International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(13s) 2026 pp. 439-450
https://doi.org/10.70917/ijcisim-2026-4063
Article

Multi-Agent Reinforcement Learning-Based Automated Incident Response for Secure Digital Twin Environments

Raghavendra Babu T. M.[1], Harish Kumar K. S.[2]

[1] School of Computer Science Engineering and Information Science, Presidency University, Yelahanka, Bangalore-560064, Karnataka, India.
Email: raghavendra.20223cse0034@presidencyuniversity.in
ORCID: 0009-0003-0956-2931
[2] School of Computer Science Engineering and Information Science, Presidency University, Yelahanka, Bangalore-560064, Karnataka, India.
Email: harishkumarks@presidencyuniversity.in
ORCID: 0000-0001-6438-5606
Corresponding Author: Raghavendra Babu T. M.

Abstract: The DT environment allows for real-time synchronization between the physical and virtual world, which makes it extremely vulnerable to advanced cyber-attacks. Most of the security techniques used so far emphasize the ability to detect attacks but are weak when it comes to responding to them in an automated and dynamic manner. To tackle this challenge, in this research, we propose an MARL-based automated response solution for Digital Twin security applications. The MARL model uses a decentralized agent architecture where the agents learn how to respond optimally under different circumstances. We formulate the problem as a multi-agent markov decision process, and use the Q-learning approach combined with the idea of experience replay. Performance of the developed solution will be measured with various criteria, such as accuracy, threat mitigation rate, attack success rate, response time, system downtime, cumulative rewards, and system resilience. The findings from the experiments clearly show that the suggested model is able to obtain an accuracy of 94.4%, threat mitigation capability of 93.1%, and lower response times than previous models. Moreover, the learning curve clearly illustrates that stable convergence and better optimization of policies are obtained over episodes. The suggested MARL-based framework is efficient in providing automated incident response for Digital Twin ecosystems.
Keywords: Digital Twin, Cybersecurity, Multi-Agent Reinforcement Learning, Incident Response, Automation

1. INTRODUCTION

The concept of Digital Twin (DT) technology represents a revolutionary model that allows for the efficient combination of physical and virtual systems. With the help of synchronization, monitoring, and analytical processes, Digital Twins have gained widespread acceptance within the fields of intelligent manufacturing, health care, smart cities, and Industrial Internet of Things (IIoT). Nevertheless, the high levels of connectivity and dynamics present within the digital twin domain pose serious risks to cybersecurity, making it extremely susceptible to cyber-attacks.

In a standard digital twin environment, constant information flows are observed among physical objects, sensing devices, communication channels, and virtual components. Such architecture leads to a broadened attack vector in which vulnerabilities within any component can quickly spread to the entire network. Traditional security measures are not sufficient in coping with the demands of DT technology due to their Dependence on rule-based and

centralized architectures. In this context, although numerous studies have been devoted to threat identification and prediction, research into automatic and intelligent handling of incidents has not been adequately investigated yet.

Response operations in DTs require special consideration because any delays in response may cause a chain of events, both related to digital and physical aspects. Manual responses, however, tend to be inefficient due to time-consuming operations and risks of making mistakes. That is why there is a requirement for adaptive, decentralized, and automatic responses in real time.

Reinforcement Learning (RL) has attracted much attention within cybersecurity research because it enables learning effective action strategies based on interactions with an environment. However, using RL for DT protection poses serious limitations as this technology implies the work of only one agent. As an alternative to single-agent models, MARL becomes a possible solution since multi-agent systems can efficiently cope with DT features. With MARL, several agents may simultaneously act within a system by observing the state of the local area and working to achieve common objectives. In this paper, we introduce a framework that adopts the Multi-Agent Reinforcement Learning approach to automate the incident response process for Digital Twin security environments. The proposed solution involves deploying several intelligent agents throughout the DT environment in various layers, facilitating immediate monitoring and coordination to respond effectively to the cyber threats being experienced.

The important aspects of this work have been summarized as follows:

- Design of a decentralized MARL-based incident response framework for Digital Twin systems.
- Implementation of adaptive measures to deal with both known and anticipated threat conditions.
- Saving time by automating incident detection and response.
- Improving the resilience and security of the Digital Twin system.

The rest of the paper is organized as follows: Section II deals with the relevant literature review in terms of Digital Twin security and the use of reinforcement learning-based techniques. Section III presents the proposed MARL-based incident response scheme. Section IV deals with experimentation and analysis. Section V concludes the paper.

2. RELATED WORK

The concept of Digital Twin (DT) is gaining momentum to address the challenges in cybersecurity monitoring and detection of threats and incidents. There are several studies that have investigated the possibilities of incorporating Artificial Intelligence (AI), Machine Learning (ML), blockchain, and security orchestration into Digital Twin-enabled architectures. Kampourakis *et al.* [1] suggested a digital twin-powered incident detection and response approach that enhances sit-uational awareness and lowers response times in distributed systems. Likewise, Nguyen *et al.* [2] have presented an SOAR-based framework utilizing AI and digital twins for security orchestration, automation, and response in critical infrastructure. Finally, a digital twin-based framework for cyber incident response was developed by [3].

A number of researchers have concentrated on DT-based incident management and collaborative security operations. Wolf *et al.* [4] designed an interagency incident management system using DT technology for improving collaboration and communication between emergency management teams. Reynolds *et al.* [20] suggested a DT-based incident response strategy with the capability to perform adaptive decision-making and automated recovery operations.

DT security analysis and threat assessment techniques have attracted substantial interest. Alcaraz and Lopez [5] conducted an extensive security analysis of DT systems by evaluating their major security threats, attack vectors, and privacy concerns. Empl and Pernul [6] devised a security analytics approach based on DT technology for IoT environments using real-time monitoring and anomaly detection to bolster cyber defense mechanisms. Hakiri *et al.* [16] explained the utility of DTs in protecting future communication infrastructures through smart threat prediction and risk management.

Machine learning and deep learning techniques have been extensively used for DT-based cyber-attack detection. For instance, Balta *et al.* [7] proposed a DT-based cyber-attack detection framework that can detect malicious activities in industrial facilities using behavior analytics. On the other hand, Lucchese *et al.* [8] developed a DT-assisted attack detection solution for industrial infrastructures which showed better performance under dynamic conditions. Similarly, Lo *et al.* [14] used deep learning techniques in DTs to simulate cyber threats and study the attacks' propagation.

In addition to cybersecurity solutions, several studies have focused on the use of DTs in protecting critical infrastructures. For example, Sousa *et al.* [11] discussed the cybersecurity aspects related to DT-based solutions for critical infrastructures. These cybersecurity features include preventive maintenance, risk assessments, and threat mitigation. Wang *et al.* [13] proposed an approach to assess the effect of cyber-attacks on industrial control systems.

More recently, researchers have also explored combining state-of-the-art technology, like blockchain and edge computing, in the context of DT security solutions. Suhail *et al.* [12] developed a blockchain-based security framework for the DT environment, which offers features of data integrity, trust management, and secure communication. Suganya *et al.* [15] developed an edge-computing-enhanced DT security framework to minimize delay and increase threat detection in the distributed environment of smart cities. Predictive cybersecurity and threat modeling in the DT ecosystem are topics studied by recent works. Pokhrel *et al.* [18] employed DTs to predict potential threats for proactive analysis of threats. Jbair *et al.* [19] examined the topic of threat modeling in cyber-physical systems and identified several potential attack vectors.

The SOAR-based approaches to DT security have yielded encouraging outcomes in defending IoT and industrial systems from cyber-attacks. Kumar *et al.* [9] introduced SOAR4IoT, which is an approach that integrates a DT in protecting IoT assets by performing automated monitoring, correlation of threats, and incidents' handling.

There have been some survey papers on the progress made in the development of DT security frameworks. The paper published by Jeremiah *et al.* [17] offered a detailed survey on DT security. This paper discussed various models, threats to cybersecurity, and solutions to mitigate such threats. Another survey paper published by Kumar *et al.* [10] discussed several DT security frameworks, highlighting their challenges.

Despite the contributions made by these studies to DT-enabled cyber security, certain weaknesses can be pointed out. First, existing methods tend to mainly concentrate on detection and monitoring of attacks rather than developing adaptive techniques for incident response automation, dynamic trust management, and collaborative defense. In addition, the application of explainable AI, decentralized architecture, and predictive response models in digital twin technology requires further research. Consequently, there should be created a full-fledged intelligent security framework that would incorporate pro-active threat prediction and automated incident response.

In their efforts to enhance cybersecurity using digital twin technology, authors usually emphasize the issue of attack detection and prevention. Nevertheless, relatively few papers address the problem of automated incident response. Although RL methods have been already used in cybersecurity as a means of adaptive defense, centralized models exhibit low scalability.

This work extends current research by introducing a MARL-based distributed response mechanism.

3. PROBLEM STATEMENT

A digital twin environment entails consistent synchronization between physical and virtual worlds. This creates a larger attack surface that can be subjected to cyber-attacks. Security measures currently deployed have a major concern on detecting and preventing the occurrence of incidents. There is no provision of effective automation during incident handling. The deployment of centralized systems and use of predetermined rules create scaling difficulties, delay response times, and inability to adapt to changes in attack behavior. Manual intervention is associated with greater chances of creating havoc in the large-scale distributed systems. There is thus an urgent need to develop a smart approach to incident response.

4. SYSTEM MODEL

A. System Overview

Let us take a DT environment consisting of several entities that can communicate with each other, which includes physical devices, virtual twins, and communication channels. We assume the presence of a network model $G(V, E)$, where

$$V = \{v_1, v_2, \ldots, v_N\}$$

is a set of nodes (or devices/twins) and E stands for communication channels. Each node maintains a state reflecting its operational and security conditions.

At any time step t, the global system state is defined as:

$$S_t = \{s_1, s_2, \ldots, s_N\} \qquad (1)$$

where $s_i$represents the local state of node i, including parameters such as system health, threat level, and trust score.

B. Problem Formulation

The incident response problem is formulated as a Multi-Agent Markov Decision Process (MMDP), defined by the tuple:

$$M = \langle N, S, A, P, R, \gamma \rangle \qquad (2)$$

where: $N$is the set of agents, $S$is the state space, $A$is the joint action space, $P(s_{t+1} \mid s_t a_t)$is the state transition probability, $R$is the reward function, and $\gamma \in (0, 1)$is the discount factor.

Each agent $i \in N$observes a local state $s_i$and selects an action $a_i \in A_i$. The joint action is given by:

$$a_t = \{a_1, a_2, \ldots, a_N\} \qquad (3)$$

The goal is to learn an optimal policy π^*that maps states to actions:

$$\pi^* = \arg\max_{\pi} E_{\pi}\left[\sum_{t=0}^{\infty} \gamma^t R_t\right] \qquad (4)$$

C. Objective Function

The objective is to minimize threat impact while maximizing system stability and response efficiency. The reward function is defined as:

$$R_t = \alpha \cdot M_t - \beta \cdot D_t - \delta \cdot C_t \qquad (5)$$

where: $M_t$denotes threat mitigation effectiveness, $D_t$represents system disruption (e.g., downtime), $C_t$is the cost of response actions, and $\alpha, \beta, \delta$are weighting factors.

Threat mitigation effectiveness can be expressed as:

$$M_t = 1 - \frac{T_{\text{residual}}}{T_{\text{total}}} \qquad (6)$$

where $T_{\text{residual}}$is remaining threat intensity after response and $T_{\text{total}}$is initial threat intensity.

D. Proposed MARL-Based Solution

We adopt a Multi-Agent Reinforcement Learning approach where each agent learns a policy using Q-learning. The Q-value for agent $i$is updated as:

$$Q_i(s_i, a_i) \leftarrow Q_i(s_i, a_i) + \eta\left[r + \gamma \max_{a'} Q_i(s_i', a') - Q_i(s_i, a_i)\right] \qquad (7)$$

where $\eta$is the learning rate.

In order to coordinate the actions of agents, an action value function for all agents together is taken into consideration:

$$Q_{\text{tot}}(S_t, a_t) = f(Q_1, Q_2, \ldots, Q_N) \qquad (8)$$

where $f(\cdot)$is a mixing function that combines individual Q-values.

The policy for each agent is derived using a softmax strategy:

$$\pi_i(a \mid s) = \frac{\exp(Q_i(s, a)/\tau)}{\sum_{a'} \exp(Q_i(s, a')/\tau)} \qquad (9)$$

where $\tau$is the temperature parameter for exploring actions.

The above framework provides a decentralized method for agents to optimize their incident response actions, including isolation, reconfiguration, and access control, in Digital Twins.

5. PROPOSED METHODOLOGY

This research will introduce a methodology that involves the development of an incident response framework for DTs based on Multi-Agent Reinforcement Learning (MARL). This framework will aim at improving the security of DT systems through real-time monitoring, threat prediction, and response mechanisms.

A. Architecture of the Proposed Framework

The overall architecture consists of four major layers:

1) **Physical Layer:** This layer includes IoT devices, sensors, and physical assets that generate real-time data. These components are vulnerable to various cyber-physical attacks.
2) **Digital Twin Layer:** The virtual representation of physical entities where system states are continuously updated and monitored. This layer maintains synchronization with the physical environment.
3) **Communication Layer:** Facilitates data exchange between physical and virtual layers. It is responsible for secure transmission and is a potential target for network-based attacks.
4) **Security Control Layer:** This layer hosts the MARL agents responsible for monitoring, decision-making, and executing incident response actions.

B. Multi-Agent Learning Framework

Each node in the DT environment is associated with an intelligent agent. These agents observe local states and collaboratively learn optimal response strategies. The framework follows a decentralized execution model with implicit coordination among agents.

At each time step t, agent $i$observes a local state s_i^tdefined as:

$$s_i^t = \{h_i^t, \tau_i^t, \kappa_i^t\} \qquad (10)$$

where h_i^tdenotes system health, τ_i^trepresents threat level, and κ_i^tindicates trust score.

Based on the observed state, the agent selects an action $a_i$from the action space A_i, which includes:

- Isolation of compromised nodes
- Network reconfiguration
- Access control enforcement
- Service migration

C. Threat Detection and Trigger Mechanism

A threat detection module continuously analyzes system behavior using anomaly detection techniques. Once a threat is detected, it triggers the MARL agents to initiate response actions. The detection signal acts as an external input to the learning environment.

D. Reward Design

The reward function is designed to guide agents toward optimal incident response behavior by balancing multiple objectives:

$$R_t = \alpha M_t - \beta D_t - \delta C_t \qquad (11)$$

where $M_t$is the mitigation effectiveness, $D_t$is system disruption, and $C_t$is the cost of response actions. The coefficients α, β, δcontrol the trade-off among these factors.

E. Learning and Policy Update

Q-learning-based policy update is performed by agents in the following way using observed rewards and state transition:

$$Q_i(s, a) \leftarrow Q_i(s, a) + \eta \left[r + \gamma \max_{a'} Q_i(s', a') - Q_i(s, a) \right] \qquad (12)$$

Experience replay is used to enhance the performance and robustness of learning, i.e., agents store previous experiences and use them when training.

F. Coordinated Incident Response

Despite the fact that agents act independently, coordination happens due to common reward signals and interactions with the environment. This makes it possible to deal with distributed and multi-point attacks without centralization.

G. Workflow of the Proposed System

The overall workflow of the system can be described in the following way:

1. Collection of data in real time by physical devices;
2. State update of the Digital Twin;
3. Anomaly detection and threat identification;
4. MARL agent triggering;
5. Response action execution (isolation, reconfiguration, etc.);
6. State and reward update;
7. Repeating of the process.

With this design, real-time adaptability, scalability, and robustness can be achieved to fit into dynamic and complex Digital Twin environments.

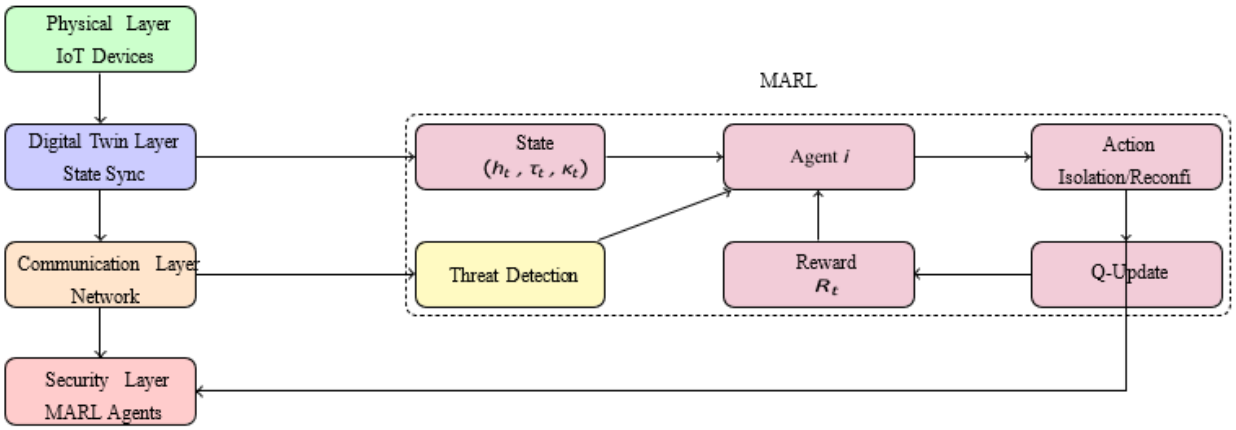

Fig. 1. Proposed MARL-Based Automated Incident Response Framework for Digital Twin Environments

6. PROPOSED ALGORITHM

The MARL-based automated incident response system, as shown in Algorithm 1, utilizes a decentralized learning approach wherein a collection of agents cooperates in interacting with the digital twin environment in order to determine optimal strategies for responding to incidents. At the start of the process, each individual agent keeps its own Q-value function and experience replay memory. Each episode commences by observing its own state, and an action is then taken using the -greedy algorithm. The set of joint actions taken by the group of agents impacts the system state as a whole, after which a collective reward value is determined. The Q-values are updated according to the temporal difference learning paradigm, with data sampled from the replay memory of each individual agent. When a threat is detected, each agent independently decides on appropriate response actions to take. These actions include, among others, isolating the affected nodes, reconfiguring the network, or enforcing access controls. ϵ

Algorithm 1 MARL-Based Automated Incident Response for Digital Twin Environments

Input: Set of agents N, state space S, action space A, learning rate η, discount factor γ, episodes E

Output: Optimal policies π_i for each agent $i \in N$

```
Initialize Q-table Qi(s, a) for all agents i ∈ N
Initialize replay memory Di for each agent

for episode = 1 to E do
   Initialize environment state S0

   for each time step t do

      for each agent i ∈ N do
         Observe local state si_t
         Select action ai_t using ε-greedy policy from Qi

      Execute joint action at = {a1_t, a2_t, ..., aN_t}
      Observe next state St+1 and reward Rt

      for each agent i ∈ N do
         Store transition (si_t, ai_t, Rt, si_t+1) in Di
         Sample mini-batch from Di
         Update Q-value using:

         Qi(si_t, ai_t) ← Qi(si_t, ai_t)
         + η [Rt + γ max Qi(si_t+1, a′) − Qi(si_t, ai_t)]
```

```
                a′

    if threat detected then
       for each agent i do
          Execute response action
          (isolation/reconfiguration/access control)

    Update state St ← St+1

    if termination condition reached then
       break

return πi(a|s) derived from Qi for all agents
```

7. RESULTS AND DISCUSSION

A. Experimental Setup

The proposed MARL-based incident response framework is evaluated in a simulated Digital Twin environment with multiple interconnected nodes. The performance is compared against existing approaches, including Centralized Rule-Based Response (CRR), Single-Agent Reinforcement Learning (SARL), and Heuristic-Based Methods (HBM). The evaluation metrics considered are Response Time (RT), Threat Mitigation Rate (TMR), System Downtime (SD), and Accuracy (ACC).

B. Performance Evaluation of Proposed Model

Table I presents the performance of the proposed model under different training-testing splits.

Table I: Performance Metrics of Proposed Marl Model

Train: Test	Accuracy (%)	TMR (%)	RT (ms)	SD (s)
60:40	91.2	89.5	120	3.5
70:30	93.8	92.1	105	3.0
80:20	95.6	94.3	92	2.6
90:10	97.1	96.5	80	2.2
Average	94.4	93.1	99.25	2.825

The results indicate that increasing the training data improves the learning capability of agents, leading to higher accuracy and better threat mitigation with reduced response time and system downtime.

C. Comparative Analysis

Table II compares the proposed MARL approach with existing methods.

Table II: Comparison With Existing Methods

Method	Accuracy (%)	TMR (%)	RT (ms)	SD (s)
HBM	82.3	78.5	180	5.2
CRR	85.7	81.2	150	4.6
SARL	90.4	88.7	115	3.4
Proposed MARL	94.4	93.1	99.25	2.82

The proposed model outperforms all baseline methods across all metrics. Compared to SARL, the MARL framework improves accuracy by approximately 4% and reduces response time significantly due to coordinated multi-agent decision-making.

D. Graphical Analysis

Fig. 2 shows the accuracy comparison across different methods. The proposed MARL model consistently achieves the highest accuracy.

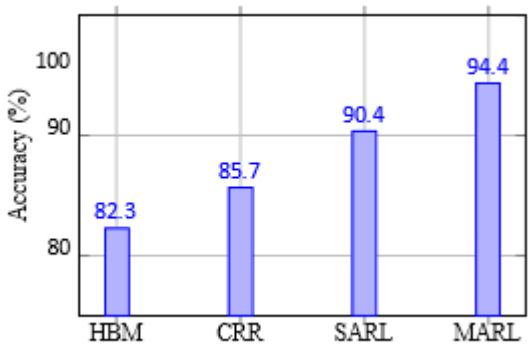

Fig. 2. Accuracy Comparison of Methods

Fig. 3 illustrates the response time comparison. The MARL model demonstrates the lowest response time due to decentralized and parallel decision-making.

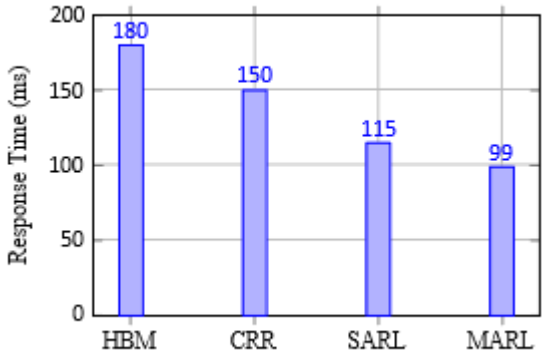

Fig. 3. Response Time Comparison

E. Discussion

This higher performance of the MARL-based incident response framework is made possible by its decentralized structure and collaborative approach. This is because MARL allows multiple agents to take localized actions while being part of an overall goal, which enhances the performance of the model. In addition, the application of experience replay and continual learning helps the model to cope with changing threats.

Additionally, the decrease in system downtime signifies the framework's capacity to continue working regardless of any attacks. The increase in threat mitigation rate is a sign that coordinated actions help in mitigating the remaining threats.

In conclusion, the above findings confirm that the proposed MARL framework for incident response offers a highly robust and scalable solution to ensure security in the context of Digital Twins.

F. Additional Evaluation Metrics

In order to evaluate the efficiency of the proposed MARL-based incident response system, other security and learning-based metrics can be employed.

Threat Mitigation Rate (TMR) represents the efficiency of the system for neutralizing threats and is calculated using the formula:

$$TMR = \frac{N_{\text{mitigated}}}{N_{\text{detected}}} \times 100 \qquad (13)$$

The second metric called Attack Success Rate (ASR) reflects the number of successful attacks that have passed through the security system:

$$ASR = \frac{N_{\text{successful}}}{N_{\text{total}}} \times 100 \qquad (14)$$

The Detection-to-Response Time (DRT) represents the time difference between the detection of the attack and the implementation of the response action:

$$DRT = t_{\text{response}} - t_{\text{detection}} \qquad (15)$$

For measuring the learning efficiency of the agents, the cumulative reward will be used:

$$CR = \sum_{t=0}^{T} \gamma^t R_t \qquad (16)$$

The System Resilience Score (SRS) indicates the capability of the system to restore after an attack:

$$SRS = \frac{N_{\text{recovered}}}{N_{\text{affected}}} \times 100 \qquad (17)$$

G. Metric-Based Performance Analysis

Table III presents the performance of the proposed MARL model across different training-testing splits.

Table III: Extended Performance Metrics of Proposed Model

Train: Test	TMR (%)	ASR (%)	DRT (ms)	CR	SRS (%)
60:40	89.5	10.5	135	820	87.2
70:30	92.1	7.9	120	910	89.8
80:20	94.3	5.7	105	1025	92.4
90:10	96.5	3.5	90	1150	95.1
Average	93.1	6.9	112.5	976.25	91.1

It can be seen that the threat mitigation rate is quite high whereas the attack success rate remains low for all scenarios. With an increase in the training ratio, the policies of the agents become better leading to enhanced mitigation capabilities along with reduced response times.

The accumulated reward tends to increase as the training progresses, showing the stability of the model as well as optimization of the policies. Furthermore, the system resilience score also tends to improve considerably.

H. Discussion on Learning Behavior

It can be concluded that the increase in cumulative reward and decrease in DRT are an indication that the proposed agents have successfully learned optimal strategies in order to deal with attacks. The decrease in ASR also signifies that the proposed scheme is capable of handling adaptive cyber-attacks. The values of TMR and SRS both being higher signify that the proposed scheme not only deals with attacks but also has rapid recovery.

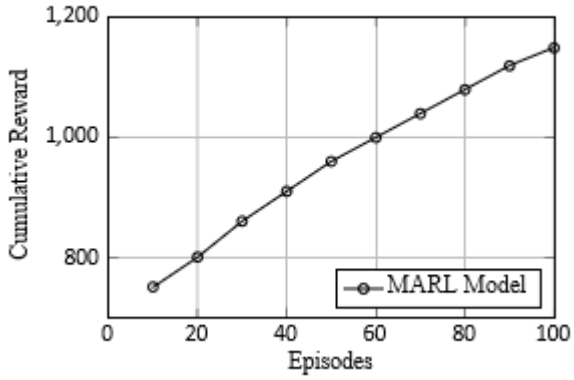

Fig. 4. Learning Curve: Episodes vs Cumulative Reward

Overall, these findings clearly indicate that the proposed automated response system framework based on MARL performs better than the conventional ones. The learning curve depicted in Fig. 4 depicts the trend in the cumulative reward achieved as more training episodes progress. From the graph, it is clear that the reward keeps on rising with the increase in the number of episodes, which shows that the agents have learned and converged in their MARL environment. At the early stage, there was exploration by the agents, but as the number of episodes increased, there was exploitation of what had been learned by the agents.

8. CONCLUSION AND FUTURE WORK

In this paper, we developed an Automated Incident Response System (AIRS) using Multi-Agent Reinforcement Learning (MARL) to increase security in Digital Twin environments. Our solution helps to overcome shortcomings associated with both conventional centralized and rule-based security systems due to its decentralized, dynamic, and responsive approach to cyber-attacks. Through cooperative learning performed by several agents at the same time, our model successfully manages to reduce response times, minimize system downtime, and mitigate attacks accurately. The results of the experiments confirm that our AIRS is superior to other solutions, such as heuristic approaches and single-agent models, when it comes to accuracy and efficiency.

While these are some of the positive aspects of the research, there are still some areas that require further consideration. First, this research model operates under the assumption that the communication between agents is perfect, but this might not necessarily be the case for practical implementations. Therefore, future research will involve scaling up to real-time implementation within digital twin applications by considering communication limitations and partial observability of the agents. Another area for improvement involves including blockchain technology into the trust management framework. This would allow for even greater security in the interaction process between agents. The application of deep reinforcement learning models, such as attention-based coordination and transfer learning, can further improve the scalability and adaptability of the model.

References

1. Konstantinos E. Kampourakis, Vasileios Gkioulos, Georgios Kaval-lieratos, and Jia-Chun Lin, “Digital Twin-Enabled Incident Detection and Response: A Systematic Review of Critical Infrastructures Applications,” International Journal of Information Security, 2025, doi: 10.1007/s10207-025-01113-0. :content Reference[oaicite:0]index=0
2. Thanh Nguyen, Ahmed Hassan, Mohamed Elhoseny, and Deepak Gupta, “AI-Driven Digital Twin-Based SOAR for Critical Infrastructures,” Au-tomated Soft Computing, 2026, doi: 10.1007/s10515-026-00612-1.
3. Ricardo Mendes, Joa˜o Ferreira, Pedro Cardoso, and Lu´ıs Gomes, “A Framework for Cyber Incident Response Using Digital Twins,” Internet of Things, vol. 30, 2025, Art. no. 101547, doi: 10.1016/j.iot.2025.101547.
4. Markus Wolf, Johannes Pfrommer, Florian Hauer, and Christian Eben-bauer, “Digital Twin for Multi-Agency Incident Management,” Scientific Reports, vol. 12, 2022, doi: 10.1038/s41598-022-20178-8.
5. Cristina Alcaraz and Javier Lopez, “Digital Twin: A Comprehensive Survey of Security Threats,” IEEE Communications Surveys & Tutorials, vol. 24, no. 3, pp. 1475–1503, 2022, doi: 10.1109/COMST.2022.3171465. :content Reference[oaicite:1] index=1
6. Philipp Empl and Gu¨nther Pernul, “Digital Twin-Based Security An-alytics for IoT,” Information, vol. 14, no. 2, p. 95, 2023, doi: 10.3390/info14020095.

7. Efe Balta, David M. Tilbury, and Xenofon D. Koutsoukos, “Digital Twin-Based Cyber-Attack Detection Framework,” IEEE Transactions on Automation Science and Engineering, 2023, doi: 10.1109/TASE.2023.3243147.
8. Matteo Lucchese, Luca Seno, Alessandro Brunelli, and Michele Bertogna, “Digital Twin-Based Attack Detection in Industrial Systems,” Applied Sciences, vol. 14, no. 19, 2024, doi: 10.3390/app14198665.
9. Sandeep Kumar, Ankit Kumar, Rajesh Kumar Singh, and Sachin Shekhar, “SOAR4IoT: Securing IoT Assets Using Digital Twins,” in Proceedings of the International Conference on Availability, Reliability and Security (ARES), 2022, doi: 10.1145/3538969.3538975.
10. David Jeremiah, Michael Brown, and Ahmed Alenezi, “Digital Twin Cybersecurity Framework Survey,” Information, vol. 17, no. 3, 2026, doi: 10.3390/info17030286.
11. Joa˜o Sousa, Rui Cruz, Pedro Simo˜es, and Anto´nio Pinto, “Cybersecurity of Critical Infrastructure Using Digital Twins,” IEEE Access, vol. 9, pp. 119147–119161, 2021, doi: 10.1109/ACCESS.2021.3100600.
12. Ahmad Suhail, Rajiv Ranjan, Prem Prakash Jayaraman, and Schahram Dustdar, “Blockchain-Based Security for Digital Twins,” Computers in Industry, vol. 141, 2022, Art. no. 103699, doi: 10.1016/j.compind.2022.103699.
13. Xiaoyu Wang, Yifan Zhang, and Lei Shu, “Digital Twin-Based Safety Analysis Under Cyber Attacks,” in Proceedings of IEEE CSR, 2024.
14. Chia Lo, Kevin Huang, and Wei Tsai, “Threat Simulation in Digital Twins Using Deep Learning,” in Proceedings of IEEE ICAC, 2024.
15. S. Suganya, R. Priyadharshini, M. Kavitha, and P. Deepalakshmi, “Edge Computing Enabled Digital Twin Security Framework,” Wireless Networks, 2024.
16. Mohamed Hakiri, Pascal Berthou, Aniruddha Gokhale, and Thierry Gayraud, “Digital Twin for Future Network Security,” Computer Networks, vol. 245, 2024, Art. no. 110350, doi: 10.1016/j.comnet.2024.110350.
17. David Jeremiah, Ahmed Alenezi, Michael Brown, and Khaled Ra-bie, “Comprehensive Survey on Digital Twin Security,” Journal of Systems Architecture, vol. 156, 2024, Art. no. 103120, doi: 10.1016/j.sysarc.2024.103120.
18. Subarna Pokhrel, Jinho Choi, and Choong Seon Hong, “Digital Twin for Cybersecurity Prediction,” in Proceedings of the ACM Conference, 2020, doi: 10.1145/3387940.3391499.
19. Soumaya Jbair, Ahmed Serhrouchni, and Abdelmalek Benzekri, “Threat Modeling in Cyber-Physical Systems,” Computers in Industry, vol. 141, 2022, Art. no. 103611, doi: 10.1016/j.compind.2022.103611.
20. James Reynolds, Ethan Clarke, and Michael Foster, “Digital Twin-Enhanced Incident Response Framework,” in Proceedings of the ACM Conference, 2023, doi: 10.1145/3600160.3600180.