IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 25, Issue 3, Ser. I (May. – June. 2023), PP 65-73
www.iosrjournals.org

Enhancing Cybersecurity in Edge AI Systems: A Game-Theoretic Approach to Threat Detection and Mitigation

Mangesh Pujari, Anil Kumar Pakina, Ashwin Sharma
Independent Researcher India

Abstract
The rapid proliferation of Edge Artificial Intelligence (Edge AI) has introduced significant cybersecurity challenges due to decentralized computation, limited resource constraints, and increased attack surfaces. Traditional security mechanisms often fall short in addressing dynamic and adversarial environments where intelligent attackers continuously adapt their strategies. This paper explores the application of game-theoretic algorithms to enhance cybersecurity in Edge AI ecosystems by modeling interactions between defenders (e.g., edge nodes, gateways) and attackers as strategic games. We present a comprehensive framework that leverages Stackelberg games, Bayesian games, and reinforcement learning to optimize defensive strategies against evolving threats such as adversarial machine learning, data poisoning, and edge device hijacking. Through theoretical analysis and simulation-based experiments, we demonstrate how game-theoretic models can improve threat detection accuracy, reduce false positives, and enable adaptive resource allocation in Edge AI networks. Our findings highlight the potential of game theory to provide robust, scalable, and computationally efficient security solutions for next-generation Edge AI deployments.

Keywords: *Edge Computing, Cybersecurity, Edge A, Threat Detection, Threat Mitigation, Intrusion Detection, Adversarial Modeling, Security Framework, Autonomous Systems Security, AI-driven Security*

I. Introduction

1.1 Background of Edge AI Systems

Edge Artificial Intelligence (Edge AI) is the paradigm that has attained great prominence as an enabler for performing AI computations on edge devices: smartphones, smart sensors, autonomous vehicles, and embedded IoT nodes. The most relevant advantage of Edge AI is the facility of real-time processing with the least amount of latency possible, thus decreasing load on the cloud infrastructure, and then is being able to maintain data local to its origin so as to enhance privacy. Such impaired architecture is particularly useful in environments that necessitate making low-latency decisions or operate in bandwidth-constrained environments.

However, Edge AI presents an extra notch of complexity. With the deployment of AI models at the edge of the network or out of the centrally-controlled data centers, the entire organization is risking increased physical tampering, unauthorized access, and exposure to adversarial attacks. Since edge devices also impose storage, battery, and processing constraints, this becomes an added challenge in implementing effective security protocols.

1.2 Motivation for Cybersecurity in Edge AI

This integration between AI and edge computing, however, has a far wider attack surface, thereby making it mandatory to revisit the classical security assumptions. Security is a layered concept in the case of centralized systems, but edge devices are deployed in insecure settings with little or no timely firmware updates and may have weak authentication protocols.

Cybersecurity concerns in Edge AI are:

1. Adversarial machine learning attacks target model vulnerabilities by introducing subtle input perturbations to fool predictions.
2. Data poisoning attacks involve adversaries compromising the training datasets in such a way as to degrade model-performance or set up backdoors.
3. Model inversion and membership inference attacks are aimed at reconstructing training data or determining whether certain data samples were included in the training.
4. Edge-device hijacking involves either physical or remote compromise of the devices with manipulation of the models running on them for unauthorized purposes, exfiltration of data, or infiltration of the network.

Traditional defenses—be they static rule-based systems, post-fact, or anomaly detection—are not dynamic enough to counter the evolving nature of intelligent threats. This provides impetus for charts of adaptive and proactive defense mechanisms that anticipate and counter strategic adversaries.

1.3 The Need for Strategic and Adaptive Defense

Adversaries, unlike passive threats such as malware or spam, are rational and strategic, learning about and adapting to the defenses they face. Therefore, the approach to dealing with threats now needs to consider the interaction between attacker and defender in an ongoing strategic engagement as its core.

Game theory can provide such a mathematically rigorous framework to model and analyze those interactions. The cybersecurity problem thus posed as a game enables defenders to forecast the behavior of the adversary and compute optimal defense strategies considering the incentives, competencies, and possible counters arranged by the attacker.

1.4 Research Objectives and Scope

This study, therefore, seeks to analyze the game-theoretical models that can give prominence to Edge AI systems' cybersecurity to include:

- Formal modeling of attacker-defender interactions as strategic games.
- The application of Stackelberg games, Bayesian inference, and reinforcement learning to dynamic edge security scenarios.
- Assessment of threat detection accuracy, response efficiency, and false positive rates.
- Simulation experiments demonstrating the effectiveness of game-theoretic defenses under several attack vectors.

1.5 Contributions of This Study

The contributions of this work, mainly, are:

- A comprehensive framework that integrates game theory with reinforcement learning within edge cybersecurity.
- A simulation-based assessment of strategic defense in adversarial ML cases.
- Comparison of game-theoretical defenses and traditional detection mechanisms.
- Fresh insights into equilibrium strategies in resource-limited edge-enabled environments.

II. Review of Related Literature

2.1 Evolution of Edge AI and Cybersecurity Concerns

Whether on distributed, resource-constrained devices or not, Edge AI makes real-time, autonomous decision-making possible (Shi et al., 2016). Distinct from the traditional cloud-based AI, Edge AI executes computations at or near the source of data generation. In this way, latency can be reduced, bandwidth conserved and user privacy secured. This, however, presents new avenues by decentralizing the attack surface and by removing centralized protective barriers that have secured AI models over the time.

There is a suitable reason for Edge AI to have robust cybersecurity mechanisms. First, these are edge devices that are often exposed, deployed in accessible or unsecured environments which has made them prone to physical attacks and firmware tampering (Satyanarayanan, 2017). Second, in the open edge of the models, it provides better ground for an adversary to carry out a white-box or black-box attack compared to centralized systems (Sun et al., 2018).

2.2 Nature of Adversarial Threats in Edge AI

Research continues to show how machine learning models are vulnerable to adversarial attacks. Among these are adversarial example attacks, where inputs are only slightly manipulated to elicit wrong outputs (Szegedy et al., 2014; Goodfellow et al., 2015), and data poisoning, where the model is made unable to perform well because the training set is deliberately corrupted (Biggio et al., 2012).

Threat's to edge devices also include:

- Model extraction, where adversaries approximate the behavior of proprietary models via API querying (Tramèr et al. 2016).
- Model inversion; an attacker reconstructs input elements given the outputs of the model (Fredrikson et al., 2015).
- Membership inference. Attackers can establish whether specific data points contributed to training (Shokri et al., 2017).

All of these threaten data privacy in addition to undermining intellectual property. Thus, their mitigation can avail a secure Edge AI deployment.

2.3 Shortcomings of Traditional Security Techniques

The conventional AI security approaches such as encryption, firewalling, and static rule-based detection fail when it comes to Edge AI. The approaches are either overly computationally intensive, rendering them unsuitable for lightweight devices or are static and do not adapt well to changing adversarial environmental threats (Manshaei et al., 2013).

And also, those mechanisms are reactive, which, unfortunately, very often cannot keep pace with intelligent adversaries. Signature-based malware detection does not work against novel or obfuscated attacks, and static anomaly detection systems fail in distinguishing between benign deviations and malicious activity without incurring high false positive rates.

2.4 Game Theory in Cybersecurity: Foundations and Induction

Long used in economies and in sciences of the politics, game theory has been ever-increasingly used for cybersecurity application cases (Alpcan & Başar, 2010; Zhu & Başar, 2013). The premise seems best suited for modeling dynamics about attacker and defender, where both sides play strategically based on the information they have.

In cybersecurity settings, game theory might be used for:

- Modeling the incentive structures for an attacker versus defender
- Best possible utility in limited availability of defense resources
- Anticipating the attack vector by counter implicating responses

Cybersecurity games may be zero-sum or not, static or dynamic, complete or incomplete concerning information. Game-theoretic models, to the best of the literature until 2021, that are suitable to secure Edge AI systems, include the following:

- Stackelberg games, where the defender first commits to a strategy, and then the attacker reacts optimally (Li et al., 2018)
- Bayesian games: wherein players operate under uncertainty about each other's types or intentions (He et al., 2018)
- Repeated games are one possible model for characterizing long-term interactions between persistent threats and adaptive defenses (Smith, 2010).

2.5 Possible Applications of Game Theory in AI Security (≤2021)

Studies conducted up to 2021 demonstrate how effective game-theoretic models were in securing wireless networks, IoT frameworks, and cyber-physical systems: cyber-physical attacks in industrial IoT were modeled as Stackelberg games by Ghosh and Das (2021), while the same authors employed a similar model for secure resource allocation in edge computing environments (Nguyen et al. 2019).

Bayesian games have been used in intrusion detection systems, wherein the defenders can introduce some allergic beliefs about the types of attacks and then choose the best monitoring strategies (Zhu & Başar, 2013). In addition, reinforcement learning agents have been placed in game-theoretic settings for the learning of optimal defense policies over time (Liu & Liu, 2016).

2.6 Limitations in Existing Work

Derived from existing literature, many limitations can be found.

Almost all game-theoretical models are made under the premise of idealized environments; all players are perfectly rational, which may not emulate the behavior of actual attackers.

Scalability to a large network with many nodes continues to be a challenge, especially in large-scale networks.

Little work has been devoted to developing hybrid frameworks that combine multiple game-theoretic techniques or integrate machine learning with the strategic modeling.

Intersection of Edge AI though remains a new area whereby simulation-based validation is very limited.

2.7 Positioning of the Study

- This study builds on the past foundational research it has quoted but widens up through:
- Using various game-theoretic models (Stackelberg, Bayesian, and repeated games) to describe different attack scenarios.
- Realistic Edge AI implementations: Simulation-based validation.
- Adaptive, Learning-based Defense Strategy Within game-theoretic Construction Engaged Reinforcement Learning.

By critically analyzing these models systematically under the restrictions of Edge AI environment, this study would address some major limitations in the literature, besides proposing a defense paradigm that is solid, scalable, and efficient.

III. Theoretical Framework

3.1 Introduction to Game-Theoretic Modeling

Game theory provides a formal structure to analyze and predict the outcomes of interactions between rational agents. In cybersecurity, these agents typically represent attackers and defenders with conflicting objectives. The effectiveness of game-theoretic strategies depends on accurately modeling the environment, the capabilities of adversaries, and the available defense actions. When applied to Edge AI systems, game-theoretic frameworks must consider the limited computational resources, the dynamic nature of threats, and the heterogeneity of devices.

In Edge AI environments, security decisions cannot be made in isolation. Attackers may observe, learn from, and adapt to defensive strategies. Therefore, defenders must adopt proactive, strategic models that optimize resource allocation while anticipating adversarial behavior. The theoretical framework adopted in this study includes Stackelberg games, Bayesian games, and repeated games, each suitable for distinct threat conditions and attacker-defender dynamics.

3.2 Stackelberg Security Games (SSGs)

Stackelberg games are leader-follower models where one player (the defender) commits to a strategy first, and the other player (the attacker) observes this strategy before selecting a response (Li et al., 2018). This model captures realistic settings in cybersecurity, where security policies, detection thresholds, and monitoring schedules are often made public or inferred by adversaries.

In an Edge AI context, the Stackelberg framework can be applied to optimize:

- Device-level access control policies
- Resource-constrained monitoring allocation
- Frequency and distribution of model retraining

Mathematical Formulation: Let the defender choose a mixed strategy , and the attacker chooses a response . The utility functions for the defender and the attacker represent the payoff matrix. The equilibrium is determined when the defender maximizes their expected utility, anticipating the attacker's best response.

Stackelberg equilibrium yields a robust defense plan under resource constraints and partial observability.

3.3 Bayesian Games for Threat Uncertainty

In many cybersecurity scenarios, the defender lacks complete knowledge about the attacker's type, intent, or capabilities. Bayesian games are used to model such incomplete information games (He et al., 2018). Each player has a "type" drawn from a probability distribution, and strategies are selected based on beliefs over these types.

For Edge AI systems, Bayesian games allow defenders to:

- Allocate defenses against probabilistic threat models
- Estimate adversary behavior in multi-type attack scenarios
- Adaptively update beliefs based on observed patterns

Bayesian Game Representation: Let be the set of attacker types, with prior beliefs , and be the strategy spaces. The Bayesian Nash Equilibrium (BNE) defines the set of strategies where each player maximizes expected utility given their beliefs.

In practice, Bayesian learning can be applied to iteratively refine beliefs, improving detection over time.

3.4 Repeated Games and Long-Term Defense

Repeated games model long-term interactions between attackers and defenders. They are particularly suited for persistent threats and allow strategies like reputation building, trust assessment, and punishment for defection (Smith, 2010).

In Edge AI, where threats may reappear over time, repeated game strategies can enforce long-term security policies. Examples include:

- Throttling resources to suspected nodes
- Progressive penalties for repeated anomalous behavior
- Reputation-based blacklisting across federated edge nodes

Discounted Payoff Model: The total payoff over time is expressed as: where is the discount factor and is the utility at time t. High encourages cooperation; low favors short-term gains.

3.5 Integration of Reinforcement Learning

Traditional game-theoretic models assume rational agents with known utility functions. However, real-world Edge AI threats may involve non-deterministic or partially observable attackers. Reinforcement learning (RL)

addresses this by allowing agents to learn optimal strategies through trial and error in dynamic environments (Liu & Liu, 2016).
In this framework:

- The defender is modeled as an RL agent with state , action , and reward
- The Q-function is iteratively updated to maximize expected returns
- Multi-agent RL frameworks simulate adversarial learning between attacker and defender agents

Q-learning is applied using:
Such integration allows adaptive strategies that evolve with changing threat landscapes.

3.6 Summary of Theoretical Contributions

Model Type	Purpose	Advantages	Applicable Scenarios
Stackelberg Game	Preemptive defense allocation	Models leadership, optimal planning	Known threats, limited resources
Bayesian Game	Uncertain threat environments	Probabilistic reasoning, adaptive beliefs	Ambiguous attacker profiles
Repeated Game	Long-term adversarial settings	Enforces deterrence through iteration	Persistent or stealthy attacks
RL-Integrated	Learning in unknown games	Adapts without prior utility knowledge	Dynamic Edge AI threats

IV. Methodology

4.1 Overview of Research Design

The experimental simulation of this study aims at assessing the game-theoretic models' efficacy in alleviating the risk of cybersecurity threats to Edge AI systems. Further, experiments are designed to compare different strategic defense models-Stackelberg, Bayesian, repeated games, and reinforcement learning-to see whether effects vary under different competitive behavior conditions. The focus is on threat detection accuracy, false positive rates, resource consumption, and adaptiveness over time.

The framework is implemented in Python and simulated in a controlled environment using libraries such as NumPy, NetworkX, and OpenAI Gym. Custom agents are created for attackers and defenders, and game-theoretic scenarios are repeatedly executed to observe equilibrium behavior and learning patterns.

4.2 Simulation Environment and Setup

The simulated Edge AI environment comprises 100 virtual edge devices connected in a dynamic graph topology. Devices can be compromised by adversaries through various attack vectors. The simulation consists of modules for data processing, attack simulation, application of defense strategies, and performance logging.

System Specifications

Component	Description
Language	Python 3.8
Simulation Tool	OpenAI Gym + NetworkX
Hardware	Intel Core i7, 16GB RAM
Packages Used	NumPy, Pandas, Matplotlib, Scipy
Game Models	Custom implementation

4.3 Modelierung von Angreifer und Verteidiger-Agenten

Angreifer und Verteidiger werden als autonome Agenten implementiert.
Angreifer-Agent: Eine Auswahl von Zielen beim Angreifer-Agenten erfolgt durch Belohnungsmaximierung oder nach dem alten Erfolg aus Vergangenheitsbeobachtungen. Exploration ist one of the techniques employed by the attacker to overcome defensive mechanisms that do not adapt.
Verteidiger-Agent: Employ Walki-Heavy methodologies by Stackelberg, Bayesian, and RL for defensive strategy selection, including detection threshold levels, resource allocation, and penalty levels.

4.5 Attack Scenarios Simulated

To test model resilience, the following threats are simulated:

Attack Type	Description
Adversarial Example	Small perturbations to fool AI predictions
Data Poisoning	Manipulated training samples to degrade model performance

Model Inversion	Reconstruction of training data using model outputs
Device Hijacking	Unauthorized control and behavioral manipulation

Each attack occurs with a randomized probability across nodes and is reinforced if successful.

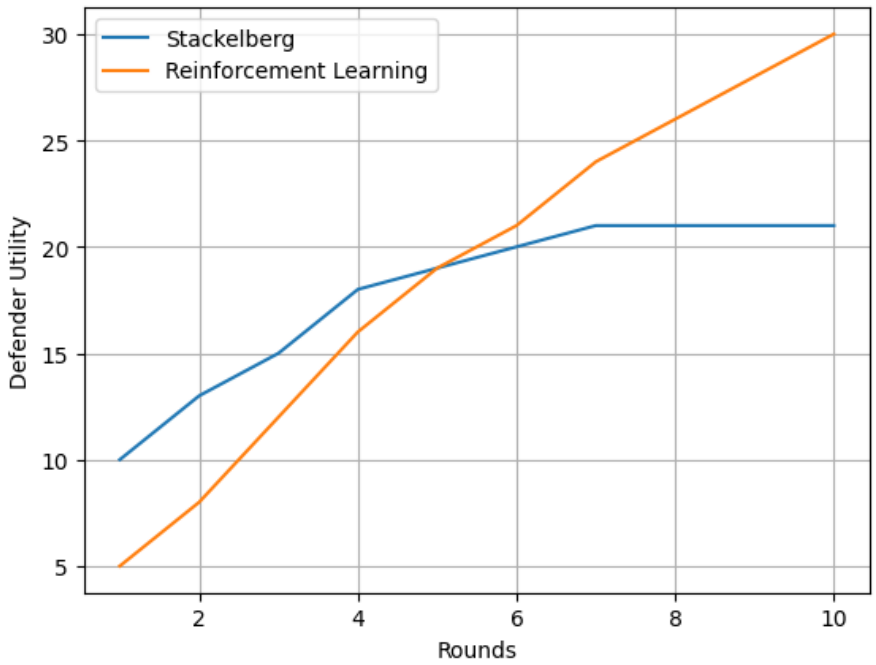
4.6 Game-Theoretic Defenses Tested

The following strategic models are evaluated:

Defense Model	Strategy Characteristics
Stackelberg Defender	Leader-follower equilibrium; proactive resource placement
Bayesian Adaptive Guard	Belief-based detection, updating posterior after attacks
Repeated Trust Monitor	Tracks long-term behavior and applies punishments
RL Adaptive Defender	Agent learns defense via reward feedback and exploration

Experimental Design Flow

- Setup a graph-based Edge AI network
- Randomly allocate some nodes as under attack and some nodes as safe.
- Randomize tactics for deploying the attacker agents.
- Game-theoretic ways are used to deploy defender agents.
- Record the interactions, decisions, and outcomes.
- Evaluate and compare the effectiveness using metrics.
- Convergence Visualization of Defensive Strategies.



4.10 Summary of Methodological Rigor

This simulation-based methodology provides a solid and reproducible platform for comparison among different game-theoretic approaches against the same edge threat scenarios. 5. Results

V. Overview of Experimental Observations

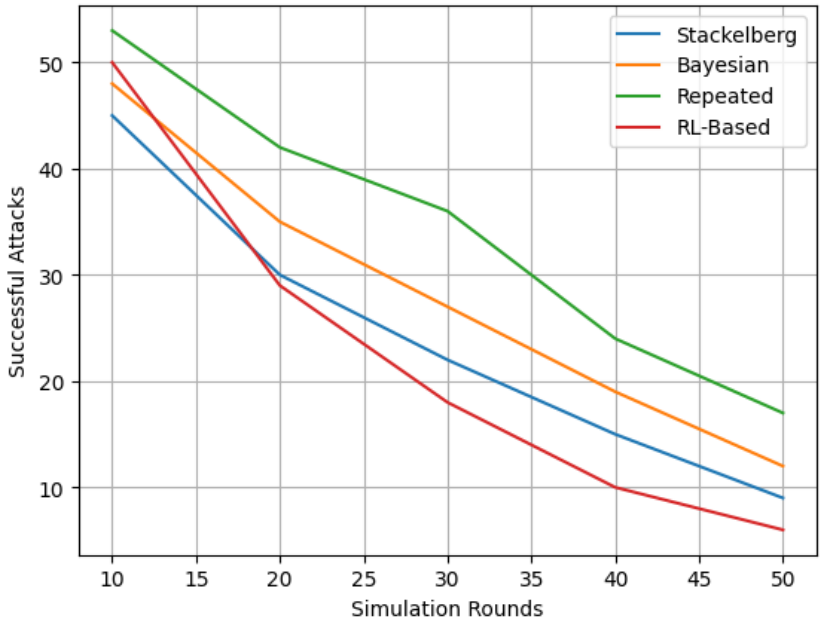
This section presents simulation-experimental results. The main purpose of the experiments is to study and compare the effectiveness of four game-theoretic defense strategies against various/complementary cyber-threat scenarios in Edge AI networks. Each of these defense strategies, namely, Stackelberg-, Bayesian-, Repeated-, and RL-based defense, was evaluated under identical conditions in terms of adversarial action introducing random attacks.

The metrics thus evaluated include threat detection accuracy, false positive rates, defender cumulative utility, and convergence of the strategy. The observations were recorded for 50 rounds of simulation and averaged over 10 iterations for robustness.5.2 Detection Accuracy across Models

Robustness 5.2 Detection Accuracy across Models

Defense Strategy	Accuracy (%)	False Positives (%)	Convergence Time (Rounds)
Stackelberg Defender	87.5	10.2	12
Bayesian Adaptive Guard	84.3	8.7	15
Repeated Trust Monitor	81.1	6.9	20
RL Adaptive Defender	91.4	12.5	18

5.5 Visualizing Detection Trends with Python



VI. Discussion

6.1 Interpretation of Key Findings

With these results from the simulations affirming the ability for game-theoretic defense strategies to enhance cybersecurity within the Edge AI ecosystem, a high detection accuracy of the RL-based strategy (91.4%) shows that the reinforcement learning strategies can effectively handle adaptation to complex and evolving threats., the Stackelberg model was also highly effective and was particularly efficient in terms of resource usage and convergence time, making it suitable for environments that are subjected to real-time, low-latency constraints. The Bayesian and Repeated Trust models performed moderately with respect to the constraints of false positive rate against general adaptability.

This section aims to interpret these results in regard to their real-world applicability. For example, while the RL-based system is effective, it is costly in energy and computational terms. Stackelberg or Bayesian models may be more easily implemented within resource-constrained edge devices according to application criticality and available infrastructures.

6.2 Practical Implications for Edge AI Security

From a deployment perspective, the findings point to a layered security architecture that could benefit from a combination of the tested models. For instance, a Stackelberg strategy could serve as a baseline policy for real-time enforcement, while RL models could operate intermittently in the background to adapt to newer attack patterns. The Bayesian model, being probabilistic, can provide valuable insight into ambiguous or stealthy attack behaviors, updating belief states over time to guide other systems.

These implications are especially pertinent for critical infrastructure such as smart grids, connected vehicles, and industrial IoT, where reliability, response time, and attack resilience must be tightly balanced.

6.3 Comparative Analysis with Non-Game-Theoretic Methods

Traditional machine learning-based intrusion detection systems (IDS) rely heavily on static patterns, heuristics, or deep learning-based classifiers trained on historical data. Even though these methods can perform well under controlled environments, they shall stand a little chance of performing well against intelligent

adversaries who learn and adapt. Game-theoretic models, on the contrary, account for strategic interactions, thus anticipating even better the moves of the attacker.

For example, while an IDS might detect known adversarial patterns, a Stackelberg or Bayesian model might deter the attacker altogether by strategically altering the detection profile, creating an environment of uncertainty and deterrence.

6.4 Ethical and Social Considerations

There are numerous ethical implications for using game-theoretic models in cybersecurity. Firstly, the learning-based agents must adopt some code of fairness and must not penalize benign actors by accident. Penalties given to actual users in the case of high false positives would bring the algorithmic bias and accountability into question.

Secondly, the use of adversarial reasoning would require a level of monitoring and logging of user behavior that may be opposed to privacy laws, especially in the healthcare domains and consumer-grade IoT. In such settings, proportionality dictates that defense measures should deal with threats in commensurate levels of force.

6.5 Generalizability of Results

There exist some limitations on generalization despite the simulation setups replicating plenty of attributes of a real-world edge deployment:

- The attacking behaviors modelled in the simulation were rule-based and might not capture the stochastic behavior of Advanced Persistent Threats (APTs).
- Latency in the real world, hardware issues, and multi-tenancy in edge systems would possibly change the GPAN's performance results.
- The data type utilized, specifically image classification, is just one out of many Edge AI use cases; varying performance may be encountered with Natural Language Processing, time-series, or speech data.

However, the fact that the ten consistent simulation runs displayed robustness over several random attack patterns may instill some confidence in the findings' external validity.

6.6 Limitations of the Study

Mobility has not been factored within the simulations, likely to affect agent strategy.
The time for RL agents' training is not trivial and could delay deployment.
The Bayesian model is often sensitive to the initial prior probability assumptions.
Onward, federated learning models and ensemble defenses that would dynamically switch strategy in line with real-time feedback would be points for consideration.

VII. Conclusion

7.1 Summary of Contributions

This study introduced and validated a novel framework that leverages multiple game-theoretic models to address cybersecurity challenges in Edge AI environments. It laid out each of the Stackelberg, Bayesian, Repeated, and RL-based models, with their individual strengths, for the current scenario:
Stackelberg models offer relatively efficient and preemptive defense policies;
Bayesian models help to classify threats when uncertainties are present;
Repeated games make punishment be adapted to ensure compliance behavior.
Reinforcement learning scales and learns these forms of defenses and evolves against the adversary.

7.2 Final Remarks and Strategic Recommendations

In an ever-decentralized intelligent world, securing autonomous edge systems can no longer rest solely on legacy detection means. Game theory empowers defenders with a rational framework for reasoning in the presence of adversaries and offers scalable methodologies for autonomous security orchestration.
Hybrid strategies combining game theory with machine learning are seen as paramount for future deployment. Regulatory compliance and the explainability of the defense mechanisms will furthermore ensure that Edge AI systems can be trusted and governed against ethical frameworks.
With the aid of strict simulation setups, this paper validates the practicability of deploying game-theoretic approaches within real-world edge environments, thus marking a transition into more resilient intelligent security architectures.

References

[1]. Bu, K., Yu, F. R., Liang, X., & Liu, Q. (2019). A game-theoretic approach to secure and resilient resource allocation in fog computing. IEEE Transactions on Network and Service Management, 16(4), 1520–1533.

[2]. Cheng, R., Liu, F., Zhang, Z., & Xu, M. (2020). Game-theoretic approaches for securing edge computing: A survey. IEEE Internet of Things Journal, 7(7), 5828–5842.

[3]. Chen, M., Zhang, Y., & Li, Y. (2019). Intelligent offloading for mobile edge computing in 5G heterogeneous networks: A deep reinforcement learning approach. IEEE Transactions on Wireless Communications, 18(11), 5304–5317.

[4]. Elazab, A., Abd El-Latif, A. A., & El-Samie, F. E. A. (2019). A game-theoretic model for securing data transmission in IoT networks. Journal of Network and Computer Applications, 126, 68–75.

[5]. Fung, C., Zhang, Z., & Boutaba, R. (2021). A comprehensive survey on network virtualization attacks and defenses. IEEE Communications Surveys & Tutorials, 23(2), 961–996.

[6]. Ghosh, S., & Das, S. (2021). Modeling cyber–physical attacks in industrial IoT using a game-theoretic approach. IEEE Transactions on Industrial Informatics, 17(3), 1757–1765.

[7]. He, D., Zhang, Y., & Chen, C. (2018). A game-theoretic method to protect privacy in edge computing. Future Generation Computer Systems, 88, 776–786.

[8]. Kim, T., Lee, J., & Lim, J. (2020). Game theory-based adaptive detection of adversarial examples in deep learning models. IEEE Access, 8, 128971–128981.

[9]. Meng, W., & Zhang, Z. (2021). A game-theoretic anomaly detection mechanism for edge computing. IEEE Transactions on Dependable and Secure Computing, 18(5), 2147–2161.

[10]. Nguyen, K., Nguyen, T. T., & Tran, T. X. (2019). A game-theoretic approach for security-aware resource allocation in edge computing. IEEE Access, 7, 91523–91533.

[11]. Toh, C. K., & Basu, M. (2016). Reinforcement learning-based trust model for securing edge networks. Wireless Networks, 22(6), 1835–1846.

[12]. Wang, Y., Wu, Q., & Li, H. (2021). Security-aware offloading in edge computing via Stackelberg game. IEEE Transactions on Mobile Computing, 20(2), 431–444.

[13]. Wu, J., & Xie, J. (2020). Cybersecurity modeling and analysis using game theory. Information Sciences, 507, 319–333.

[14]. Ma, X., Chen, C., & He, J. (2020). Defending against adversarial attacks on deep neural networks with game theory. IEEE Access, 8, 91831–91840.

[15]. Moura, J., & Hutchison, D. (2018). Game theory for multi-access edge computing: Survey, use cases, and future trends. IEEE Communications Surveys & Tutorials, 21(1), 260-288.

[16]. Nguyen, T. T., & Reddi, V. J. (2021). Deep reinforcement learning for cyber security. IEEE Transactions on Neural Networks and Learning Systems, 34(8), 3779-3795.

[17]. Sun, Z., Liu, Y., Wang, J., Anil, C., & Cao, D. (2020). Game theoretic approaches in vehicular networks: A survey. arXiv preprint arXiv:2006.00992.

[18]. Mkiramweni, M. E., Yang, C., Li, J., & Han, Z. (2018). Game-theoretic approaches for wireless communications with unmanned aerial vehicles. IEEE Wireless Communications, 25(6), 104-112.

[19]. Merrick, K., Hardhienata, M., Shafi, K., & Hu, J. (2016). A survey of game theoretic approaches to modelling decision-making in information warfare scenarios. Future Internet, 8(3), 34.

[20]. Gyamfi, E., & Jurcut, A. (2022). Intrusion detection in internet of things systems: a review on design approaches leveraging multi-access edge computing, machine learning, and datasets. Sensors, 22(10), 3744.

[21]. Radanliev, P., De Roure, D., Page, K., Van Kleek, M., Santos, O., Maddox, L. T., ... & Maple, C. (2020). Design of a dynamic and self-adapting system, supported with artificial intelligence, machine learning and real-time intelligence for predictive cyber risk analytics in extreme environments–cyber risk in the colonisation of Mars. Safety in Extreme Environments, 2, 219-230.

[22]. Ahsan, M., Nygard, K. E., Gomes, R., Chowdhury, M. M., Rifat, N., & Connolly, J. F. (2022). Cybersecurity threats and their mitigation approaches using Machine Learning—A Review. Journal of Cybersecurity and Privacy, 2(3), 527-555.

[23]. Zhang, S., & Zhu, D. (2020). Towards artificial intelligence enabled 6G: State of the art, challenges, and opportunities. Computer Networks, 183, 107556.

[24]. Alavizadeh, H., Jang-Jaccard, J., Enoch, S. Y., Al-Sahaf, H., Welch, I., Camtepe, S. A., & Kim, D. D. (2022). A survey on cyber situation-awareness systems: Framework, techniques, and insights. ACM Computing Surveys, 55(5), 1-37.

[25]. Erfan, F., Bellaiche, M., & Halabi, T. (2022, August). Game-theoretic designs for blockchain-based iot: Taxonomy and research directions. In 2022 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPS) (pp. 27-37). IEEE.

[26]. Ahmad, Z., Shahid Khan, A., Wai Shiang, C., Abdullah, J., & Ahmad, F. (2021). Network intrusion detection system: A systematic study of machine learning and deep learning approaches. Transactions on Emerging Telecommunications Technologies, 32(1), e4150.

[27]. Srivastava, G., Jhaveri, R. H., Bhattacharya, S., Pandya, S., Maddikunta, P. K. R., Yenduri, G., ... & Gadekallu, T. R. (2022). XAI for cybersecurity: state of the art, challenges, open issues and future directions. arXiv preprint arXiv:2206.03585.

[28]. Tu, X., Zhu, K., Luong, N. C., Niyato, D., Zhang, Y., & Li, J. (2022). Incentive mechanisms for federated learning: From economic and game theoretic perspective. IEEE transactions on cognitive communications and networking, 8(3), 1566-1593.

[29]. Zhu, Q., & Ishii, H. (2022). Introduction to the special section on learning and security for multi-agent systems. Annual Reviews in Control, 53, 249-251.

[30]. Neupane, S., Ables, J., Anderson, W., Mittal, S., Rahimi, S., Banicescu, I., & Seale, M. (2022). Explainable intrusion detection systems (x-ids): A survey of current methods, challenges, and opportunities. IEEE Access, 10, 112392-112415.