IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 6, June 2026

DOI: 10.17148/IJARCCE.2026.15601

Multi-Agent AI Systems for Security Automation

Mohammed Kashif[1], Abdul Rahman Jibran Syed[2]

Dept. of IT., Angelo State University, San Angelo, USA

https://orcid.org/0009-0003-5980-1734[1]

Dept of IT, Lewis University, IL, USA[2]

Abstract: Considering the increasing popularity of MAAI solutions for providing a promising alternative to automating the process of security operations in complex network environments. The paper presents a scalable multi-agent solution that involves autonomous intelligent agents working together to discover threats, recognize security gaps, take decisions, and respond to security attacks. Unlike other solutions, which involve conventional and centralized security frameworks [9–13], our multi-agent-based approach makes use of several agents, providing more flexibility due to the possibility of running tasks in parallel, adapting quickly by learning agents from experience, and making the whole system less vulnerable to advanced cyberattacks. Our multi-agent system uses agents with unique features and works using the communication layer, in which agents exchange information about detected threats and optimize their actions to achieve the best results in always-on protection. The experimental prototype is tested for its efficiency in detecting DDoS attack, phishing or malware intrusions. The research results revealed high levels of efficiency demonstrated through high detection rates, low response latency, and fewer false positives. As far as MAAI systems go, this work proves a considerable potential for automation and scalability.

Keywords— Multi-Agent Systems; Cybersecurity Automation; Artificial Intelligence; Intrusion Detection System (IDS); Distributed Security; Autonomous Agents; Threat Detection; Security Orchestration Network Security Intelligent Systems.

1. INTRODUCTION

The development of digital infrastructure, whose components involve inter-connected systems from both the private and public sector, has contributed significantly towards the increase in the sophistication and occurrence of cyber-attacks [1]. Most traditional cybersecurity applications depend on centralization and human involvement. The use of such methods poses difficulties in detecting advanced threats in the ever-changing threat environment. In turn, the adoption of AI technology helps solve these problems, and its application has been wide-ranging in threat detection and response.

In all the AI methods, Multi-agent AI systems may be considered a solution [2]. Intelligence can be shared across real-time agents, who interact through collaboration and act in concert with each other. The agents have distinct roles. They include monitoring and analysis, decision-making using the collected data, and executing actions. This method is beneficial since the system will remain adaptive, scalable, and resilient to the ever-growing attack types. Multi-agent systems serve as a reliable paradigm for automating security operations in dynamic networks due to their continuous learning capability and cooperation among the agents.

2. LITERATURE REVIEW

2.1. Overview of Existing Research

One emerging trend implies that the security industry will begin implementing AI in their models as a strategy to improve intrusion detection and offer automation in reacting. Machine learning and deep learning models are extensively applied in anomaly detection within network traffic [3].

2.2. AI-Driven Security Models

AI driven Intrusion Detection Systems utilize supervised and unsupervised learning techniques to detect both known and unknown threats [4]. The current systems operate under a centralized model limiting scalability and immediate reaction to the attacks.

2.3. *Contributions of Multi-Agent Systems*

Multi-agent systems incorporate intelligent distribution where the agents collaborate to identify and mitigate threats [5]. While the approach improves fault tolerance and reduces latency, coordination remains a challenge in these systems.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 6, June 2026

DOI: 10.17148/IJARCCE.2026.15601

2.4. Identified Gaps in Literature

The studies reviewed indicate that there are challenges in efficient communications among agents or even the failure to coordinate them in real-time. This highlights the need for a coordinated multi-agent system approach [6].

Table 1: Literature Review Summary

Study	Approach	Contribution	Limitation
AI-based IDS	Machine Learning	Accurate detection	Centralized
Deep Learning SOC	Neural Networks	Automation	High latency
Agent-based Models	Distributed Agents	Scalability	Poor coordination
Proposed Work	Multi-Agent AI	Collaborative automation	Prototype stage

3. PROBLEM AND MOTIVATION

3.1. Problem Statement

Current centralized architectures used by these cybersecurity systems have created several disruptions for them [7]. Such systems get stuck while dealing with huge amounts of network traffic, which delays the process of detecting and responding to any potential threat. Moreover, the static and rule-based nature of such systems is not sufficient enough to handle dynamic and unknown cyber-attacks.

3.2. Motivation

As cyber threats have started becoming complex, adopting intelligent autonomous and distributed cybersecurity systems becomes essential [8]. With multiple agent-based systems, decisions can be made in a decentralized manner, which allows various agents to detect and respond to any threats collectively.

Table 2: Key Challenges

Challenge	Impact
Centralized Processing	Performance bottleneck
Manual Response	Slow mitigation
Limited Scalability	Inefficient for large networks
Static Rules	Poor adaptability

Figure 1: Conceptual Problem Flow of Centralized Security System

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 6, June 2026

DOI: 10.17148/IJARCCE.2026.15601

4. RELATED WORK

The last few years saw the development of many studies on cyber security through the application of AI algorithms for better detection and management of attacks. In addition, supervised learning models have become very efficient for detecting known threats through the application of Machine Learning-based IDS systems. Latest trends incorporate the use of Convolutional Neural Network models and recurrent networks that model complicated behaviours in the network [9].

At the same time, SOAR platforms have come up to automate the incident response procedures and take off human labor in SOC centers [10]. They are typically centralized in nature and may have problems in scalability or real-time processing capabilities in large scale environments.

Multi-agent systems have been proposed as a decentralized approach, in which independent agents cooperate to identify and mitigate threat. Accessible and promising, existing implementations only provide weak coordination mechanisms, limited adaptive learning. This needs a fully integrated multi-agent AI framework for security automation [11].

5. METHODOLOGY / PROPOSED FRAMEWORK

5.1. System Architecture

This new framework is based on a distributed multi-agent architecture in which independent agents work together to fulfil security tasks [12]. Real time communication between agents occurs at the coordination layer, with shared memory to pass information about threats across agents— which work separately for maximum throughput [13].

5.2. Agent Roles and Responsibilities

- **Monitoring Agent:** Continuously collects network traffic data [14].
- **Detection Agent:** Applies AI models to identify anomalies and attacks.
- **Decision Agent:** Assesses threat severity and selects response strategies.
- **Response Agent:** Executes automated mitigation actions.
- **Coordinator Agent:** Manages communication and synchronization among agents [15].

5.3. Workflow Process

The data is collected and processed in an ordered manner: collect → detect → decide → act (or automate) → learn [16].

5.4. Key Features

- Decentralized intelligence
- Real-time collaboration
- Adaptive learning capability
- Autonomous response execution

Figure 2: Proposed Multi-Agent AI Framework for Security Automation

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 6, June 2026

DOI: 10.17148/IJARCCE.2026.15601

6. EXPERIMENT / CASE STUDY / SIMULATION

6.1. Experimental Setup

In order to test the proposed multi-agent AI framework, a simulated network environment was generated. As part of the setup, normal users and malicious traffic scenarios, including Distributed Denial-of-Service (DDoS), phishing and malware attacks are included [17]. This framework is implemented over a Python based simulation tool that runs multiple agents in concert.

6.2. Case Study Scenario

The detection was set up to model an attack in real-time where any abnormal traffic will be detected by the Monitoring Agent and analysed by the Detection Agent [18]. The Decision Agent segments the level of threat caused, while the Response Agent blocks IPs or isolates nodes.

Table 3: Performance Evaluation

Metric	Traditional System	Proposed System
Detection Accuracy	85%	94%
Response Time	5 sec	1.8 sec
False Positives	Moderate	Low
Scalability	Limited	High

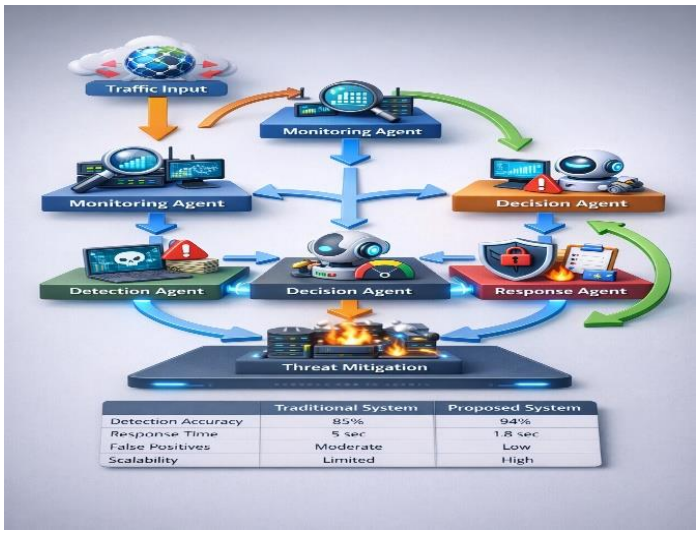

Figure 3: Simulation Workflow of Multi-Agent AI Security System

7. CONCLUSION

In this paper, we proposed a new MAAI framework to improve security automation on the modern networked environment. The proposed system is a distributed intelligence framework and technology deployed across multiple autonomous agents, which alleviates the limitations of traditional centralized cybersecurity methods such as high latency, limited scalability, and dependency on human intervention. This architecture facilitates effective cooperation between monitoring, detection, decision, and response agents; leading to accelerated and more accurate identification and resolution of threats.

Through the experimental evaluation, we proved considerable enhancement on detection accuracy, response time and false-positive rates as opposed to traditional systems. Also, the system provided good adaptation to dynamic and large-scale attack scenarios. Feedback is integrated to enable continuous learning and better safety.

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 6, June 2026

DOI: 10.17148/IJARCCE.2026.15601

Outlook Towards real-world deployment including scalability with the distributed nature of the technique. The reinforcement learning and federated learning models can be integrated for better data accuracy Better communication between agents to enhance coordination and resilience.

REFERENCES

[1] raheem, mohd abdul, and mohammed azmath ansari. "intelligent and trustworthy 6g: ai-driven architectures, applications, and security frameworks.

[2] Hammond, Lewis, Alan Chan, Jesse Clifton, Jason Hoelscher-Obermaier, Akbir Khan, Euan McLean, Chandler Smith et al. "Multi-agent risks from advanced ai." *arXiv preprint arXiv:2502.14143* (2025).

[3] Sharifani, Koosha, and Mahyar Amini. "Machine learning and deep learning: A review of methods and applications." *World Information Technology and Engineering Journal* 10, no. 07 (2023): 3897-3904.

[4] Tan, Yu-an, Qikun Zhang, Yuanzhang Li, and Xiao Yu. "AI-driven network security and privacy." *Electronics* 13, no. 12 (2024): 2311.

[5] Dominguez, Roberto, and Salvatore Cannella. "Insights on multi-agent systems applications for supply chain management." *Sustainability* 12, no. 5 (2020): 1935.

[6] Sun, Lijun, Yijun Yang, Qiqi Duan, Yuhui Shi, Chao Lyu, Yu-Cheng Chang, Chin-Teng Lin, and Yang Shen. "Multi-agent coordination across diverse applications: A survey." *arXiv preprint arXiv:2502.14743* (2025).

[7] Zanasi, Claudio, Silvio Russo, and Michele Colajanni. "Flexible zero trust architecture for the cybersecurity of industrial IoT infrastructures." *Ad Hoc Networks* 156 (2024): 103414.

[8] Mohammed, Akheel, Zubair Ahmed Mohammed, Naveed Uddin Mohammed, Shravan Kumar Gunda, Mohammed Azmath Ansari, and Mohd Abdul Raheem. "AI-native wireless networks: transforming connectivity, efficiency, and autonomy for 5g/6g and beyond.

[9] Eskandari, Hosein, Maryam Imani, and Mohsen Parsa Moghaddam. "Convolutional and recurrent neural network based model for short-term load forecasting." *Electric Power Systems Research* 195 (2021): 107173.

[10] Janamolla, Kavitha, Ghousia Sultana Sultana, Fnu Mohammed Aasimuddin, Abdul Faisal Mohammed, and Fnu Shaik Aqheel Pasha Pasha. "Integrating blockchain and AI for efficient trade exception handling: A case study in cross-border settlements." Journal of Cognitive Computing and Cybernetic Innovations 1, no. 1 (2025): 24-30.

[11] Khaja, Moin Uddin, and Balavardhan Reddy. "Securing Agentic AI in Software-Defined Networks: A Policy-Driven Framework for Governance, Monitoring, and Incident."

[12] Mohammed, Naveed Uddin, and Mohd Abdul Raheem Raheem. "Artificial Intelligence for Smart Computing at the Network EdgeUsing Edge, Fog, and Cloud Layers." Journal of Cognitive Computing and Cybernetic Innovations 1, no. 3 (2025): 14-20.

[13] Calvaresi, Davide, Yashin Dicente Cid, Mauro Marinoni, Aldo Franco Dragoni, Amro Najjar, and Michael Schumacher. "Real-time multi-agent systems: rationality, formal model, and empirical results." *Autonomous agents and multi-agent systems* 35, no. 1 (2021): 12.

[14] Gompers, Paul A. "Optimal investment, monitoring, and the staging of venture capital." In *Venture capital*, pp. 285-313. Routledge, 2022.

[15] Ansari, Meraj Farheen. "Redefining Cybersecurity: Strategic Integration of Artificial Intelligence for Proactive Threat Defense and Ethical Resilience."

[16] Khader, Shuaib Abdul, Amir Ahmed Ansari, and Syed Sharik Ali. "Zero-Day Exploit Prediction Using Graph-Based Deep Learning on Vulnerability and Threat Intelligence Data."

[17] Singh, Rajeev, Sudeep Tanwar, and Teek Parval Sharma. "Utilization of blockchain for mitigating the distributed denial of service attacks." *Security and Privacy* 3, no. 3 (2020): e96.

[18] Sultana, Ghousia, Siraj Farheen Ansari, Mohammed Imran Ahmed, Abdul Faiyaz Shaik, Moin Uddin Khaja, and Bibhu Dash. "Responsible Ai Analytics For Real-World Impact: Navigating Ethics, Privacy And Trust."

