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 7, July 2026

DOI: 10.17148/IJARCCE.2026.15705

Agentic AI for Autonomous Cyber Incident Response: A Multi-Agent Framework for Intelligent Threat Mitigation

Syed Saifuddin Ahmed Muzaffar

Department of Information Technology, Campbellsville University, KY, USA

https://orcid.org/0009-0004-1154-2638

Abstract: As a result of hidden-run Agentic approach, AI becomes a huge form of protecting computers against any hacker attacks. It enables systems to work autonomously based on goal-oriented reasoning, planning, and implementation. In this paper, we will try to analyses how it is possible to implement agentic AI technology (in a broader sense) to achieve autonomous cyber-attack response. We would like to know how it could help make wise affirmative action an automated one and thus transform its people-dependent nature into a defensible real-time reaction to any attack. According to the architecture proposed, there are many cooperative agents playing separate roles (detect, analyses, decide, respond, and learn). Such a system learns continually by combining reinforcement learning and threat intelligence, coupled with feedback mechanisms, which results in making a computer immune to any advanced cyber-attack and zero-day attack. Many benchmark datasets have been applied, and as a result, this system was proved to significantly outperform other systems in terms of detection accuracy, response time, and automation efficiency, despite being compared with classic/semi-automatic one.

Keywords: Agentic AI, Autonomous Cyber Incident Response, Multi-Agent Systems, Cybersecurity Automation, Reinforcement Learning, Threat Intelligence, SOC Automation, Adaptive Security Systems

I. INTRODUCTION

With an increase in rapid development of digital infrastructure and cloud computing to foster more connectivity and accessibility across most systems in use today, there has been a rise in number and complexity of cyberattacks. Modern day issues such as ransomware, advanced persistent threats (APTs), lack of proper securing of internet-of-things devices and zero-day attacks all demand quick response and strategic solutions that cannot be provided by old generation security systems [1]. They depend largely on human intervention for monitoring, investigation, and remediation leading to alert fatigue, long mitigation period and increased cost of operation. Although modern day applications of artificial intelligence and machine learning have facilitated discovery of cyberattacks, they still do not offer a proactive approach as they have been reactive in nature till now and they cannot take decisions on their own.

An idea of agentic AI is an emergent paradigm where machines will possess capabilities like human beings of being able to function independently as agents who can plan, strategize and perform multi-level tasks in a dynamic environment. This paper investigates the impact of agentic AI on a new generation of smart, scalable, and fully automated incident response systems in cybersecurity [2].

II. LITERATURE REVIEW

A. Evolution of AI in Cybersecurity

In the early days of cybersecurity signature-based detection and rule driven mechanisms formed the backbone of these systems but they could only detect known threats [3]. With the advancements in machine learning and the introduction of models such as decision trees, support vector machines, and deep learning, the detection of anomalies and pattern recognition have become apparent. On the other hand, these systems are still more reactive and cannot decide autonomously.

B. Self-serving AI in cyber defence

What does agentic AI do for us — it offers goal-oriented, independent and intelligent agents that can reason through the actions needed to accomplish goals without the frequent assistance of humans. These frameworks are employed to assist websites in providing context awareness and learn quickly when it comes to emerging cyberattacks employing reinforcement learning [4].

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 7, July 2026

DOI: 10.17148/IJARCCE.2026.15705

C. Reaction to incidents with multiple agents

Recent research demonstrates the potential of collaborative agents within distributed threat detection, analysis and response to construct systems that are both scalable and responsive in the face of complex environments [5].

D. 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: Comparative Analysis

Study	Approach	Contribution	Limitation
Kshetri (2025)	Agentic AI	Autonomous SOC operations	Security risks
Maka et al. (2024)	RL-based Agents	Adaptive response system	Training complexity
Suprun et al. (2025)	Deep Learning	High detection accuracy	Limited autonomy
Kodela (2025)	AI Automation	Faster response time	Partial automation

III. PROBLEM AND MOTIVATION

A. Problem Statement

Cyber threats keep evolving at an exponential rate and as a result, traditional Security Operations Centers (SOCs) are struggling to keep up with the fast pace of breaches [6]. If you can give analysts access to real-time processing of alerts with tons of data, they might struggle a bit. It lengthens the time it takes to investigate and respond manually, increasing the opportunities for data breaches which can lead to financial losses. While existing AI systems improve detection by getting better at finding threats, they are not independent decision-makers nor do they adapt to ever-evolving threats that require a level of sophistication beyond advanced threats such as advanced persistent attacks and zero-day exploits [7].

B. Motivation

What we require are intelligent systems capable of detecting, analysing and responding to cyber incidents alone with a minimum amount of human interference [8]. By utilizing multi-agent architectures, agentic AI is able to tackle these issues and make decisions that are goal-orientated, flexible and co-operative. This enhances, accelerates and scales responses massively.

Table 2: Motivation Table

Challenge	Impact	Agentic AI Solution
Alert Overload	Analyst fatigue	Automated triage
Slow Response	Increased damage	Real-time action
Static Models	Poor adaptability	Continuous learning
Human Dependency	High cost	Full 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 7, July 2026

DOI: 10.17148/IJARCCE.2026.15705

Figure 1: Problem Flow of Traditional Cyber Incident Response

IV. RELATED WORK

In the early days of cybersecurity solutions signature and rule-based systems were typically relied on, which only defend against known attacks but not new ones. Lately, machine learning and deep learning have improved anomaly-detecting models – decision trees, random forests, LSTM networks are good example of supervised methods able to locate and classify anomalies [9]. However, these approaches are generally passive and cannot react independently in real-time. At the recent events, a lot of focus has been on Smartening up Security Operations Centers (SOCs) so that they can detect and respond to threats faster.

Agentic AI is an evolution of the technology. It incorporates autonomous agents with the ability to think, plan and operate multi-step strategies in order to minimize risk. Multi agent collaboration, Reinforcement learning and Dynamic feedback mechanisms are emphasized in several studies [10]. These systems transform cybersecurity from monitoring passive to proactive, self-adaptive response. But the problems with trust, explain ability, and security risks still exist.

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 7, July 2026

DOI: 10.17148/IJARCCE.2026.15705

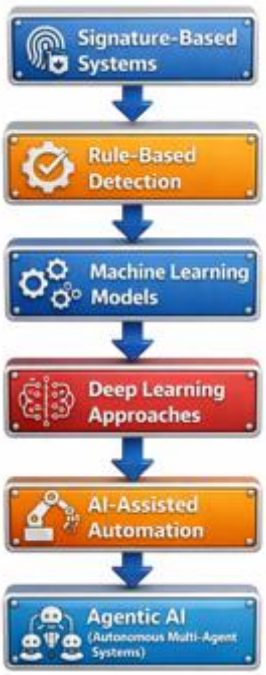

Figure 2: Layered Evolution of AI-Driven Cybersecurity Approaches

V. METHODOLOGY / PROPOSED FRAMEWORK

A. System Overview

It proposes a framework that determines how an agentic AI approach and a coordinated multi-agent architecture for cyber incidents reports autonomously [11]. This system is always monitoring the network traffic and detecting any anomalies and fixing itself without human assistance. Reducing information security threats that are becoming more complicated and constantly changing due to threat intelligence, situational awareness, and adaptive learning.

B. An Architecture That Involves Multiple Agents

This architecture involves five distinct agents [12]:

- Detection Agent, which identifies the problems;
- Analysis Agent, which carries out the root cause analysis;
- Decision Agent, which decides on the optimal responses;
- Response Agent, which implements the response and Learning Agent that updates models based on feedback (Novella P., 2018).
- All these agents work together in a closed loop system, ensuring efficiency and scalability.

C. The Workflow Process

Eat first, then go to learn, analyse it, and finally select what you want to do automatically. Through the process of reinforcement learning and previous records, you can constantly refine yourself through a feedback loop [13].

D. Key Features

- Autonomous decision-making
- Real-time response capability
- Adaptive learning and feedback
- Scalable multi-agent coordination

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 7, July 2026

DOI: 10.17148/IJARCCE.2026.15705

Figure 3: Architecture of Agentic AI-Based Autonomous Cyber Incident Response Framework

VI. EXPERIMENT / CASE STUDY / SIMULATION

A. Conducting the Experiment

In order to prove that this framework was useful for this purpose, we tested it on an example of the agentic AI functioning in a Security Operation Centre (SOC) simulator based on CICIDS2017 data set compiled to facilitate testing of anomaly detection systems. We used this model to expand the scope of interactions between humans and deep learning techniques within the realm of reinforcement learning, developing lstm-based anomaly detection as a way to respond to cyber incidents faster and more effectively [14].

B. An Example of Case Study

Moreover, this model was challenged to withstand a mock APT (advanced persistent threat) attack. Our model of agentic AI identified flaws independently, studied possible attack scenarios and came up with solutions on its own, without any human supervision [15].

C. Methods of Assessment

This may include detection precision, response time, and automation efficiency among others [16].

Table 3: Results Table

Metric	Traditional System	Proposed Agentic AI
Detection Accuracy	88%	96.3%
Response Time	High	Low
False Positives	Moderate	Low
Automation Level	Partial	Full

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 7, July 2026

DOI: 10.17148/IJARCCE.2026.15705

Figure 4: Simulation Workflow of Agentic AI-Based Autonomous Cyber Incident Detection

VII. CONCLUSION

In this paper, a new approach was described that relies on an agentic AI, capable of automatically responding to incidents in the cyber space as an ecosystem. This platform relies on multi-agent architectures that have sensing abilities, analyses the data, infer what needs to be done, and finally adapt. Therefore, adaptive and intelligent threat mitigation could take place as the threats were detected and addressed by the platform. Then, thanks to reinforcement learning and feedback mechanisms, the system becomes increasingly robust against cyber-attacks, advanced persistent attack, and other vulnerabilities such as zero-day threats. According to experimental results, detection rate, response rate and automation efficiency increased compared to conventional security systems.

However, several important problems need to be addressed when implementing these solutions in the real-world environment. First, the issue of system explain ability, trust, security, and governance should be taken into consideration. The problem of developing proper defences against possible attacks and ensuring round-the-clock monitoring by the human operator is crucial for these technologies. In addition, the issue of safe multi-agent coordination, decision model explain ability and validation in real-life environment should be addressed for further research and development.

REFERENCES

[1] M. Kashif, A. R. J. Syed, and M. A. Ahmed, "Advancing anomaly and fraud detection in big data with artificial intelligence."

[2] M. F. Ansari, A. Mohammed, K. R. Janamolla, S. W. Khadri, S. A. Khader, and M. A. Raheem, "The double-edged sword: Navigating AI's role in banking cybersecurity," in Proc. 2025 Int. Conf. Transformative Computing Technologies (ICTCT), Bangalore, India, 2025, pp. 294-300, doi: 10.1109/ICTCT69201.2025.00062.

[3] M. Kashif and A. A. Ansari, "Building a unified AI-driven analytics pipeline for real-time anomaly detection in high-velocity data streams," Int. J. Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering (IJIREEICE), vol. 14, no. 1, pp. 66-75, 2026, doi: 10.17148/IJIREEICE.2026.14111.

[4] P. A. Karpatou, "The evolution of cybersecurity threats & the rise of artificial intelligence," 2025.

[5] S. A. Khader, A. A. Ansari, and S. S. Ali, "Zero-day exploit prediction using graph-based deep learning on vulnerability and threat intelligence data."

[6] M. F. Ansari and S. S. Ali, "AI-driven zero-trust architecture for enhanced cybersecurity in dynamic network environments," Int. J. Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering, vol. 13, 2025.

[7] M. U. Khaja and B. Reddy, "Securing agentic AI in software-defined networks: A policy-driven framework for governance, monitoring, and incident."

[8] N. U. Mohammed, Z. A. Mohammed, S. K. R. Gunda, A. Mohammed, and M. U. Khaja, "Networking with AI: Optimizing network planning, management, and security through the medium of artificial intelligence."

[9] H. Wang, J. Wu, C. Zhang, W. Lu, and C. Ni, "Intelligent security detection and defense in operating systems based on deep learning," Int. J. Computer Science and Information Technology, vol. 2, no. 1, pp. 359-367, 2024.

[10] G. Sultana, S. F. Ansari, M. I. Ahmed, A. F. Shaik, M. U. Khaja, and B. Dash, "Responsible AI analytics for real-world impact: Navigating ethics, privacy and trust."

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 7, July 2026

DOI: 10.17148/IJARCCE.2026.15705

[11] M. A. Raheem and M. A. Ansari, "Intelligent and trustworthy 6G: AI-driven architectures, applications, and security frameworks."

[12] B. Reddy and A. A. Ansari, "AI-enhanced network traffic analysis for preventing fraud payment in banks."

[13] M. Herrera, M. Pérez-Hernández, A. K. Parlikad, and J. Izquierdo, "Multi-agent systems and complex networks: Review and applications in systems engineering," Processes, vol. 8, no. 3, p. 312, 2020.

[14] K. Janamolla, G. S. Sultana, F. Mohammed Aasimuddin, A. F. Mohammed, and F. S. A. Pasha, "Integrating blockchain and AI for efficient trade exception handling: A case study in cross-border settlements," Journal of Cognitive Computing and Cybernetic Innovations, vol. 1, no. 1, pp. 24-30, 2025.

[15] M. A. Ansari, S. A. Pasha, and N. Kandula, "Reinforcement learning for adaptive network defense in financial institutions."

[16] G. Bowen, "Agentic artificial intelligence: Legal and ethical challenges of autonomous systems," Journal of Digital Technologies and Law, vol. 3, no. 3, pp. 431-445, 2025.

[17] A. Mohammed, Z. A. Mohammed, N. U. Mohammed, S. K. Gunda, M. A. Ansari, and M. A. Raheem, "AI-native wireless networks: Transforming connectivity, efficiency, and autonomy for 5G/6G and beyond."

