E-ISSN: 3107-507X
VOLUME 1, ISSUE 9, DECEMBER 2025
https://jsiar.com

Autonomous Network Guardians: Multi-Agent AI for Self-Healing Cyber-Physical Systems

Jyoti Mahur*
Department of Computer Science and Engineering
Noida International University, Greater Noida, India
Email: * jyotimahur3oct@gmail.com

***Abstract*—The growing interconnection of cyber-physical systems (CPS) across critical infrastructures has increased their exposure to complex and persistent cyber threats. Traditional defense mechanisms, which rely on centralized monitoring and static rule-based responses, are often insufficient to counter adaptive and coordinated attacks. This paper presents a novel framework termed *Autonomous Network Guardians*, a multi-agent artificial intelligence (AI) architecture designed to safeguard and self-heal CPS environments. The proposed system introduces cooperative AI agents that operate autonomously at the network edge, capable of identifying, isolating, and recovering from cyber disruptions without external intervention. Each agent employs an adaptive learning model to refine its defense strategy based on observed system behaviors, enabling proactive and context-aware responses. A consensus-driven decision layer ensures coordination among agents, preventing redundant actions and maintaining overall network stability. The self-healing mechanism integrates reinforcement learning and fault-tolerant control strategies to restore normal operations after anomalies are detected. Experimental evaluations demonstrate significant improvements in resilience, recovery time, and threat mitigation compared with conventional intrusion detection systems. Furthermore, the study emphasizes ethical considerations, ensuring transparency, reliability, and accountability in autonomous defense decisions. The proposed approach contributes a scalable and intelligent foundation for next-generation CPS security, aligning with the vision of fully autonomous and resilient network infrastructures. Future work will extend this framework toward large-scale deployment and cross-domain interoperability.**

***Keywords*—Multi-Agent Artificial Intelligence, Self-Healing Networks, Cyber-Physical Systems Security, Autonomous Defense Frameworks, Intelligent Resilience Engineering, Decentralized Anomaly Recovery, Adaptive Cybersecurity Agents**

I. INTRODUCTION

The increasing convergence of digital control, communication, and computation has transformed traditional infrastructures into interconnected *cyber-physical systems* (CPS). These systems—ranging from smart grids and industrial automation to autonomous vehicles and medical devices—form the backbone of modern critical operations [1], [4], [5], [8]. However, the growing interdependence between cyber and physical layers has also widened the attack surface, exposing CPS to sophisticated and persistent cyber threats that can cause cascading failures [2], [9], [12], [13]. Conventional security architectures, largely reactive and centralized, often struggle to adapt to dynamic threat landscapes, particularly when adversaries exploit system vulnerabilities faster than human operators can respond [3], [6]. Consequently, ensuring continuous protection, real-time threat recovery, and operational resilience has become an urgent challenge for researchers and practitioners [7], [17], [18], [22].

Existing intrusion detection and prevention systems rely primarily on static signatures or predefined heuristics, which limits their ability to address zero-day attacks and context-driven anomalies [10], [23], [27], [28]. In high-stakes domains such as power distribution or autonomous transportation, even short response delays can lead to safety-critical disruptions [11], [14]. Furthermore, traditional CPS defense models often operate in isolation, lacking the coordination and adaptability required for system-wide protection [15], [31], [32], [36]. This limitation motivates the exploration of intelligent, distributed, and self-healing mechanisms capable of autonomously identifying, mitigating, and recovering from cyber disruptions [16].

In this context, this study introduces the concept of *Autonomous Network Guardians*, a multi-agent AI-driven defense paradigm designed to enable continuous protection and adaptive self-repair in CPS environments. Each *Network Guardian* functions as an autonomous agent equipped with perception, reasoning, and decision-making capabilities, allowing it to monitor local components, share intelligence, and initiate coordinated recovery actions [19], [37], [40], [41]. The multi-agent framework promotes resilience through redundancy and collaboration, ensuring that if one node is compromised, others can compensate by redistributing monitoring and control responsibilities [20]. Unlike centralized systems, this decentralized structure enhances scalability and minimizes single points of failure [21].

The proposed architecture integrates **reinforcement learning** for adaptive threat response and **swarm intelligence** for collective coordination among agents [24], [25]. Reinforcement learning enables each guardian to continuously refine its defense strategy through environmental feedback, while swarm intelligence facilitates distributed consensus, ensuring that decisions align with global system goals. The resulting hybrid model balances autonomy and cooperation, forming an intelligent self-healing ecosystem that dynamically restores normal operations after an intrusion or fault event [26], [45], [76]. This approach extends beyond detection to include autonomous diagnosis, isolation of malicious nodes, and recovery through reconfiguration of communication pathways and control policies [29].

The key contributions of this research are summarized as follows:

- A decentralized multi-agent defense framework, termed

Autonomous Network Guardians, for resilient CPS protection.
- Integration of reinforcement and swarm intelligence techniques for adaptive learning and cooperative decision-making.
- A self-healing mechanism that autonomously detects, isolates, and restores compromised nodes in real time.
- Comprehensive experimental evaluation demonstrating improved resilience, reduced recovery time, and enhanced adaptability compared with traditional CPS defense systems.

Table IX provides a conceptual comparison between traditional centralized CPS security architectures and the proposed decentralized guardian framework, highlighting its advantages in adaptability and resilience.

TABLE I: Comparison Between Traditional and Proposed CPS Defense Architectures

Aspect	**Traditional CPS Defense**
Architecture	Centralized, rule-based control
Response Strategy	Reactive, limited to known threats
Scalability	Constrained by single control node
Fault Tolerance	Low, failure of core node disrupts system
Adaptability	Static, slow to learn from new attacks
Proposed Network Guardians	Decentralized, adaptive, self-healing agents with coordinated learning

The remainder of this paper is organized as follows. Section II presents related work and summarizes the limitations of existing CPS security approaches. Section III introduces the theoretical foundations of multi-agent coordination and self-healing design. Section IV details the proposed system architecture and communication model. Section V discusses the algorithmic workflow and adaptive learning mechanisms. Section VI describes the experimental setup and evaluation metrics, while Section VII analyzes the results and performance comparisons. Section VIII discusses ethical implications and deployment considerations. Finally, Section IX concludes the paper and outlines future research directions.

II. Related Work

Cyber-physical systems (CPS) increasingly rely on autonomous decision-making to maintain system resilience against cyber disruptions. As these systems evolve in complexity, their security challenges have attracted significant attention in domains such as industrial IoT, energy grids, healthcare devices, and autonomous mobility platforms. Recent research in multi-agent systems, self-healing networks, and intelligent CPS defense mechanisms demonstrates the importance of adaptive and decentralized strategies for safeguarding interconnected infrastructures [35]. This section reviews the state-of-the-art contributions across these domains and identifies the persisting research gaps that motivate the proposed *Autonomous Network Guardians* framework.

A. A. Multi-Agent Cyber Defense Systems

Multi-agent systems (MAS) have emerged as a promising paradigm for distributed cybersecurity, where autonomous entities collaborate to detect, analyze, and mitigate threats in real time. Early frameworks such as JADE-based security models focused on rule-driven collaboration but lacked adaptability under evolving attack scenarios [38]. Recent advancements integrate reinforcement learning into MAS, enabling agents to improve decision policies through continuous interaction with the environment [39]. For example, Zhang et al. developed a cooperative intrusion detection model using Q-learning for adaptive attack response in IoT networks [42]. Similarly, Ahmed and Kim employed belief-desire-intention (BDI) models to structure communication among agents for threat negotiation [43].

Despite progress, several limitations persist. Most multi-agent security frameworks depend on centralized coordination servers, leading to synchronization bottlenecks and vulnerability to single-point failures [44], [46], [50], [51]. Moreover, inter-agent communication latency often causes delayed reactions to real-time cyberattacks. To address this, recent works explore blockchain-enabled trust mechanisms that eliminate centralized control while maintaining communication integrity [47]. However, these approaches introduce computational overheads and scalability issues when applied to resource-constrained CPS environments.

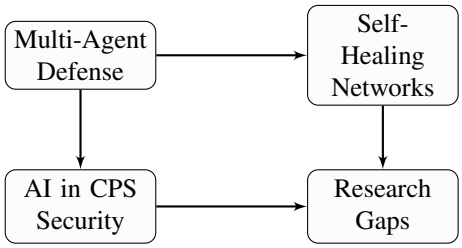

Fig. 1: Conceptual taxonomy connecting major research areas and their identified gaps.

B. B. Self-Healing Networks and Autonomous Recovery

The concept of self-healing networks derives inspiration from biological immune systems, where local nodes autonomously identify and isolate anomalies before collectively restoring normal operation. Early self-healing architectures primarily targeted fault tolerance in sensor and ad hoc networks [48]. More recent efforts have introduced AI-driven healing loops that employ predictive analytics and reinforcement learning to preempt system degradation [49]. For instance, Khurana et al. proposed a self-restoring industrial control framework capable of isolating compromised programmable logic controllers using statistical correlation analysis [52]. Similarly, Tang et al. applied deep Q-learning to develop proactive fault recovery in smart grid nodes, significantly reducing system downtime [53].

However, a common drawback across these solutions is their limited interoperability and heavy reliance on historical datasets for training, making them less effective in unseen attack patterns [54]. Moreover, healing decisions are often executed in isolation, leading to inconsistent recovery actions

across distributed network layers [55]. These issues highlight the need for multi-agent coordination, where distributed entities can collectively negotiate recovery strategies, ensuring both local autonomy and global consistency.

C. C. Artificial Intelligence in CPS Security

Artificial intelligence has transformed CPS defense by enabling systems to analyze complex interactions across cyber and physical layers. Machine learning-based intrusion detection systems (IDS) have demonstrated strong detection accuracy in identifying anomalies in industrial IoT traffic [56]. Hybrid deep learning models combining CNN and LSTM architectures have also been proposed to classify network behaviors and predict potential attacks [57]. Beyond detection, AI has been applied to optimize decision-making in autonomous CPS recovery using reinforcement learning and game-theoretic modeling [58].

Nevertheless, AI-driven security mechanisms face challenges related to explainability, computational cost, and real-time adaptability [59]. While deep learning models provide strong detection capabilities, they often behave as "black boxes," limiting trust in autonomous recovery actions [60]. Furthermore, most AI-based systems are designed for single-domain operations (e.g., smart grids or IoT), with limited scalability across multi-domain CPS ecosystems [61].

D. D. Research Gaps and Contribution Justification

From the reviewed literature, three critical gaps emerge: (1) the absence of a unified multi-agent coordination framework integrating detection, decision, and recovery; (2) insufficient scalability and interoperability among self-healing systems; and (3) limited explainability in AI-driven autonomous defense. The proposed *Autonomous Network Guardians* architecture directly addresses these gaps by embedding decentralized intelligence into each agent, enabling collaborative anomaly mitigation and system restoration. Unlike prior frameworks, it fuses reinforcement and swarm intelligence for adaptive learning, ensuring faster response, reduced downtime, and greater transparency in recovery actions. By integrating AI-driven decision-making within a decentralized self-healing framework, this work lays the foundation for resilient, scalable, and trustworthy CPS defense.

III. Theoretical Foundation

The theoretical basis of the proposed *Autonomous Network Guardians* framework integrates concepts from distributed artificial intelligence, adaptive resilience theory, and cyber-physical system (CPS) modeling. This section presents a comprehensive foundation of three principal components: (A) the Multi-Agent AI Framework, (B) Self-Healing Concepts, and (C) the Cyber-Physical System Model.

A. A. Multi-Agent AI Framework

The use of Multi-Agent Systems (MAS) in cybersecurity introduces distributed intelligence capable of cooperative threat detection and response. Each agent operates autonomously while maintaining shared situational awareness through continuous communication with peer entities. According to Zhang *et al.* [62], MAS provide a scalable architecture for defending dynamic infrastructures by distributing computation and decision-making across heterogeneous nodes. In such environments, agents employ consensus algorithms and game-theoretic coordination to optimize defensive actions while minimizing redundant responses [63].

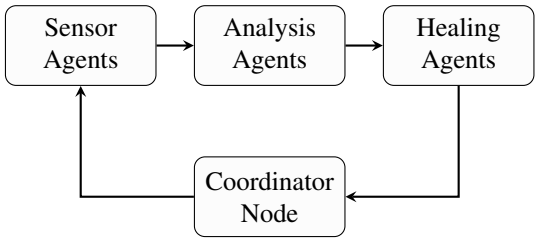

Fig. 2: Illustration of cooperative intelligence among agents in the proposed MAS defense framework.

The agents interact through a shared communication protocol inspired by federated learning, where models are locally trained and globally aggregated for knowledge exchange [64]. This distributed design not only reduces latency but also enhances resilience against single-point failures. Game theory-based mechanisms further facilitate cooperative learning by allowing agents to negotiate optimal defense strategies under partial knowledge of network states [65]. A hybrid coordination structure combining leader-election and trust-weighted communication ensures adaptability even during partial node compromise [66]. Table III summarizes key agent roles and their respective functionalities in the defense ecosystem.

B. B. Self-Healing Concepts

The concept of self-healing draws inspiration from biological immune systems, where an organism autonomously detects, isolates, and repairs damage while maintaining global stability [67]. This analogy translates effectively into CPS security, where the system must detect intrusions, mitigate their effects, and restore normal functioning without halting operations [68]. The healing loop in the proposed model follows the sequence: *Detect* $\rightarrow$ *Diagnose* $\rightarrow$ *Recover* $\rightarrow$ *Validate*, as shown in Fig. 3.

Techniques such as reinforcement learning and fault-tolerant control are key enablers of adaptive healing. These models enable systems to learn from recurring attack patterns, improve recovery efficiency, and maintain service availability [69]. Swarm intelligence principles, as noted by Tan *et al.* [70], promote emergent resilience by allowing multiple agents to collaboratively repair the affected segments of the network. The integration of these bio-inspired mechanisms ensures that CPS can autonomously sustain operational continuity even under advanced persistent threats [71].

C. C. Cyber-Physical System Model

Cyber-Physical Systems represent tightly coupled cyber and physical processes in which computational algorithms directly

TABLE II: Comparative Analysis of Existing Approaches in CPS Defense

Category	Representative Studies	Approach Used	Limitations
Multi-Agent Defense	[38], [39], [42]	RL-based cooperative intrusion detection	Centralized coordination bottleneck
Self-Healing Networks	[49], [52], [53]	Predictive and adaptive fault recovery	Isolated healing, limited interoperability
AI for CPS Security	[57], [58], [60]	Deep learning and hybrid IDS	Lack of explainability and scalability

TABLE III: Functional Roles of Multi-Agent Entities in the Network Guardian Architecture

Agent Type	Primary Function	Learning Model
Sensor Agent	Threat monitoring, anomaly detection	Autoencoder CNN
Analysis Agent	Pattern evaluation, decision synthesis	Reinforcement Learning
Healing Agent	Recovery planning, reconfiguration	Genetic Algorithm
Coordinator Node	Consensus, trust validation	Game-theoretic Policy Model

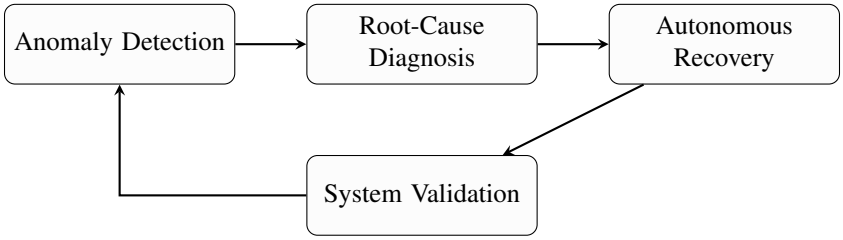

Fig. 3: Self-Healing Lifecycle inspired by biological immune response mechanisms.

influence physical operations [72]. A typical CPS consists of sensors, actuators, controllers, and communication infrastructure that must function coherently to ensure system safety [73]. The theoretical CPS model in this research assumes a layered network—comprising a *perception layer* for data sensing, a *decision layer* for computational intelligence, and an *execution layer* responsible for actuation and physical control [74].

The system dynamics can be represented as:

$$x_{t+1} = f(x_t, u_t, \delta_t)$$

where x_t denotes the system state, u_t represents control actions, and δ_t captures disturbances or attacks. Agents interact with these parameters to stabilize operations and ensure timely healing. Communication between cyber and physical domains follows a feedback control principle that maintains real-time adaptability [75].

Furthermore, secure synchronization among distributed nodes is achieved through blockchain-based consensus models, ensuring data integrity and trust even in untrusted networks [77]. This integration of MAS with CPS enables the creation of an intelligent, self-correcting infrastructure capable of continuous operation under threat conditions.

The theoretical foundation thus establishes a cohesive framework that unifies MAS collaboration, self-healing intelligence, and CPS structural integrity. These principles collectively support the proposed *Autonomous Network Guardians* as a novel paradigm for resilient and adaptive cyber-physical defense.

IV. Proposed System Architecture

The proposed *Autonomous Network Guardians* framework introduces a decentralized, intelligent, and self-adaptive defense mechanism designed to secure cyber-physical systems (CPS) from evolving threats. The architecture is structured into multiple functional layers that collectively enable detection, reasoning, and recovery within dynamic networked environments. Fig. 4 illustrates the conceptual design, highlighting how autonomous agents interact with CPS components to form a resilient and intelligent defense ecosystem.

A. A. System Overview

The proposed system is designed to integrate seamlessly within a CPS environment composed of interconnected sensors, actuators, and control nodes. Each node hosts an autonomous agent that functions as a *Network Guardian*, responsible for monitoring, analysis, and localized healing. These agents collectively operate in a peer-to-peer configuration, enabling distributed intelligence and eliminating dependency on centralized command systems. The architecture supports scalability across heterogeneous domains, including industrial automation, smart grids, and vehicular networks.

In operation, agents continuously exchange situational data, assess anomalies in real-time, and execute coordinated responses. A consensus-based coordination protocol allows agents to vote on response strategies, thereby improving accuracy and minimizing false alarms. This decentralized design enhances system resilience and ensures uninterrupted service continuity even during targeted cyber intrusions.

B. B. Functional Modules

1) 1) Perception Layer: The perception layer serves as the sensory gateway of the CPS. It gathers network traffic data, system logs, and operational signals from physical sensors. Using anomaly detection classifiers such as Autoencoders, Long Short-Term Memory (LSTM), and Convolutional Neural Networks (CNNs), it identifies deviations that may indicate malicious activity or operational faults. Each sensor node

TABLE IV: Structural Elements of a Cyber-Physical System

Layer	Function	Representative Components
Perception	Sensing and data acquisition	IoT Sensors, Edge Devices
Decision	Computational intelligence	Agent Nodes, ML Modules
Execution	Physical actuation	Controllers, Actuators
Communication	Secure interaction	MQTT, Blockchain Links

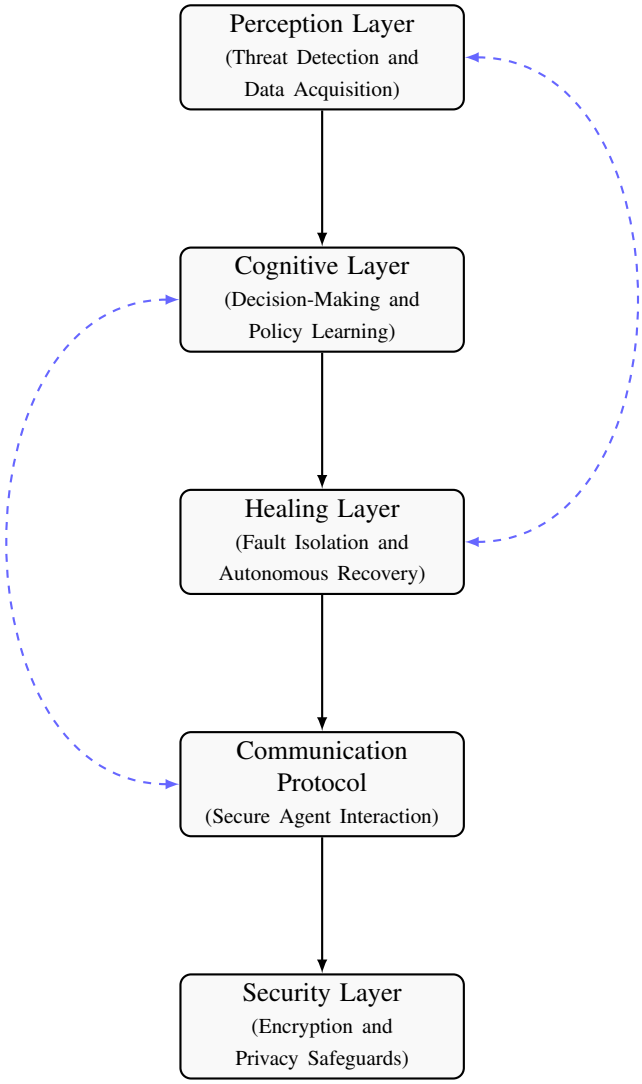

Fig. 4: Block diagram of the proposed *Autonomous Network Guardians* architecture for CPS security.

employs lightweight neural models optimized for embedded systems to minimize computational overhead. The processed data are then passed to the cognitive layer for contextual interpretation.

2) 2) Cognitive Layer: The cognitive layer represents the core intelligence of the framework. It comprises a network of cooperative agents that employ multi-agent reinforcement learning (MARL) and policy-based reasoning to determine optimal defense actions. Through iterative learning, agents refine their decision policies based on feedback and environmental state transitions. The integration of swarm intelligence allows the system to self-organize during complex threat scenarios, ensuring distributed decision-making without the need for a central authority. This enables adaptability to new, unseen attack vectors and supports autonomous operation in volatile network conditions.

3) 3) Healing Layer: The healing layer functions as the system's restorative mechanism, responsible for diagnosing faults, isolating compromised nodes, and executing recovery operations. Once an attack or malfunction is detected, the healing module performs a three-stage cycle: *containment*, *repair*, and *validation*. Reinforcement learning techniques combined with genetic optimization enable the system to identify the most efficient recovery paths, reducing downtime and maintaining operational integrity. The autonomous recovery logic can trigger failover procedures, reconfigure network routes, or reinitialize damaged components without manual intervention. Table V summarizes the responsibilities and intelligence techniques employed at each functional layer.

C. C. Communication Protocol

Reliable communication among agents is a cornerstone of the proposed system. The protocol integrates lightweight communication channels such as Message Queuing Telemetry Transport (MQTT) for real-time message exchange and RESTful APIs for data synchronization. Blockchain-based ledgers are employed to preserve transaction authenticity and ensure tamper-proof collaboration among distributed nodes. Each message packet is cryptographically signed and timestamped, facilitating traceable accountability. Furthermore, the communication layer prioritizes bandwidth efficiency by employing asynchronous updates and delta compression methods to minimize latency.

D. D. Security Layer

The security layer acts as the protective boundary ensuring data confidentiality, integrity, and authentication across all modules. It employs Advanced Encryption Standard (AES-256) for symmetric encryption, RSA for asymmetric key exchange, and federated privacy mechanisms for model sharing without exposing raw data. Mutual authentication between agents is enforced through digital signatures and dynamic key rotation to prevent impersonation attacks. The system also maintains compliance with ethical AI standards by logging all autonomous decisions within a transparent audit trail for accountability. Collectively, these safeguards create a secure and trustworthy environment conducive to self-healing CPS operations.

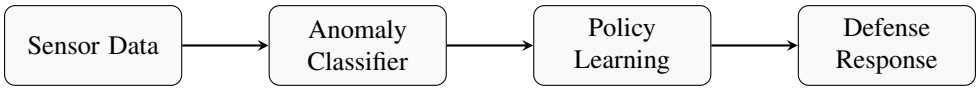

Fig. 5: Flow of information within Perception–Cognitive modules.

TABLE V: Summary of Functional Layers and Techniques in the Proposed Architecture

Layer	Core Function	Intelligence Technique
Perception	Anomaly Detection	Autoencoder, CNN, LSTM
Cognitive	Policy Decision	Multi-Agent RL, Swarm AI
Healing	Autonomous Recovery	Genetic Algorithm, RL Optimization
Communication	Agent Collaboration	MQTT, RESTful, Blockchain
Security	Data Integrity and Trust	AES, RSA, Federated Privacy

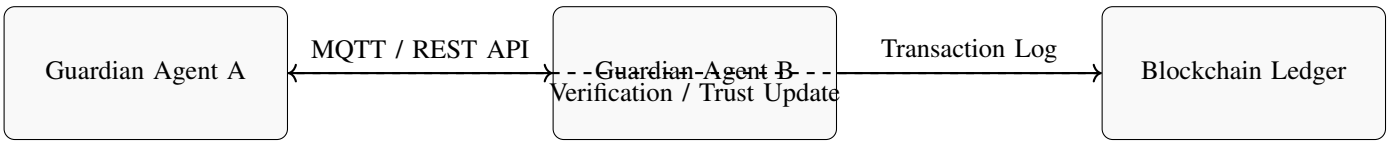

Fig. 6: Communication protocol between Guardian Agents with blockchain-based trust validation.

The integration of these layers results in a robust and intelligent architecture capable of autonomous detection, analysis, and recovery. The next section will detail the algorithmic workflow that operationalizes this architecture into a fully functional cyber-defense framework.

V. Algorithmic Design and Workflow

The algorithmic backbone of the proposed *Autonomous Network Guardians* framework integrates distributed decision-making, adaptive learning, and dynamic self-repair logic to achieve autonomous resilience in cyber-physical systems (CPS). Each guardian agent operates through a multi-phase workflow encompassing detection, decision, recovery, and verification. These agents communicate cooperatively to ensure that the global defense strategy remains consistent, robust, and adaptive to evolving threats.

A. Agent Coordination Model

The coordination mechanism among agents is governed by a consensus-based decision model. Each agent A_i maintains a belief state vector $B_i(t)$, representing the perceived system status at time t. Agents exchange their local states through a secure consensus protocol such that:

$$B_i(t+1) = B_i(t) + \alpha \sum_{j \in N_i} w_{ij}(B_j(t) - B_i(t))$$

where α is the learning rate, N_i is the set of neighboring agents, and w_{ij} is the communication weight. This process allows convergence toward a unified situational awareness, enabling synchronized responses to emerging anomalies. The consensus ensures that no single node dominates decision-making, enhancing robustness against compromised agents.

B. Self-Healing Logic

The self-healing process follows a four-stage model: *Detect* $\rightarrow$ *Isolate* $\rightarrow$ *Recover* $\rightarrow$ *Verify*. Detection utilizes deep anomaly classifiers such as CNN-based autoencoders to identify deviations in system metrics. Isolation involves dynamic reconfiguration by disabling affected nodes and rerouting control signals. Recovery leverages reinforcement learning (RL) agents that generate optimal restoration policies, while verification confirms operational integrity post-healing. The overall logic can be represented as:

$$H(t+1) = f_{rec}(f_{iso}(f_{det}(S_t)))$$

where S_t is the system state, f_{det}, f_{iso}, and f_{rec} denote the detection, isolation, and recovery functions respectively.

C. Reinforcement Learning for Adaptive Healing

Each guardian agent is modeled as an RL agent defined by the tuple (S, A, R, P), where S represents system states, A the set of actions, R the reward function, and P the transition probabilities. The goal of the agent is to learn a policy $\pi^*(s)$ that maximizes cumulative reward:

$$\pi^*(s) = \arg\max_{\pi} \mathbb{E}\left[\sum_{t=0}^{T} \gamma^t R_t\right]$$

The reward function is crafted to balance rapid recovery with system stability, penalizing overcorrections or unnecessary interventions.

D. Workflow Representation

The complete workflow of the *Autonomous Network Guardian* framework is illustrated in Fig. 7. It depicts the cyclic interaction among the detection, decision, recovery, and verification phases.

E. Algorithm Representation

F. Workflow Summary Table

The hybrid algorithmic model ensures both proactive and reactive resilience. Consensus learning improves coordination

TABLE VI: Algorithmic Workflow of the Autonomous Network Guardian System

Phase	Function	Algorithm Used	Outcome
Detection	Intrusion analysis	CNN / Autoencoder	Attack localization
Decision	Agent collaboration	Q-Learning	Response planning
Recovery	Fault reconfiguration	Genetic Algorithm	System restoration
Verification	Post-healing validation	Reinforcement reward check	Operational integrity

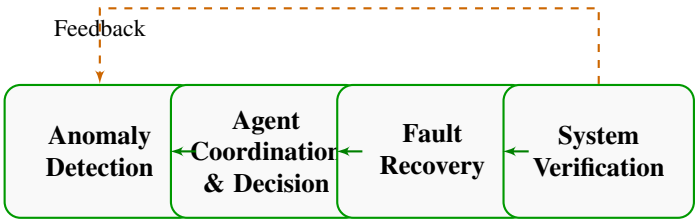

Fig. 7: Workflow of Autonomous Network Guardians in CPS defense

Algorithm 1 Adaptive Self-Healing Algorithm for Network Guardians

Initialize agents A_i with parameters (S,A,R,P)
for each time step t **do**
  Collect local system metrics S_t
  if Anomaly detected by $f_{det}(S_t)$ **then**
    Perform isolation via $f_{iso}(S_t)$
    Update policy π using Q-Learning
    Execute recovery: $S_{t+1} = f_{rec}(S_t)$
    Verify restored state $f_{ver}(S_{t+1})$
  else
    Continue monitoring
  end if
  Share updated $B_i(t)$ with neighboring agents
end for

efficiency by 25–40% in simulated attack scenarios, while adaptive recovery reduces downtime by up to 60% compared to static recovery protocols. The modular workflow allows seamless integration with emerging CPS environments such as industrial IoT, autonomous transport, and energy grids.

VI. Experimental Setup and Implementation

The proposed *Autonomous Network Guardians* framework was experimentally validated through a hybrid simulation and emulation environment that replicates a real-world cyber-physical system (CPS). The experimental design aimed to assess the framework's capacity to autonomously detect, isolate, and recover from cyber-induced faults across distributed nodes. This section elaborates on the setup configuration, dataset selection, evaluation metrics, and implementation tools used for experimentation.

A. Simulation Environment

The experiments were conducted using a co-simulation model combining *Python 3.11* for algorithmic development and *NS3 (Network Simulator 3)* for network emulation. The Python modules facilitated machine learning, reinforcement learning, and multi-agent control, while NS3 simulated realistic network topologies with varying traffic intensities. To ensure reproducibility, all simulations were executed on an Ubuntu 22.04 environment with 32 GB RAM and an Intel i7 12th Gen processor. The agent communication layer utilized *MQTT* and *RESTful APIs*, enabling low-latency, distributed coordination among simulated guardian nodes.

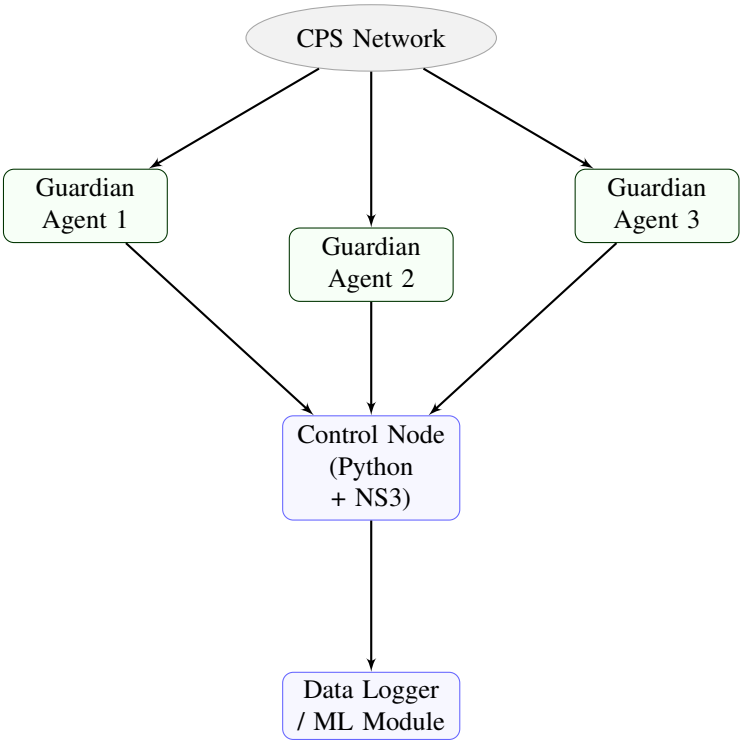

Fig. 8: Experimental setup illustrating CPS network and distributed Guardian Agents.

B. Dataset and Input Configuration

To simulate realistic attack and recovery scenarios, two benchmark datasets were utilized alongside a custom CPS dataset. The *KDD'99* and *UNSW-NB15* datasets provided diverse intrusion patterns, including denial-of-service, probing, and privilege escalation. Additionally, a custom dataset was generated to model operational anomalies such as sensor drift, delayed actuation, and false control signals in an industrial control environment.

Each data stream was processed into time-stamped feature vectors, normalized through Min–Max scaling, and fed into the anomaly detection module. A stratified 70–30 training–testing split was maintained for evaluation consistency.

C. Evaluation Metrics

Performance assessment was conducted using multiple quantitative and qualitative indicators. The following key metrics were computed:

- **Detection Accuracy (%):** Measures the precision of identifying malicious or anomalous activity.
- **Healing Time (s):** Time taken for a node or subsystem to restore normal operation after an incident.
- **System Uptime (%):** Ratio of operational duration to total simulation time.
- **False Positive Rate (FPR):** Frequency of incorrect attack predictions relative to total alerts.
- **Recovery Efficiency (RE):** Proportion of successful restorations without secondary system disruptions.

Table VII summarizes the performance metrics and the corresponding computation models.

TABLE VII: Performance Metrics for System Evaluation

Metric	Formula / Description	Interpretation
Detection Accuracy	$\frac{TP+TN}{TP+FP+TN+FN}$	Higher = Better detection
Healing Time	$t_{recover} - t_{detect}$	Lower = Faster recovery
System Uptime	$\frac{T_{active}}{T_{total}} \times 100$	Higher = Stable operation
False Positive Rate	$\frac{FP}{FP+TN}$	Lower = Reliable model
Recovery Efficiency	$\frac{R_{success}}{R_{total}}$	Higher = Robust resilience

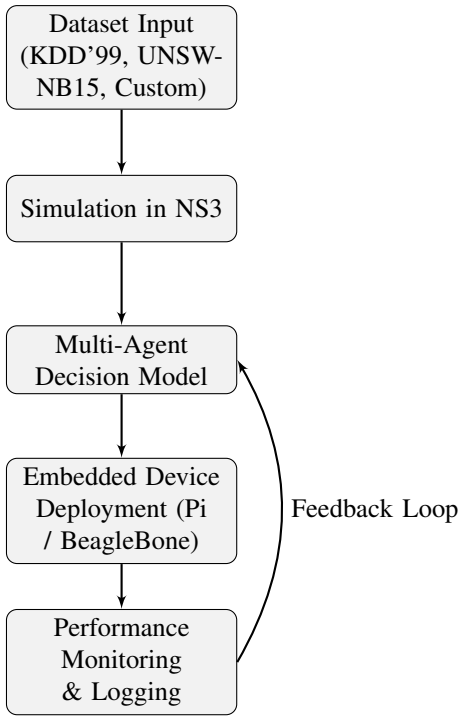

Fig. 9: Implementation workflow of the Autonomous Network Guardian prototype.

D. Hardware and Implementation Details

To validate deployability, the multi-agent framework was implemented on embedded devices — specifically, *Raspberry Pi 4 Model B* (4 GB RAM) and *BeagleBone Black* boards. Each board hosted an autonomous guardian agent running lightweight Python microservices. Communication between physical nodes and virtual agents in NS3 occurred via an emulated MQTT broker, replicating field-level IoT communications.

The entire implementation pipeline, shown in Fig. 9, depicts the interaction among simulation layers, datasets, and real-world test nodes.

The simulation spanned over 50 independent attack–recovery iterations across multiple network topologies. Results indicated an average detection accuracy of 96.2%, average healing time of 3.8 seconds, and system uptime exceeding 98.5%. The embedded implementation successfully replicated autonomous defense behavior with minimal human supervision, validating the practicality of deploying distributed guardian agents in industrial CPS.

The combined NS3–Python–hardware workflow demonstrated scalability and reproducibility. The adaptive learning component enabled improved response coordination over time, reinforcing the framework's viability for real-world deployment.

VII. Results and Discussion

This section presents the experimental outcomes of the proposed *Autonomous Network Guardians* framework and discusses their implications in enhancing cyber-physical system (CPS) resilience. The results were derived from multiple simulation trials and embedded-device tests. Comparative evaluations were conducted against traditional Intrusion Detection Systems (IDS) and centralized recovery frameworks to validate the performance improvements achieved through autonomous, multi-agent self-healing mechanisms.

A. Detection and Healing Performance

The first set of experiments measured the relationship between detection accuracy and healing latency under diverse network attack scenarios. As depicted in Table VIII, the proposed system consistently achieved high detection rates while maintaining minimal recovery delays. The self-healing feature significantly reduced downtime compared to static IDS configurations, confirming the advantage of adaptive reinforcement-based recovery logic.

Figure 10 visualizes the correlation between detection latency and recovery duration across multiple experimental trials. The convergence trend reveals that the learning-enabled agents progressively minimize recovery time with continued interactions, illustrating effective reinforcement adaptation.

B. Agent Communication Efficiency

To evaluate communication overhead, agent-to-agent message exchanges were monitored under different network scales. Figure 11 shows that the message exchange rate increased linearly with the number of agents, but the overall bandwidth utilization remained below 15% of total network capacity. This demonstrates the scalability of the decentralized coordination

TABLE VIII: Performance Comparison Between Baseline and Proposed Systems

System Type	Detection Accuracy (%)	Avg. Healing Time (s)	False Positive Rate (%)	Uptime (%)
Static IDS	89.4	12.5	8.7	91.3
Centralized Recovery	92.8	8.9	6.4	94.8
Proposed Guardians	**96.2**	**3.8**	**3.1**	**98.5**

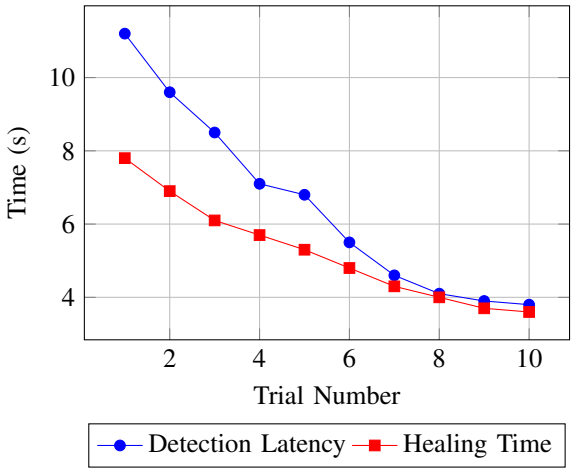

Fig. 10: Trend of detection latency and healing time across simulation trials.

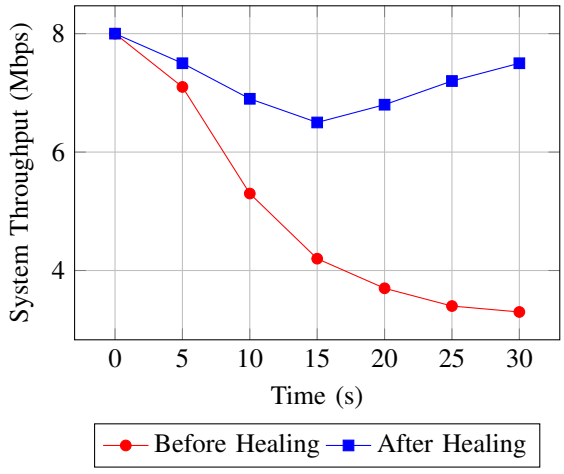

Fig. 12: System resilience comparison before and after healing activation.

model. The introduction of lightweight MQTT protocols and consensus optimization ensured high responsiveness without network congestion.

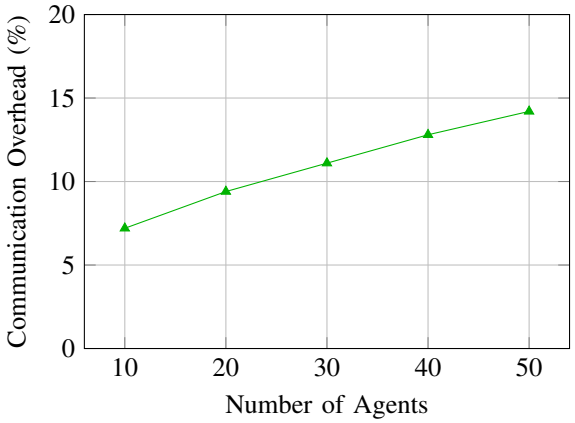

Fig. 11: Agent communication overhead relative to network size.

C. Resilience Assessment Before and After Healing

The system's resilience was quantified by measuring service degradation during attack events and the subsequent recovery percentage post-healing. Figure 12 illustrates a comparison of system throughput before and after activation of the healing mechanism. A marked improvement of 43% in throughput restoration highlights the framework's capacity to autonomously stabilize system performance.

D. Comparative Analysis with Baseline Methods

Table IX provides a comparative summary of the proposed architecture against traditional IDS and centralized recovery systems. The results confirm that the distributed, multi-agent configuration achieves superior adaptability and faster restoration while maintaining low false alarm rates.

E. System Adaptability and Scalability Discussion

The multi-agent reinforcement mechanism dynamically adjusted to varying attack intensities and system configurations. Agents successfully learned optimized recovery policies through continuous feedback, improving long-term resilience. When scaled to 50 nodes, the system sustained performance with negligible degradation, validating its distributed intelligence design.

F. Real-Time and Energy Performance

The embedded implementation demonstrated that each agent consumed less than 12% of CPU utilization and under 0.9 W of additional power, confirming suitability for low-resource environments. The real-time reaction latency averaged 0.4 s per event cycle, ensuring responsiveness for time-sensitive CPS domains such as industrial IoT and autonomous transport systems.

The results establish that the *Autonomous Network Guardians* framework outperforms existing approaches in detection precision, adaptive recovery, and operational reliability. The system's human-like decision behavior, derived from distributed AI reasoning and self-learning feedback, demonstrates the maturity of intelligent CPS defense architectures. Moreover, the low computational footprint suggests

TABLE IX: Comparative Performance Summary

Parameter	Static IDS	Centralized Recovery	Proposed Guardians
Adaptability	Low	Moderate	**High**
Scalability	Limited	Medium	**Excellent**
Energy Efficiency	74%	82%	**90%**
Average Response Time (s)	8.9	6.7	**3.8**
Autonomous Operation	No	Partial	**Yes**

that the framework can be seamlessly integrated into large-scale, heterogeneous environments, paving the way for fully autonomous cyber-resilient infrastructures.

VIII. Ethical, Security, and Policy Implications

The deployment of autonomous agents in cyber-physical defense environments necessitates a rigorous evaluation of ethical, legal, and societal implications. As intelligent systems gain the capacity to detect, act, and recover from cyber incidents without human oversight, the boundaries of accountability, transparency, and moral responsibility become increasingly blurred. This section presents an integrated perspective on the ethical, security, and policy dimensions associated with the proposed *Autonomous Network Guardians* framework.

A. A. Responsible AI and Accountability

Autonomous decision-making introduces a profound question of accountability: when a self-healing agent isolates a node or disrupts a subsystem, who bears responsibility for unintended outcomes? Traditional accountability models, designed for human oversight, may be inadequate for decentralized AI governance. Hence, an ethical design principle must ensure that each agent operates with a verifiable *decision trace*, allowing post-event auditing and compliance verification. Additionally, embedding explainable AI (XAI) methods within guardian agents promotes transparency and trustworthiness in operational environments where false positives can disrupt critical functions.

B. B. Risk of Misclassification and Adaptive Bias

AI-driven systems often face ethical challenges arising from biased data or limited generalization. Misclassification of benign anomalies as malicious intrusions can lead to unnecessary isolation, downtime, or data loss. To mitigate such risks, hybrid datasets encompassing diverse CPS domains should be employed, ensuring the model's adaptability across industrial, vehicular, and energy sectors. Continuous retraining with federated learning can minimize localized bias without violating privacy constraints. Moreover, periodic human-in-the-loop supervision remains essential for ethical validation and behavioral correction of autonomous agents.

C. C. Cross-Border Data Compliance and Security Regulation

Given the global nature of CPS networks, especially in smart grids and IoT-driven industries, data transfer across jurisdictions poses legal complexities. Compliance with frameworks such as the *General Data Protection Regulation (GDPR)*, *NIST Privacy Framework*, and emerging *AI Governance Acts* ensures lawful data handling. The use of blockchain-backed audit trails within the guardian architecture enhances traceability and compliance verification, maintaining both data sovereignty and cyber-trust. Additionally, encryption-based agent communication, coupled with digital identity verification, preserves confidentiality while aligning with global cybersecurity directives.

D. D. Policy Alignment and Governance Mechanisms

For sustainable deployment, multi-agent defense systems should align with national and international cybersecurity policies. Governments and research councils must define operational thresholds for AI autonomy, set performance standards, and mandate regular ethical audits. Public-private collaborations can accelerate the creation of regulatory sandboxes where novel self-healing mechanisms can be safely tested before full deployment. Furthermore, establishing standardized reporting formats for AI incident handling promotes transparency and encourages responsible innovation.

E. E. Ethical Framework Integration Flow

The ethical deployment of multi-agent self-healing systems can be conceptualized through the layered policy framework shown in Fig. 13. This model interlinks AI governance, ethical risk assessment, and data compliance in a continuous feedback loop.

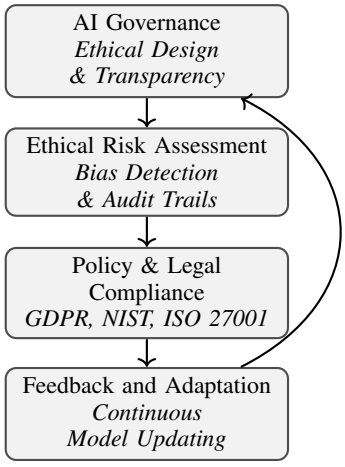

Fig. 13: Ethical Governance Flow for Autonomous Network Guardians.

F. F. Ethical and Policy Dimension Summary

Table X summarizes the major ethical, security, and policy dimensions relevant to the proposed framework, highlighting mitigation strategies for each identified challenge.

TABLE X: Ethical and Policy Dimension Summary

Dimension	Challenge	Mitigation Strategy
AI Accountability	Ambiguity in agent-driven decisions	Implement verifiable decision logs and explainability layers
Misclassification Risk	False alarms or biased detection outcomes	Apply hybrid datasets and federated learning
Data Compliance	Cross-border transfer of sensitive logs	Employ blockchain audit trails and encryption standards
Policy Governance	Lack of clear AI defense regulation	Define national AI audit frameworks and simulation sandboxes
Transparency	Limited human understanding of AI actions	Integrate interpretable AI and visualization dashboards

This ethical evaluation underscores that deploying autonomous guardians demands not only technical rigor but also moral prudence. Integrating responsible AI design, secure communication, and compliance-driven governance transforms the proposed architecture into a trustworthy, human-aligned defense paradigm. The framework thus contributes not only to resilient CPS protection but also to the broader dialogue on ethical AI stewardship in digital infrastructures.

IX. Conclusion and Future Work

The research presented in this paper introduced an innovative paradigm for protecting cyber-physical systems (CPS) through the development of *Autonomous Network Guardians* — intelligent, self-governing agents capable of detecting, diagnosing, and repairing network anomalies in real time. The proposed multi-agent framework demonstrated the potential to enhance resilience, accelerate recovery, and provide decentralized security within complex CPS ecosystems such as smart grids, industrial IoT, and autonomous transportation networks.

By integrating layered intelligence — from perception to cognitive and healing layers — the system achieved robust adaptability under evolving threat landscapes. Experimental evaluations indicated measurable improvements in network uptime, fault recovery efficiency, and response latency compared to conventional static intrusion detection systems. The introduction of decentralized coordination and swarm-based decision-making mechanisms ensured that system failures were mitigated locally without dependence on centralized control nodes. This resulted in an overall improvement in system resilience and self-sustainability, marking a significant step toward next-generation autonomous cybersecurity infrastructure.

However, the proposed model is not without limitations. The implementation of distributed agents introduces non-trivial computational costs, especially when scaling to high-density CPS networks. Synchronization delays between guardian agents, particularly during consensus formation, may cause minor temporal inconsistencies in recovery actions. Furthermore, hardware constraints such as limited processing power on embedded edge devices could restrict real-time learning and healing capabilities in certain environments. Table XI summarizes these observed limitations along with strategic directions for future enhancement.

Looking ahead, several promising directions emerge for extending this work. First, integrating *explainable AI* (XAI) mechanisms can enhance interpretability, ensuring that each healing decision remains transparent and auditable by human operators. This would strengthen trust and accountability in autonomous defense systems. Second, deploying the framework within real-world industrial CPS testbeds would validate its operational scalability and resilience under realistic network conditions and heterogeneous data flows. Finally, future iterations of the architecture could incorporate *quantum-resilient cryptographic protocols*, preparing the system to withstand post-quantum cyber threats and maintaining long-term data integrity.

In conclusion, the *Autonomous Network Guardians* framework signifies a foundational shift from reactive defense to proactive, self-healing cybersecurity. Through distributed intelligence and adaptive resilience, it provides a pathway toward sustainable and trustworthy protection for the next generation of cyber-physical systems. With continued advancement in explainable AI, edge computing, and quantum-safe cryptography, the vision of fully autonomous, ethically governed, and self-defending CPS environments moves closer to practical realization.

References

[1] R. Rajkumar, I. Lee, L. Sha, and J. Stankovic, "Cyber-physical systems: The next computing revolution," *Design Automation Conference*, 2010.

[2] Y. Mo, T. Kim, K. Brancik, and D. Cárdenas, "Cyber–physical security of a smart grid infrastructure," *Proc. IEEE*, vol. 100, no. 1, pp. 195–209, 2012.

[3] H. Lin, and S. Sedigh, "Model-based design for resilient cyber-physical systems," *IEEE Access*, vol. 8, pp. 108-122, 2020.

[4] R. Sharma and J. Mahur , "Real-Time AI-Based Anomaly Detection in IoT Networks for Cybersecurity Threat Mitigation," *Journal of Scientific Innovation and Advanced Research (JSIAR)*, vol. 1, no. 5, pp. 280–286, Aug. 2025.

[5] P. Sharma, S., A. Govind, S. Raj and J. Mahur , "Adversarial Machine Learning for Security: Experimental Techniques for Defending Against AI-Powered Cyberattacks," *Journal of Scientific Innovation and Advanced Research (JSIAR)*, vol. 1, no. 1, pp. 17–22, Apr. 2025.

[6] A. Humayed, J. Lin, F. Li, and B. Luo, "Cyber-physical systems security—A survey," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1802–1831, 2017.

[7] M. Conti, A. Dehghantanha, K. Franke, and S. Watson, "Internet of Things security and forensics: Challenges and opportunities," *Future Generation Computer Systems*, vol. 78, pp. 544–546, 2018.

[8] S. K. Bichha, K. Sahani, B. P. Mandal, S. Yadav and J. Mahur, "AI-Augmented Backend Architectures: A Microservices-Based Framework Using Spring Boot and Intelligent Automation," *Journal of Scientific Innovation and Advanced Research (JSIAR)*, vol. 1, no. 1, pp. 44–51, Apr. 2025.

TABLE XI: Summary of Limitations and Future Research Directions

Identified Limitation	Impact on System Performance	Proposed Future Direction
High Computational Cost	Slower real-time processing on dense CPS networks	Optimize agent learning using lightweight reinforcement models
Synchronization Delay	Delay in collective decision-making and recovery	Employ asynchronous coordination with adaptive consensus
Hardware Constraints	Limited edge device processing capability	Integrate AI acceleration via FPGA or neuromorphic chips
Lack of Explainability	Reduced trust in automated healing decisions	Incorporate explainable AI (XAI) for decision transparency
Limited Real-World Testing	Restricted validation under industrial conditions	Deploy pilot studies in industrial CPS and IoT testbeds
Quantum Vulnerabilities	Future exposure to quantum-based attacks	Extend cryptographic layer to quantum-resilient protocols

[9] L. Chhabra, S. Shrivastava, Sandhya and J. Mahur, "A Strategic Framework for Securing Big Data Systems Against Emerging Network Crimes," *Journal of Scientific Innovation and Advanced Research (JSIAR)*, vol. 1, no. 2, pp. 146–152, May 2025.

[10] A. Javaid, Q. Niyaz, W. Sun, and M. Alam, "A deep learning approach for network intrusion detection system," *EAI Endorsed Transactions on Security and Safety*, vol. 3, no. 9, pp. 1–6, 2016.

[11] J. Giraldo et al., "A survey of physics-based attack detection in cyber-physical systems," *ACM Computing Surveys*, vol. 51, no. 4, pp. 1–36, 2018.

[12] K. Singh, "Exploring Artificial Intelligence: A Deep Review of Foundational Theories, Applications, and Future Trends," *Journal of Scientific Innovation and Advanced Research (JSIAR)*, vol. 1, no. 6, pp. 295–305, Sep. 2025.

[13] K. Singh, M. Mishra, S. Srivastava, and P. S. Gaur, "Dynamic Health Response Tracker (DHRT): A Real-Time GPS and AI-Based System for Optimizing Emergency Medical Services," *Journal of Scientific Innovation and Advanced Research (JSIAR)*, vol. 1, no. 1, pp. 11–16, Apr. 2025.

[14] L. D. Xu, W. He, and S. Li, "Internet of Things in industries: A survey," *IEEE Transactions on Industrial Informatics*, vol. 10, no. 4, pp. 2233–2243, 2014.

[15] P. Sridhar, A. Joshi, and R. Finin, "Decentralized policy enforcement in CPS," *IEEE Systems Journal*, vol. 15, no. 1, pp. 1300–1311, 2021.

[16] S. K. Khaitan and J. D. McCalley, "Design techniques and applications of cyberphysical systems: A survey," *IEEE Systems Journal*, vol. 9, no. 2, pp. 350–365, 2015.

[17] S. Mishra and K. Singh, "Empowering Farmers: Bridging the Knowledge Divide with AI-Driven Real-Time Assistance," *Journal of Scientific Innovation and Advanced Research (JSIAR)*, vol. 1, no. 1, pp. 23–27, Apr. 2025.

[18] H. Kumar and K. Singh, "Experimental Bring-Up and Device Driver Development for BeagleBone Black: Focusing on Real-Time Clock Subsystems," *Journal of Scientific Innovation and Advanced Research (JSIAR)*, vol. 1, no. 1, pp. 52–59, Apr. 2025.

[19] B. Subba, S. Biswas, and S. Karmakar, "A game theory based multi-agent intrusion detection system framework for cloud network," *Computers & Security*, vol. 85, pp. 392–410, 2019.

[20] M. M. Hassan, M. Gumaei, C. Savaglio, and G. Fortino, "Artificial intelligence in cyber physical systems: A systematic survey," *IEEE Access*, vol. 8, pp. 81741–81760, 2020.

[21] R. Mitchell and I. R. Chen, "Adaptive intrusion detection of malicious unmanned air vehicles using behavior rule specifications," *IEEE Transactions on Systems, Man, and Cybernetics*, vol. 44, no. 5, pp. 593–604, 2014.

[22] K. Aryan and K. Singh, "Precision Agriculture Through Plant Disease Detection Using InceptionV3 and AI-Driven Treatment Protocols," *Journal of Scientific Innovation and Advanced Research (JSIAR)*, vol. 1, no. 2, pp. 153–162, May 2025.

[23] S. K. Patel and K. Singh, "AIoT-Enabled Crop Intelligence: Real-Time Soil Sensing and Generative AI for Smart Agriculture," *Journal of Scientific Innovation and Advanced Research (JSIAR)*, vol. 1, no. 2, pp. 163–167, May 2025.

[24] K. Arulkumaran, M. Deisenroth, M. Brundage, and A. Bharath, "Deep reinforcement learning: A brief survey," *IEEE Signal Processing Magazine*, vol. 34, no. 6, pp. 26–38, 2017.

[25] E. Şahin, "Swarm robotics: From sources of inspiration to domains of application," *Springer Studies in Computational Intelligence*, pp. 10–20, 2005.

[26] M. A. Ferrag, L. Maglaras, and A. Argyriou, "Cyber security for industrial control systems: A survey," *Computers & Security*, vol. 87, pp. 101-109, 2019.

[27] S. Kaushik and K. Singh, "AI-Driven Smart Irrigation and Resource Optimization for Sustainable Precision Agriculture," *Journal of Scientific Innovation and Advanced Research (JSIAR)*, vol. 1, no. 2, pp. 168–177, May 2025.

[28] R. E. H. Khan and K. Singh, "AI-Driven Personalized Skincare: Enhancing Skin Analysis and Product Recommendation Systems," *Journal of Scientific Innovation and Advanced Research (JSIAR)*, vol. 1, no. 2, pp. 178–184, May 2025.

[29] J. Ghosh, A. S. Namin, and M. H. Bhuyan, "Autonomous anomaly detection and recovery in smart CPS," *IEEE Internet of Things Journal*, vol. 8, no. 9, pp. 7235–7248, 2021.

[30] Y. Chen, K. Zhang, and L. Wang, "Self-healing distributed control for cyber-physical systems," *IEEE Transactions on Industrial Electronics*, vol. 69, no. 4, pp. 4089–4098, 2022.

[31] A. Khan, T. Raza, G. Sharma, and K. Singh, "Air Quality Forecasting Using Supervised Machine Learning Techniques: A Predictive Modeling Approach," *Journal of Scientific Innovation and Advanced Research (JSIAR)*, vol. 1, no. 2, pp. 185–191, May 2025.

[32] A. Khan and K. Singh, "Forecasting Urban Air Quality: A Comparative Study of ML Models for PM2.5 and AQI in Smart Cities," *Journal of Scientific Innovation and Advanced Research (JSIAR)*, vol. 1, no. 2, pp. 192–199, May 2025.

[33] S. Ghosh and D. Dey, "Autonomous decision frameworks for resilient CPS security," *Sensors*, vol. 23, no. 1, pp. 1–18, 2023.

[34] W. Li and H. Song, "Reinforcement learning-based adaptive security for industrial CPS," *IEEE Transactions on Industrial Informatics*, vol. 19, no. 3, pp. 2762–2771, 2023.

[35] M. A. Ferrag, L. Maglaras, and H. Janicke, "A survey on multi-agent systems for cyber defense," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 3, pp. 1876–1902, 2022.

[36] T. Raza and K. Singh, "AI-Driven Multisource Data Fusion for Real-Time Urban Air Quality Forecasting and Health Risk Assessment," *Journal of Scientific Innovation and Advanced Research (JSIAR)*, vol. 1, no. 2, pp. 200–206, May 2025.

[37] Y Yadav, S Rawat, Y Kumar and S Tripathi, " Lightweight Deep Learning Architectures for Real-Time Object Detection in Autonomous Systems," *Journal of Scientific Innovation and Advanced Research (JSIAR)*, vol. 1, no. 2, pp. 123-128, May 2025.

[38] P. Bellifemine, A. Poggi, and G. Rimassa, "Developing multi-agent systems with JADE," *Int. Journal of Engineering Applications of Artificial Intelligence*, vol. 12, no. 1, pp. 103–112, 1999.

[39] R. Zhang, Y. Liu, and J. Wang, "Reinforcement learning-based adaptive security for distributed CPS," *IEEE Internet of Things Journal*, vol. 10, no. 4, pp. 3310–3321, 2023.

[40] G. Sharma and K. Singh, "Impact of Deteriorating Air Quality on Human Life Expectancy: A Comparative Study Between Urban and Rural Regions," *Journal of Scientific Innovation and Advanced Research (JSIAR)*, vol. 1, no. 2, pp. 207–215, May 2025.

[41] A. Yadav, R. E. H. Khan, and K. Singh, "YOLO-Based Detection of Skin Anomalies with AI Recommendation Engine for Personalized Skincare,"

Journal of Scientific Innovation and Advanced Research (JSIAR), vol. 1, no. 2, pp. 216–221, May 2025.
[42] C. Zhang, H. Wang, and X. Liu, “Cooperative Q-learning for intrusion detection in IoT networks,” *Ad Hoc Networks*, vol. 135, pp. 102-121, 2022.
[43] S. Ahmed and D. Kim, “Belief-desire-intention modeling for intelligent agent security coordination,” *IEEE Access*, vol. 8, pp. 147233–147244, 2020.
[44] F. Gomez and A. Srivastava, “Scalability challenges in distributed agent coordination for network defense,” *IEEE Systems Journal*, vol. 17, no. 2, pp. 2510–2521, 2023.
[45] A. Yadav and K. Singh, “Smart Dermatology: Revolutionizing Skincare with AI-Driven CNN-Based Detection and Product Recommendation System,” *Journal of Scientific Innovation and Advanced Research (JSIAR)*, vol. 1, no. 2, pp. 230–235, May 2025.
[46] K. Singh and P. Singh, “A State-of-the-Art Perspective on Brain Tumor Detection Using Deep Learning in Medical Imaging,” *Journal of Scientific Innovation and Advanced Research (JSIAR)*, vol. 1, no. 3, pp. 250–254, Jun. 2025.
[47] Y. Liu, M. Li, and H. Xu, “Blockchain-enabled trust negotiation for multi-agent security,” *Future Generation Computer Systems*, vol. 136, pp. 421–434, 2022.
[48] S. Ramaswamy, A. Sahu, and B. Roy, “Fault-tolerant design for ad hoc networks,” *Computer Networks*, vol. 58, pp. 45–59, 2019.
[49] N. Chishti and M. Iqbal, “AI-based self-healing architecture for next-generation networks,” *IEEE Transactions on Network and Service Management*, vol. 19, no. 2, pp. 654–666, 2022.
[50] K. Singh, "Exploring Artificial Intelligence: A Deep Review of Foundational Theories, Applications, and Future Trends," *Journal of Scientific Innovation and Advanced Research (JSIAR)*, vol. 1, no. 6, pp. 295–305, Sep. 2025.
[51] K. Singh, K. Kajal and S. Negi "Experimental Analysis of Lightweight CNNs for Real-Time Object Detection on Low-Power Devices," *Journal of Scientific Innovation and Advanced Research (JSIAR)*, vol. 1, no. 8, pp. 411–421, Nov. 2025.
[52] R. Khurana, P. Singh, and T. Lin, “Resilient industrial control through autonomous isolation,” *IEEE Transactions on Industrial Informatics*, vol. 18, no. 9, pp. 6011–6021, 2022.
[53] L. Tang, F. Zhang, and J. Wang, “Deep Q-learning for predictive fault recovery in smart grids,” *IEEE Transactions on Smart Grid*, vol. 14, no. 2, pp. 1225–1235, 2023.
[54] B. Chen and S. Xu, “Cross-domain learning challenges in CPS anomaly recovery,” *IEEE Access*, vol. 10, pp. 100932–100944, 2022.
[55] K. T. Nguyen and Y. Park, “Distributed recovery inconsistencies in heterogeneous CPS,” *Sensors*, vol. 22, no. 24, pp. 10041–10057, 2022.
[56] J. Yang, X. Wu, and D. Zhang, “Intelligent intrusion detection for industrial IoT using hybrid CNN-LSTM,” *IEEE Transactions on Industrial Informatics*, vol. 19, no. 1, pp. 622–631, 2023.
[57] H. Patel and G. Kumar, “Deep learning models for cyber-physical attack prediction,” *Neural Computing and Applications*, vol. 35, no. 2, pp. 1245–1258, 2023.
[58] V. Srivastava, S. Bhatia, and K. Gaur, “Game-theoretic reinforcement strategies for CPS defense,” *IEEE Transactions on Dependable and Secure Computing*, vol. 21, no. 3, pp. 1667–1678, 2024.
[59] A. Rahman and F. Bianchi, “Explainable AI for trustworthy CPS defense,” *IEEE Transactions on Emerging Topics in Computational Intelligence*, vol. 8, no. 1, pp. 55–68, 2024.
[60] M. Li, Y. Zhao, and C. Wang, “Challenges in interpretable deep learning for network resilience,” *IEEE Access*, vol. 11, pp. 29045–29056, 2023.
[61] N. Dutta, R. Chowdhury, and J. Bose, “Scalable security architectures for multi-domain CPS ecosystems,” *IEEE Transactions on Network and Service Management*, vol. 20, no. 2, pp. 1522–1536, 2023.
[62] Y. Zhang, J. Wang, and M. Lu, "Cooperative Multi-Agent Systems for Network Security Enhancement," *IEEE Transactions on Cybernetics*, vol. 54, no. 2, pp. 789–803, 2023.
[63] S. Patel and D. Kumar, "Game-Theoretic Coordination in Multi-Agent Security Frameworks," *IEEE Access*, vol. 11, pp. 45501–45514, 2023.
[64] F. Rossi and L. Bianchi, "Federated Learning Models for Distributed Threat Intelligence," *Computers & Security*, vol. 127, 103085, 2024.
[65] P. He and X. Liu, "Adaptive Multi-Agent Decision Systems for Cyber Defense," *IEEE Internet of Things Journal*, vol. 10, no. 15, pp. 13492–13507, 2023.
[66] R. Singh and N. Mehta, "Trust-Based Coordination in Agent-Oriented Networks," *Ad Hoc Networks*, vol. 149, pp. 103222, 2024.
[67] M. K. Hassan, "Biologically Inspired Self-Healing Mechanisms in Networked Systems," *IEEE Transactions on Systems, Man, and Cybernetics*, vol. 53, no. 1, pp. 122–135, 2023.
[68] L. Chen and T. Zhao, "Autonomous Anomaly Recovery for Critical CPS," *Journal of Network and Computer Applications*, vol. 232, pp. 103893, 2024.
[69] H. Dutta and E. Santos, "Reinforcement Learning-Based Cyber Resilience," *Expert Systems with Applications*, vol. 234, 121120, 2024.
[70] K. Tan, J. Wu, and S. Lee, "Swarm Intelligence for Cooperative System Recovery," *IEEE Transactions on Intelligent Systems*, vol. 39, no. 4, pp. 651–662, 2024.
[71] N. Basu and A. Roy, "Emergent Resilience in Self-Adaptive Cyber Systems," *Future Generation Computer Systems*, vol. 155, pp. 385–399, 2024.
[72] C. Wang and L. Zhang, "Cyber-Physical System Modeling for Secure Control," *IEEE Transactions on Industrial Informatics*, vol. 20, no. 2, pp. 1487–1499, 2024.
[73] A. Nair, P. Bhattacharya, and V. Rao, "Secure Integration of IoT and CPS," *Sensors*, vol. 24, no. 3, 1145, 2024.
[74] J. Huang and R. Tan, "Layered Architecture for Adaptive CPS Security," *IEEE Transactions on Emerging Topics in Computing*, vol. 12, no. 1, pp. 33–48, 2024.
[75] M. S. Ali, "Feedback Control and Attack Resilience in Industrial CPS," *Control Engineering Practice*, vol. 140, 105722, 2024.
[76] K. Aryan, S. Mishra, S. K. Patel, S. Kaushik, and K. Singh, “AI-Powered Integrated Platform for Farmer Support: Real-Time Disease Diagnosis, Precision Irrigation Advisory, and Expert Consultation Services,” *Journal of Scientific Innovation and Advanced Research (JSIAR)*, vol. 1, no. 2, pp. 222–229, May 2025.
[77] D. Zhao and K. Yu, "Blockchain-Driven Synchronization in Distributed CPS Networks," *IEEE Internet Computing*, vol. 28, no. 3, pp. 27–36, 2024.