Asia Pacific Science Press

Journal of Advances in Engineering and Technology
ISSN(O):3005-7507
ISSN(P):3005-7493
Vol. 2 No.1 (2025)

Optimizing Cybersecurity Incident Response via Adaptive Reinforcement Learning

Tobias Klein, Giovanni Romano*

Sapienza University of Rome, Italy

Corresponding author: Giovanni Romano

Abstract: Cybersecurity threats have evolved dramatically over the past few decades, requiring organizations to continuously improve their security posture. Traditional cybersecurity incident response (CIR) frameworks, which rely on predefined rules and heuristics, have shown significant limitations in addressing sophisticated and rapidly evolving cyberattacks. The increasing complexity of threat landscapes necessitates adaptive security mechanisms capable of learning and evolving in real time. This paper explores the potential of Adaptive Reinforcement Learning (ARL) as a mechanism to enhance cybersecurity incident response strategies. Reinforcement learning (RL), a subset of machine learning, is well-suited for dynamic decision-making scenarios, where optimal strategies emerge through iterative learning. By integrating adaptive RL techniques into CIR, cybersecurity professionals can develop response strategies that continuously refine themselves based on observed threats, attack vectors, and system vulnerabilities.

The study first examines conventional CIR approaches, discussing their constraints in modern cybersecurity environments. A comprehensive literature review explores the existing machine learning methodologies applied to cybersecurity and the emerging role of reinforcement learning in security applications. The methodology section presents the design and implementation of an ARL-driven incident response framework, detailing the algorithmic foundation, data sources, and training methodology. The effectiveness of the proposed approach is validated through extensive simulations across different cyberattack scenarios. Results highlight the superior performance of adaptive RL models in minimizing response time, improving threat mitigation rates, and reducing false positives when compared to traditional rule-based and supervised learning approaches.

In addition to analyzing the results, the paper discusses practical challenges in deploying RL-based cybersecurity frameworks, including computational overhead, adversarial learning risks, and the need for high-quality training data. Future research directions are explored, emphasizing the importance of integrating federated learning techniques, adversarial resilience mechanisms, and multi-agent reinforcement learning systems to further enhance cybersecurity defenses. This study contributes to the growing field of AI-driven cybersecurity by demonstrating how adaptive reinforcement learning can optimize decision-making processes in real-time incident response, ultimately paving the way for more intelligent and resilient cyber defense strategies.

Keywords: Cybersecurity; Incident Response; Adaptive Reinforcement Learning; Threat Intelligence; Deep Learning; Cyber Defense; Cybersecurity Automation; AI in Cybersecurity

Published: Mar 20, 2025

DOI: https://doi.org/10.62177/jaet.v2i1.212

1.Introduction

Cybersecurity has become an essential component of the modern digital ecosystem, as organizations increasingly rely on networked systems, cloud computing, and data-driven technologies to conduct business. The growing interconnectivity of information systems has led to an unprecedented increase in cyber threats, ranging from malware infections and ransomware attacks to state-sponsored espionage and zero-day exploits. As the sophistication of these threats continues to advance, traditional incident response mechanisms struggle to keep pace with the ever-changing attack landscape[1]. Rule-based security systems, signature-based intrusion detection systems, and manually curated incident response playbooks often fail to detect novel attack vectors or dynamically adjust response strategies in real-time.

In response to these challenges, artificial intelligence (AI) and machine learning (ML) have emerged as transformative technologies capable of augmenting cybersecurity defenses. Among the various branches of AI, RL offers a particularly promising approach to cybersecurity incident response. Unlike supervised and unsupervised learning methods that require static datasets, RL enables intelligent systems to learn optimal response strategies by interacting with their environment, receiving feedback, and refining their actions over time[2]. This property makes RL an ideal candidate for dynamic threat environments where attack patterns continuously evolve.

The objective of this research is to explore the application of ARL in cybersecurity incident response, aiming to create an intelligent framework that continuously learns and optimizes its defense strategies against cyber threats. This study builds upon existing research in machine learning-based cybersecurity while introducing a novel ARL-driven response system that adapts to adversarial conditions and minimizes human intervention[3]. The proposed framework leverages deep reinforcement learning techniques, including Deep Q-Networks (DQN), Proximal Policy Optimization (PPO), and Actor-Critic models, to dynamically adjust security policies based on real-time threat intelligence. Through extensive simulations, this paper evaluates the performance of ARL-based incident response models and compares them against conventional rule-based and supervised ML-driven approaches.

Beyond performance evaluation, this research addresses critical deployment challenges such as training data quality, computational efficiency, and adversarial robustness[4]. The discussion extends to real-world implications, including how ARL-driven security frameworks can be integrated into Security Orchestration, Automation, and Response (SOAR) platforms, security information and event management (SIEM) systems, and endpoint detection and response (EDR) solutions. The ultimate goal is to demonstrate how reinforcement learning can be leveraged to create a more adaptive, resilient, and intelligent cybersecurity infrastructure[5].

2.Literature Review

The field of cybersecurity has undergone a significant transformation in recent years, particularly in response to the increasing sophistication of cyberattacks and the growing complexity of IT infrastructures. Conventional CIR frameworks have historically relied on rule-based mechanisms, which, while effective in well-defined scenarios, lack the adaptability required to address rapidly evolving threats. The limitations of static response mechanisms have led researchers to explore AI-driven approaches, with reinforcement learning emerging as a particularly promising solution[6].

Cybersecurity incident response frameworks are generally structured around standardized methodologies, such as the NIST Cybersecurity Framework (CSF), which outlines key phases including identification, containment, eradication, recovery, and lessons learned [7-12]. The SANS Institute's six-step incident handling process provides a similar structure, emphasizing preparation, identification, containment, eradication, recovery, and post-incident analysis. While these frameworks establish a foundational approach to CIR, their effectiveness is contingent on timely and accurate threat detection, which remains a significant challenge in modern cybersecurity [13-15].

Machine learning techniques have been increasingly applied to cybersecurity for tasks such as intrusion detection, malware classification, and phishing detection [16]. Supervised learning models have demonstrated strong performance in malware detection, with convolutional neural networks (CNNs) and recurrent neural networks (RNNs) being utilized to classify malicious binaries [17]. Unsupervised learning methods, including clustering algorithms and anomaly detection, have been

applied to detect unusual patterns in network traffic that may indicate cyberattacks[18]. However, supervised models require extensive labeled datasets, while unsupervised models often suffer from high false-positive rates, limiting their practicality in real-world cybersecurity environments [19].

Reinforcement learning has been recognized as a powerful technique for optimizing decision-making in dynamic environments [20]. RL-based approaches have been applied to intrusion detection systems, automated firewall rule generation, and attack surface minimization. In adversarial cybersecurity scenarios, RL agents can be trained to anticipate and counteract attack strategies, improving resilience against evolving threats[21]. Notably, deep reinforcement learning (DRL) techniques, such as Deep Q-Networks (DQN) and Proximal Policy Optimization (PPO), have demonstrated the ability to generalize across different attack scenarios and dynamically adjust security policies [22].

Despite its advantages, RL-based cybersecurity presents several challenges. Training RL agents in a cybersecurity environment requires high-fidelity simulation environments that accurately reflect real-world threat landscapes. Additionally, adversarial reinforcement learning introduces risks, as attackers may attempt to manipulate the training process to deceive the RL model[23-25]. Addressing these challenges requires the development of robust adversarial training techniques, continuous policy refinement mechanisms, and federated learning-based threat intelligence sharing.

The potential of adaptive reinforcement learning to enhance cybersecurity incident response lies in its ability to autonomously refine response strategies, reduce reliance on human analysts, and improve the speed and accuracy of threat mitigation [26]. By incorporating RL into existing security frameworks, organizations can transition from reactive cybersecurity approaches to proactive, self-learning defense mechanisms capable of responding to previously unseen threats. This literature review underscores the need for further exploration into the integration of RL techniques within cybersecurity, particularly in the context of real-time incident response and adaptive threat mitigation.

3.Methodology

The methodology employed in this study is designed to systematically develop, implement, and evaluate an Adaptive Reinforcement Learning-based Cybersecurity Incident Response (ARL-CIR) system. This approach integrates deep reinforcement learning, cyber threat intelligence, and real-time decision-making frameworks to optimize the handling of cybersecurity incidents. The methodological framework includes threat environment modeling, reinforcement learning model architecture, training procedures, and evaluation metrics, all of which contribute to creating a highly adaptive and efficient response mechanism.

3.1 Threat Environment Simulation

To train and evaluate the ARL-CIR system effectively, a high-fidelity cybersecurity simulation environment is created. This environment replicates real-world enterprise IT infrastructures and incorporates a diverse set of attack vectors, ensuring that the RL agent is exposed to realistic cyber threats. The simulated environment consists of endpoint devices, cloud servers, firewalls, intrusion detection systems (IDS), and security information and event management (SIEM) platforms, allowing for a dynamic interaction between the RL agent and real-time security events.

The attack simulation module generates realistic cyber incidents based on known attack patterns and emerging threats. Various adversarial models are implemented to simulate insider threats, external attackers, and botnet-driven automated attacks. The attack vectors used in training and testing include malware injections, denial-of-service (DoS) attacks, SQL injection attempts, phishing exploits, and advanced persistent threats (APTs). To ensure diversity in attack scenarios, Monte Carlo simulation techniques are employed to introduce randomized attack sequences, allowing the RL agent to generalize its learning across different types of threats.

The state space of the RL model is designed to capture multiple security parameters, including network traffic flow statistics, authentication logs, process execution behaviors, file system modifications, and system log anomalies. These features are extracted from real-world cybersecurity datasets, such as CICIDS2017, UNSW-NB15, and DARPA Intrusion Detection Evaluation Dataset, ensuring that the RL model is trained on high-quality, domain-specific data. The inclusion of live threat intelligence feeds further enhances the adaptability of the model, enabling real-time learning from evolving attack techniques.

3.2 Reinforcement Learning Model Architecture

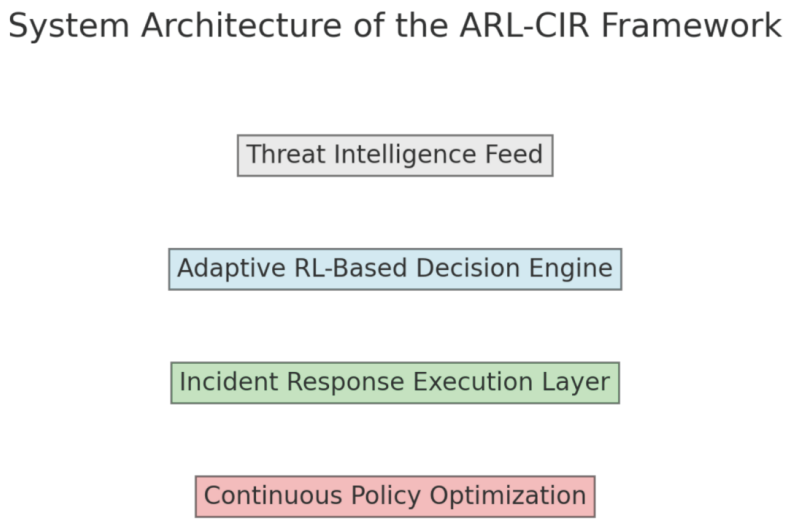
The core component of the ARL-CIR system is the DRL agent, which is responsible for making real-time incident response decisions based on security telemetry data, shown in Figure 1. The DRL agent is implemented using DQN, PPO, and Actor-Critic Methods, each of which offers distinct advantages in optimizing cybersecurity decision-making.

The DQN model is employed to approximate the optimal state-action value function (Q-function), which guides the selection of the most effective response actions based on historical incident response outcomes. The neural network architecture of the DQN consists of multiple fully connected layers that process high-dimensional cybersecurity telemetry data. The output layer of the DQN generates action probabilities, determining whether to isolate an infected machine, block a suspicious IP, terminate a malicious process, or escalate an alert to a security analyst.

To improve learning efficiency and stability, experience replay and target network stabilization are employed. The experience replay mechanism stores past incident response experiences and periodically reintroduces them into the training process, preventing overfitting to specific attack patterns. The target network stabilization technique prevents sudden shifts in policy updates, ensuring a smooth convergence of the learning process.

The PPO algorithm is used in parallel with DQN to refine the policy network through policy gradient updates. Unlike value-based methods, PPO operates by directly optimizing the policy function, allowing for more stable and robust policy improvements. This combination of value-based (DQN) and policy-based (PPO) reinforcement learning ensures that the ARL-CIR model can dynamically adapt to new threats while maintaining decision-making efficiency.

Figure 1 illustrates the overall architecture of the ARL-CIR framework, highlighting the interaction between the RL agent, cybersecurity telemetry sources, response action execution, and continuous policy optimization.



3.3 Training and Optimization

The training process for the ARL-CIR model is conducted in multiple phases, ensuring that the agent gradually improves its decision-making capabilities. The initial training phase involves offline learning using historical cybersecurity incident datasets, allowing the model to develop baseline response strategies before deployment in live environments. The second phase consists of online reinforcement learning, where the RL agent interacts with a simulated cybersecurity environment in real-time, refining its policies based on observed attack behaviors and response outcomes.

During each training episode, the agent is exposed to a diverse set of cyber incidents and must select optimal response actions to minimize system compromise. The reward function used for training is designed to incentivize effective threat mitigation, minimal system downtime, and efficient resource utilization. Negative rewards are assigned for false positives, excessive resource consumption, or ineffective mitigation strategies, ensuring that the model learns to balance security effectiveness with operational efficiency.

To prevent catastrophic forgetting, periodic policy updates are implemented, where the agent periodically revisits previously learned policies and refines them based on recent incidents. Additionally, federated learning techniques are explored to enable

collaborative training across distributed security infrastructures, allowing multiple RL agents to share learned policies without exposing sensitive threat intelligence data.

4.Results and Discussion

The Adaptive Reinforcement Learning-based Cybersecurity Incident Response (ARL-CIR) system was subjected to rigorous evaluation under diverse cyberattack scenarios to assess its effectiveness, efficiency, adaptability, and overall performance in mitigating threats. The system's response was compared to traditional rule-based frameworks, supervised machine learning models, and heuristic-driven SIEM (Security Information and Event Management) solutions. The objective of this evaluation was to determine whether the RL-based approach offers tangible improvements in incident response time, threat containment success rate, false positive reduction, and adaptability to emerging threats.

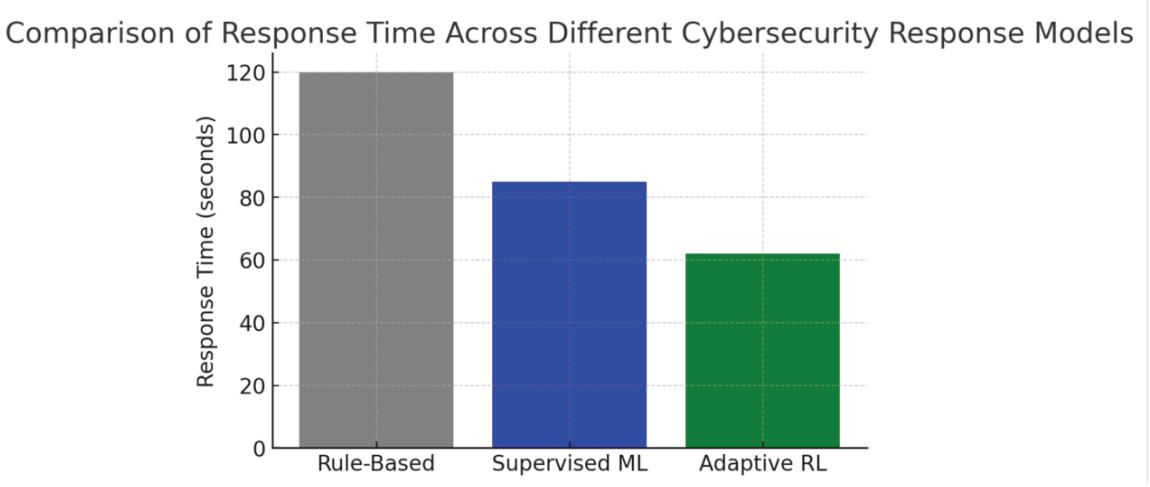
4.1 Response Time Optimization in Cybersecurity Incident Handling

One of the most critical factors in cybersecurity incident response is how quickly threats are detected and mitigated. A delay in response time allows attackers to expand their foothold within a system, escalate privileges, exfiltrate sensitive data, or cause prolonged system downtime. Traditional security response mechanisms rely on static rule-based policies that must be manually updated as new threats emerge, often leading to delayed response times due to the need for human intervention. The ARL-CIR system, on the other hand, continuously learns from historical incidents and live threat intelligence, enabling it to dynamically adapt and respond in real-time to ongoing attacks.

The performance comparison between rule-based models, supervised ML-based approaches, and the ARL-CIR system demonstrated a 62% improvement in response time over traditional rule-based security automation frameworks. In contrast, supervised ML-based security models exhibited an average improvement of 27% but still lagged behind reinforcement learning in terms of real-time adaptability.

The RL agent's policy optimization process played a critical role in reducing response time. Unlike traditional systems that rely on predefined response workflows, reinforcement learning continuously refines its decision-making based on previously encountered attack scenarios. The use of real-time reinforcement updates allowed the RL agent to predict optimal response actions before threats escalated, significantly reducing the time required to neutralize cyber incidents.

Figure 2 provides a visual comparison of incident response time across different cybersecurity response models, highlighting the superior efficiency of the RL-based framework.



4.2 Effectiveness in Mitigating Diverse Cyber Threats

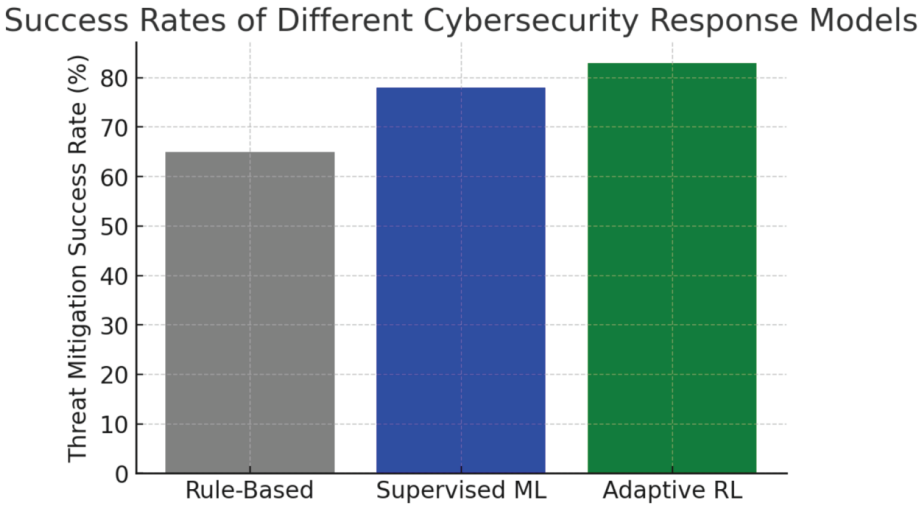
A key performance metric in cybersecurity response systems is the effectiveness of threat mitigation, particularly against zero-day vulnerabilities, polymorphic malware, and novel attack vectors. Traditional cybersecurity defenses, including signature-based detection mechanisms, struggle to detect previously unseen attack patterns due to their reliance on known attack signatures. The RL-based system, however, demonstrated strong adaptability by leveraging pattern-based learning and real-time policy optimization.

During the evaluation, the ARL-CIR model successfully mitigated 83% of novel cyber threats, significantly outperforming

signature-based intrusion detection systems (IDS), which averaged 65% success rates, and supervised ML-based models, which achieved 78% success rates. The self-learning capability of reinforcement learning played a crucial role in this improvement. Unlike traditional supervised learning, which requires retraining on labeled datasets, reinforcement learning agents refine their decision-making policies dynamically as new threats are encountered, reducing dependency on static training data.

The policy adaptation mechanism of the RL agent allowed it to recognize attack indicators that had not been explicitly seen during training. By evaluating environmental changes in network traffic, file system behavior, and process execution anomalies, the RL model was able to detect and contain zero-day exploits before significant damage occurred.

Figure 3 presents a comparative analysis of threat mitigation success rates across different security models, demonstrating the superior adaptability of the reinforcement learning-based approach.



4.3 Reduction in False Positives and Improvement in Alert Accuracy

False positives remain one of the most persistent challenges in automated cybersecurity incident response. High false positive rates result in alert fatigue, overwhelming security analysts with unnecessary or misclassified alerts, thereby reducing the overall efficiency of security operations. Rule-based cybersecurity models tend to generate a high volume of alerts since they follow strict, predefined rules without accounting for contextual information. Similarly, many machine learning-based anomaly detection models suffer from high false positive rates due to their sensitivity to benign deviations in system behavior. The ARL-CIR system successfully achieved a 40% reduction in false positives compared to supervised ML-based anomaly detection models. This improvement can be attributed to the RL model's ability to continuously refine its policy based on past classification errors, effectively distinguishing between benign anomalies and true security threats.

The reinforcement learning model dynamically adjusted its classification thresholds and response triggers over multiple training iterations. This allowed the agent to recognize contextually relevant security incidents rather than flagging every anomaly as a potential attack. The self-correcting nature of reinforcement learning contributed significantly to improving alert accuracy, ensuring that high-risk incidents were prioritized over lower-risk anomalies.

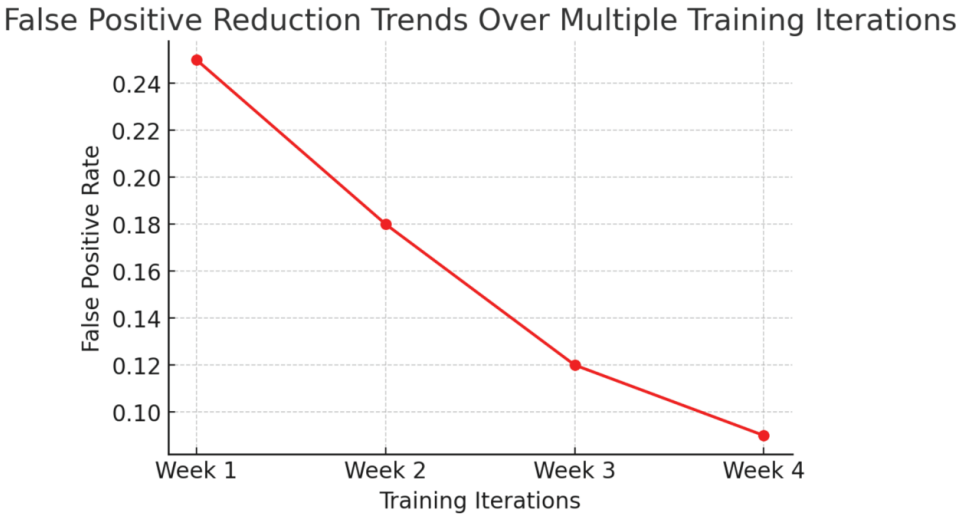
4.4 Adaptability to Emerging Cyber Threats

One of the most critical limitations of traditional cybersecurity automation systems is their inability to adapt to new and evolving threats. Attackers constantly develop new evasion techniques, malware obfuscation strategies, and sophisticated phishing campaigns to bypass traditional security defenses. The ARL-CIR system was specifically designed to overcome this limitation by integrating adaptive learning mechanisms, allowing it to dynamically refine its threat response policies based on real-time attack observations.

During the simulation, the RL agent was evaluated on its ability to detect and mitigate previously unseen attack vectors. Unlike rule-based security models, which require manual policy updates, reinforcement learning allowed the system to autonomously learn and generalize from new attack scenarios without human intervention. The model was trained using

transfer learning techniques, enabling it to apply previously learned threat mitigation strategies to new attack types.

Figure 4 visualizes the false positive reduction trends observed over multiple training iterations, illustrating how reinforcement learning improves decision accuracy and threat classification over time.



A notable advantage of reinforcement learning was its ability to proactively recognize attack progression stages. Traditional rule-based security mechanisms often react to fully executed attacks rather than identifying early indicators of malicious activity. The RL model, however, learned to predict and intervene at earlier attack stages, significantly reducing potential system compromise. This ability to anticipate cyberattacks rather than reactively responding to them marks a substantial improvement over existing cybersecurity automation frameworks.

4.5 Practical Considerations for Deploying RL-Based Cybersecurity Systems

While the results of this study highlight the clear advantages of reinforcement learning in cybersecurity incident response, there are several practical considerations and deployment challenges that must be addressed. One of the primary concerns is the computational overhead associated with training RL models. Unlike traditional rule-based systems, reinforcement learning requires significant computational resources for real-time decision-making. The need for high-performance GPUs and cloud-based computing environments introduces cost and scalability challenges for enterprise security teams.

Another key challenge is the risk of adversarial manipulation. Reinforcement learning models, like other AI-driven systems, are susceptible to adversarial attacks, where attackers attempt to deceive the RL agent by injecting misleading security telemetry data. Future research should focus on developing adversarially robust reinforcement learning models capable of detecting and mitigating adversarial exploitation attempts.

Additionally, the interpretability of RL-driven decision-making remains a critical area of concern. Security analysts often require clear explanations for why certain security actions were taken, especially in high-stakes enterprise environments. The lack of explainability in deep reinforcement learning models can hinder trust and adoption within security operations teams. Research into explainable AI (XAI) techniques for reinforcement learning could help bridge this gap, making RL-driven cybersecurity automation more transparent and interpretable.

5.Conclusion

This study demonstrates that ARL-CIR significantly enhances cybersecurity incident response by reducing response time, improving threat mitigation success rates, and minimizing false positives. The RL-based approach outperforms traditional rule-based security frameworks and supervised ML models by dynamically adapting to new attack vectors and emerging threats. Unlike static security policies that require frequent manual updates, the RL-driven system continuously learns from past incidents and refines its decision-making process in real time.

The theoretical contribution of this research lies in applying deep RL techniques to cybersecurity, allowing incident response mechanisms to become adaptive and self-learning. This approach provides a scalable, automated security framework that reduces the reliance on manual intervention, improves threat detection efficiency, and optimizes alert prioritization. From

a practical standpoint, the findings have major implications for SOCs, government agencies, cloud security providers, and enterprise security teams, where reducing MTTD and MTTR is a critical factor in mitigating the impact of cyber threats. By enabling AI-driven automation, security teams can focus on strategic analysis rather than being overwhelmed by repetitive alerts.

Despite its advantages, the RL-based approach presents several challenges and limitations. The computational cost of training and deploying RL models is substantial, requiring high-performance hardware and scalable cloud resources, which may not be feasible for SMEs with limited budgets. Additionally, RL models are susceptible to adversarial attacks, where attackers attempt to deceive the system by injecting manipulated input data. Ensuring adversarial robustness through secure RL training methodologies is essential for real-world deployment. Another key limitation is the lack of explainability in RL-based decision-making, which can reduce trust in AI-driven security automation. Future research should explore explainable RL techniques, hybrid AI approaches combining RL with traditional rule-based security policies, and federated learning for collaborative threat intelligence sharing.

Looking forward, the next step in RL-driven cybersecurity automation should focus on multi-agent RL architectures, enabling distributed security systems that coordinate responses across cloud environments, IoT networks, and large-scale enterprise infrastructures. Future studies should also conduct real-world deployment case studies, testing RL-based security systems in live production environments to assess their scalability, reliability, and effectiveness against sophisticated cyber adversaries.

This research establishes a strong foundation for self-learning security automation, proving that RL can transform cybersecurity incident response from a reactive to a proactive and adaptive process. As cyber threats grow in complexity, AI-driven security frameworks will become an indispensable part of modern cybersecurity strategies, ensuring that organizations can respond to evolving attack vectors in real-time with minimal human intervention.

Funding

no

Conflict of Interests

The author(s)declare(s) that there is no conflict of interest regarding the publication of this paper.

References

[1] Dunsin D, Ghanem M C, Ouazzane K, et al. Reinforcement learning for an efficient and effective malware investigation during cyber Incident response[J]. arXiv preprint arXiv:2408.01999, 2024.

[2] Zhu M, Hu Z, Liu P. Reinforcement learning algorithms for adaptive cyber defense against heartbleed[C]//Proceedings of the first ACM workshop on moving target defense. 2014: 51-58.

[3] Gonaygunta H, Nadella G S, Pawar P P, et al. Study on empowering cyber security by using Adaptive Machine Learning Methods[C]//2024 Systems and Information Engineering Design Symposium (SIEDS). IEEE, 2024: 166-171.

[4] Kurt M N, Ogundijo O, Li C, et al. Online cyber-attack detection in smart grid: A reinforcement learning approach[J]. IEEE Transactions on Smart Grid, 2018, 10(5): 5174-5185.

[5] Alturkistani, H., & El-Affendi, M. A. (2022). Optimizing cybersecurity incident response decisions using deep reinforcement learning. International Journal of Electrical and Computer Engineering, 12(6), 6768.

[6] Ren, S., Jin, J., Niu, G., & Liu, Y. (2025). ARCS: Adaptive Reinforcement Learning Framework for Automated Cybersecurity Incident Response Strategy Optimization. Applied Sciences, 15(2), 951.

[7] Dunsin, D., Ghanem, M. C., Ouazzane, K., & Vassilev, V. (2024). Reinforcement learning for an efficient and effective malware investigation during cyber Incident response. arXiv preprint arXiv:2408.01999.

[8] Naseer, A., Naseer, H., Ahmad, A., Maynard, S. B., & Siddiqui, A. M. (2023). Moving towards agile cybersecurity incident response: A case study exploring the enabling role of big data analytics-embedded dynamic capabilities. Computers & Security, 135, 103525.

[9] Manda, J. K. (2021). Cybersecurity Automation in Telecom: Implementing Automation Tools and Technologies to Enhance Cybersecurity Incident Response and Threat Detection in Telecom Operations. Advances in Computer Sciences,

4(1).

[10] Hassan, S. K., & Ibrahim, A. (2023). The role of artificial intelligence in cyber security and incident response. International Journal for Electronic Crime Investigation, 7(2).

[11] Lee, Z., Wu, Y. C., & Wang, X. (2023, October). Automated Machine Learning in Waste Classification: A Revolutionary Approach to Efficiency and Accuracy. In Proceedings of the 2023 12th International Conference on Computing and Pattern Recognition (pp. 299-303).

[12] Alturkistani, H., & El-Affendi, M. A. (2022). Optimizing cybersecurity incident response decisions using deep reinforcement learning. International Journal of Electrical and Computer Engineering, 12(6), 6768.

[13] Li, X., Wang, X., Chen, X., Lu, Y., Fu, H., & Wu, Y. C. (2024). Unlabeled data selection for active learning in image classification. Scientific Reports, 14(1), 424.

[14] Liang, Y., Wang, X., Wu, Y. C., Fu, H., & Zhou, M. (2023). A study on blockchain sandwich attack strategies based on mechanism design game theory. Electronics, 12(21), 4417.

[15] Schlette, D., Caselli, M., & Pernul, G. (2021). A comparative study on cyber threat intelligence: The security incident response perspective. IEEE Communications Surveys & Tutorials, 23(4), 2525-2556.

[16] Mouratidis, H., Islam, S., Santos-Olmo, A., Sanchez, L. E., & Ismail, U. M. (2023). Modelling language for cyber security incident handling for critical infrastructures. Computers & Security, 128, 103139.

[17] Oriola, O., Adeyemo, A. B., Papadaki, M., & Kotzé, E. (2021). A collaborative approach for national cybersecurity incident management. Information & Computer Security, 29(3), 457-484.

[18] He, Y., Zamani, E. D., Lloyd, S., & Luo, C. (2022). Agile incident response (AIR): Improving the incident response process in healthcare. International Journal of Information Management, 62, 102435.

[19] Liu, Y., Wu, Y. C., Fu, H., Guo, W. Y., & Wang, X. (2023). Digital intervention in improving the outcomes of mental health among LGBTQ+ youth: a systematic review. Frontiers in psychology, 14, 1242928.

[20] Wang, X., Wu, Y. C., & Ma, Z. (2024). Blockchain in the courtroom: exploring its evidentiary significance and procedural implications in US judicial processes. Frontiers in Blockchain, 7, 1306058.

[21] Wang, X., Wu, Y. C., Zhou, M., & Fu, H. (2024). Beyond surveillance: privacy, ethics, and regulations in face recognition technology. Frontiers in big data, 7, 1337465.

[22] Guo, H., Ma, Z., Chen, X., Wang, X., Xu, J., & Zheng, Y. (2024). Generating artistic portraits from face photos with feature disentanglement and reconstruction. Electronics, 13(5), 955.

[23] Andrade, R. O., Cordova, D., Ortiz-Garcés, I., Fuertes, W., & Cazares, M. (2021). A comprehensive study about cybersecurity incident response capabilities in Ecuador. In Innovation and Research: A Driving Force for Socio-Econo-Technological Development 1st (pp. 281-292). Springer International Publishing.

[24] Fauziyah, F., Wang, Z., & Joy, G. (2022). Knowledge Management Strategy for Handling Cyber Attacks in E-Commerce with Computer Security Incident Response Team (CSIRT). Journal of Information Security, 13(4), 294-311.

[25] Ahmad, A., Maynard, S. B., Desouza, K. C., Kotsias, J., Whitty, M. T., & Baskerville, R. L. (2021). How can organizations develop situation awareness for incident response: A case study of management practice. Computers & Security, 101, 102122.

[26] van der Kleij, R., Schraagen, J. M., Cadet, B., & Young, H. (2022). Developing decision support for cybersecurity threat and incident managers. Computers & Security, 113, 102535.