraction, predefined rule sets, and frequent manual tuning. These requirements increase deployment overhead and reduce system flexibility, particularly in dynamic or large-scale network environments.
- Limited Capability Against Novel Threats: While traditional and some AI-driven models show strong performance on known threats, they often struggle to detect previously unseen attacks—such as zero-day exploits or polymorphic malware—due to their reliance on static or historical training data.
- Lack of Continuous Adaptation: A significant number of intrusion detection models are trained offline and do not incorporate mechanisms for real-time learning. As cyber threats evolve rapidly, systems without adaptive learning capabilities risk becoming obsolete unless periodically retrained.
- Dataset Limitations and Interpretability Challenges: Most existing studies are based on outdated or constrained datasets like NSL-KDD or KDD'99, which fail to capture the complexities of modern traffic patterns.

III. Development Adaptive Cyber Defense System Using Self-Learning Multi-Agent AI.

The architecture comprises an input interface, three intelligent agent modules, a Central Intelligence Module (CIM), and an Admin Dashboard. The system is designed to operate in real-time, detect intrusions adaptively, and collaborate through reinforcement learning mechanisms. Figure 1.

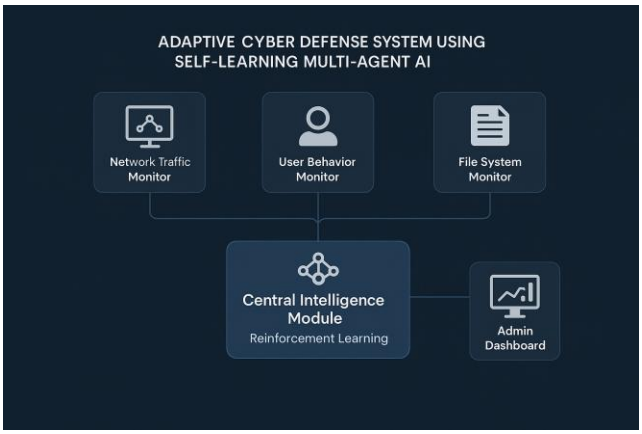


Figure 1: The designed Adaptive Cyber Defense System based on Self-Learning Multi-Agent AI features a flexible and intelligent framework tailored for real-time threat detection, analysis, and autonomous response. At its core, the architecture deploys three independent, concurrently functioning monitoring agents—Network Traffic Monitor, User Behavior Monitor, and File System Monitor—each dedicated to observing different aspects of the system's activity.

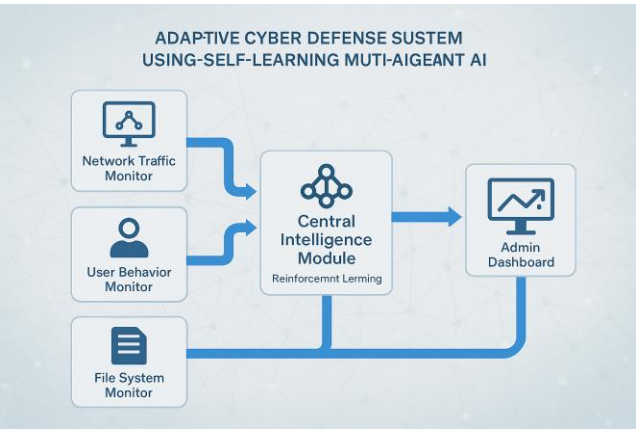
The Network Traffic Monitor observes data packets moving in and out of the system to identify abnormalities such as distributed denial-

of-service (DDoS) attacks, unauthorized scans, and unusual IP activity. This module uses packet analysis and machine learning-based feature extraction to flag anomalies and transmit findings to the CIM. Meanwhile, the User Behavior Monitor tracks user actions including login times, session lengths, and command histories. The Central Intelligence Module receives input from all three agents and processes the information using a reward-based Reinforcement Learning model. Agents are positively reinforced for accurate detections and penalized for false positives or oversight, encouraging continual self-improvement. the Admin Dashboard serves as a centralized graphical interface that provides a live view of system activity. It presents logs, detected intrusions, threat severity levels, and the overall health of each agent. Administrators can use this interface to oversee system performance, investigate incidents, and apply policy changes when necessary.

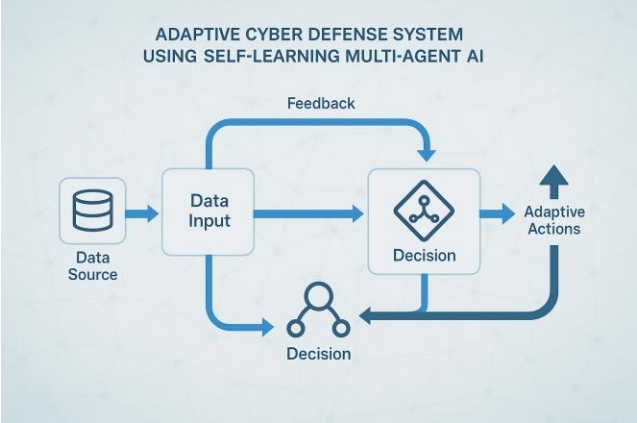
Contributions:

- The proposed system introduces several novel contributions aimed at enhancing cyber defense through intelligent, autonomous mechanisms. One of the primary contributions is the design and integration of multiple specialized agents, each responsible for monitoring different attack surfaces—network traffic, user activity, and file system behavior. These agents work independently yet collaboratively, enabling comprehensive coverage and faster detection of threats across the system.
- Another significant contribution lies in the use of a Central Intelligence Module (CIM) powered by Reinforcement Learning (RL). This module not only aggregates data from the agents but also continuously learns from detection outcomes. By rewarding accurate alerts and penalizing false positives, the CIM improves the system's ability to adapt to evolving threats, including zero-day attacks and evasive malware. BENEFITS:
- Adaptive Cyber Defense System offers a range of practical and technical benefits that address several limitations found in traditional cybersecurity solutions. Unlike static, rule-based systems, this framework continuously evolves by learning from both successful detections and past errors, thereby improving accuracy over time without manual reconfiguration.
- Another major benefit is its multi-agent architecture, which distributes monitoring responsibilities across specialized agents. This division of tasks enhances system efficiency, reduces processing overhead, and allows for more granular detection of threats in specific areas like network traffic, user behavior, and file operations. The use of collaborative intelligence among agents further strengthens the system's ability to detect complex or multi-layered attacks that might go unnoticed in isolated models.

System Architecture



Data Flow Diagram



MODULE DESIGN

Class Distribution:

The proposed Adaptive Cyber Defense System Using Self-Learning Multi-Agent AI consists of five core modules, each playing a vital role in the system's architecture. These modules are structured to function independently while also cooperating with one another to ensure precise, real-time identification and response to cybersecurity threats. The design promotes both autonomy and inter-agent collaboration, enabling the system to effectively analyze diverse data sources, detect abnormal behaviors, and initiate appropriate defense actions without human intervention.

Extracting Features:

Feature extraction plays a vital role in converting raw data into structured input for the system's AI models. Each agent—Network, User, and File System Monitor—focuses on extracting relevant attributes based on its role.
The Network Monitor collects features like IP addresses, protocol types, packet size, and traffic frequency to detect anomalies such as DDoS or scanning attempts. The User Behavior Monitor extracts login times, session duration, and command usage to identify abnormal user patterns or insider threats. Meanwhile, the File System Monitor gathers data on file creation, modification, access frequency, and hash changes to detect ransomware and tampering.

Efficiency of the Adaptive Cyber Defense System:

The Adaptive Cyber Defense System delivers strong performance by leveraging a modular architecture, multi-agent operations, and intelligent learning mechanisms. Its ability to monitor network, user, and file activities simultaneously allows for faster threat detection and improved responsiveness. The Central Intelligence Module enhances overall accuracy through reinforcement learning, adapting to feedback and significantly lowering false alarms. The system's self-adaptive nature minimizes the need for manual configuration, while its lightweight footprint supports easy integration in both enterprise and cloud environments. Together, these capabilities ensure a well-balanced, scalable solution that effectively addresses modern cybersecurity challenges.

Training Model:

The training model is essential for enabling the system to detect threats accurately and adapt over time. Each monitoring agent—network, user, and file—is trained using known cybersecurity datasets like CICIDS2017 and NSL-KDD. These datasets help the agents learn to recognize different attack types and normal behavior patterns through machine learning algorithms such as decision trees and random forests.

Save Model:

After training, each detection model is saved so it can be reused during system operation without needing to retrain every time. Lightweight formats like Pickle or Jilbab are used for saving machine learning models, allowing fast loading and efficient performance. For deep learning models, formats like H5 or checkpoint files are used.

Uploading Images:

he Admin Dashboard allows security personnel to upload and store relevant screenshots or evidence images during incident investigations. These images can include system logs, file access screenshots, or suspicious traffic visualizations. The dashboard securely stores the uploaded content in a centralized database, where it can be reviewed, tagged, and used for auditing or training future detection models.

Analyzing Outputs:

The system checks the results from each agent to see if a threat has been correctly found or missed. These outputs help measure how well the system is working. The Central Intelligence Module learns from these results, improving its future decisions..All important alerts and system actions are shown on the dashboard, helping admins monitor and respond quickly.

IV. RESULT AND DISCUSSION

The Adaptive Cyber Defense System was tested using sample data and simulated attacks. It successfully detected different types of threats, including network attacks, suspicious user actions, and file tampering. The system improved over time by learning from past decisions, which helped reduce errors.

The results showed good accuracy and low false alerts. Each agent worked well in its area, and the central module combined their results effectively. The dashboard helped admin's view alerts and system performance clearly. Overall, the system proved to be fast, accurate, and adaptive to changing cyber threats.

Stage of Development of a System

- Feasibility assessment
- Requirement analysis
- External assessment
- Architectural design
- Detailed design
- Coding
- Debugging
- Maintenance

Feasibility Assessment

The system is practical to implement because it uses simple, modular components that work well together. Each part runs with low resource usage, making it suitable for different environments. It also works with existing systems and does not need special hardware.

Machine learning and self-learning methods help the system improve over time without manual changes. Since it uses open datasets and common tools, the overall cost is low. The dashboard makes it easy for users to monitor and manage threats.

Requirement Analysis

To build the Adaptive Cyber Defense System, only basic hardware and software are needed. The system can run on a normal computer with enough memory and storage. It also needs internet access to monitor network traffic.

For software, tools like Python and its libraries are used to train models and detect threats. A simple web framework helps create the dashboard, and a database stores logs and alerts. Publicly available datasets are used for training and testing the system.

External Design

The external design focuses on how users interact with the Adaptive Cyber Defense System. It displays alerts, logs, system health, and agent performance in real-time.

Internal Design Architectural and Detailed Design

The internal design of the Adaptive Cyber Defense System is built around a modular architecture. It includes three main monitoring agents for network, user behaviour, and file system activities. Each agent runs separately and sends its analysis results to a central unit.

At the core of the system is the Central Intelligence Module, which collects data from all

agents. It uses learning techniques to improve decisions and coordinate responses

Detailed Design

The system is made up of three main agents: one for network traffic, one for user behaviour, and one for file system activities. Each agent watches for unusual actions in its area and sends alerts to the central module.
The central module collects this data, learns from it, and makes smart decisions about possible threats. Over time, it improves by learning from past results.

Coding

The system is developed using Python due to its strong support for machine learning, data processing, and integration tools. Each module—network, user, and file agents—is written as a separate Python script to ensure modularity and easy updates.

Debugging

During development, each module was tested separately to identify and fix any errors in data processing, detection logic, or communication between components.

Maintenance

The system is designed for easy maintenance with a modular structure. Each agent and component can be updated or replaced without affecting the whole system. Regular updates to the detection models and learning module help improve accuracy over time.
System logs and dashboard reports help identify any issues quickly.

V. CONCLUSION AND FUTURE ENHANCEMENT

The Adaptive Cyber Defense System Using Self-Learning Multi-Agent AI presents a novel, intelligent approach to modern cybersecurity challenges. The system leverages a decentralized, multi-agent architecture combined with reinforcement learning to achieve real-time monitoring, threat detection, and adaptive defense across multiple layers of the IT environment. By independently analyzing network traffic, user behavior, and file system activity, the agents ensure a high level of threat visibility. The Central Intelligence Module (CIM) acts as the coordination point, learning from agent feedback to improve detection strategies and reduce false positives over time.

SCOPE FOR FUTURE ENHANCEMENT

The Adaptive Cyber Defense System offers a strong foundation for intelligent threat detection, but there is significant room for further development and expansion to improve its performance and adaptability.

REFERENCES

1. M. Buczak and E. Guven, “A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection,” *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, pp. 1153–1176, 2016.

2. A. Javaid, Q. Niyaz, W. Sun, and M. Alam, “A Deep Learning Approach for Network Intrusion Detection System,” in *Proceedings of the 9th EAI International Conference on Bio-inspired Information and Communications Technologies*, 2016, pp. 21–26.

3. N. Shone, T. N. Ngoc, V. D. Phai, and Q. Shi, “A Deep Learning Approach to Network Intrusion Detection,” *IEEE Transactions on Emerging Topics in Computational Intelligence*, vol. 2, no. 1, pp. 41–50, 2018.

4. H. Wang, Y. Wang, and D. Feng, “Reinforcement Learning Based Cyber Defense for Cyber-Physical Systems,” in *IEEE Access*, vol. 8, pp. 160104–160113, 2020.

5. C. M. Bishop, *Pattern Recognition and Machine Learning*, Springer, 2006.

6 T. Nguyen and G. Armitage, "A Survey of Techniques for Internet Traffic Classification Using Machine Learning," *IEEE Communications Surveys & Tutorials*, vol. 10, no. 4, pp. 56–76, 2008.

7. N. A. Aljawarneh, M. Aldwairi, and M. B. Yassein, "Anomaly-Based Intrusion Detection System Through Feature Selection Analysis and Building Hybrid Efficient Model," *Journal of Computational Science*, vol. 25, pp. 152–160, 2018.

8. N. Zhang, W. Chen, X. He, and Z. Zhang, "A Survey on Security and Privacy Issues in Artificial Intelligence," in *IEEE Access*, vol. 9, pp. 86135–86145, 2021.

9. CICIDS 2017 Dataset – Canadian Institute for Cybersecurity

10. NSL-KDD Dataset for Network-Based Intrusion Detection Systems