Volume 4 Issue VIII, August 2025, No. 71, pp. 927-939
Submitted 22/7/2025; Final peer review 16/8/2025
Online Publication 18/8/2025
Available Online at http://www.ijortacs.com

# ZERO-DAY ATTACK MANAGEMENT CHALLENGES AND PROPOSED SOLUTION

[1*]Nyia Okechukwu Cosmos., [1]Gilbert Aimufua., [2]Julius Adebowale M., [3]Victor Emmanuel Kulugh
[1*,1]Centre for Cyberspace; Nasarawa State University, Keffi (NSUK), Nigeria
[2]Department of Computer Science, Baze University Abuja
[3]Department of cybersecurity, Bingham University, Karu
[1*]okechukwunyia@gmail.com, [1]aimufuagio@gmail.com, [2]telljulius@gmail.com,
[3]vkulugh30@gmail.com
Corresponding Author Email: [1*]okechukwunyia@gmail.com,

**Abstract**

Zero-day attacks pose one of the most formidable challenges in modern cybersecurity due to their unpredictability and the absence of prior signatures. Traditional vulnerability management approaches often fail to respond dynamically or deceive attackers effectively in real time and therefore requires more study to explore options to help manage the situation. The aim of this paper is a study on zero-day attack management challenges and solution. The methodology is systematic review method, which involves empirical studies on the different method of zero-day attack management, specifically machine learning and deception approach, then challenges such as false alarm, complexity, lack of scalability are issues raised. To solve this problem a stochastic game theory approach was suggested. In conclusion, the Stochastic Game Theory (SGT) will help improved reliability of zero-day attack management and the study recommends that an approach to managing zero-day vulnerabilities in cyber systems through SGT and cyber deception mechanisms. By modelling attacker-defender interactions as probabilistic sequential games, the framework accommodates uncertainty, adaptive strategies, and multi-layer threat dynamics

**Keywords: Zero-day attack, stochastic game theory, machine learning, deception, scalability**

## 1. INTRODUCTION

Globally, one of the main challenges facing computer system networks is Zero-Day Attack (ZDA). [1]Revealed ZDA as an unknown cybersecurity vulnerability, which hackers exploit to illegally penetrate and attack a network. The term "Zero-day" implies that these vulnerabilities are hidden or not known to the network administrator, hence leaving them zero time of notice to fix the flaws before they are exploited for attack [2]. Zero-day attacks have potentials for monumental consequences when successfully carried out on critical network assets [15]. This is because by their nature, they have not been previously known by the network's hardware or software vendors or the network operators. According to [3, 16, 17], there are issues of poor performance in conventional approaches (honeypot, honeytoken, mimicking, etc) for detecting, preventing, or mitigating them, nor are there robust response mechanisms in place to subdue their impact on the enterprise' digital infrastructure. Although previous researches have applied several techniques such as machine learning-based techniques, camouflaging, moving target defence

methods, honeypot, honey token, honey-web, and honey net. [4, 18-21] revealed that these have failed to provide real-time zero-day detection effectively and also the deception models due to their static nature are easily identified by attackers. There is need for more research to investigate existing methods in literature, identify their weakness and propose solution to help improved reliability of zero-day management. The paper contributions are as follows;

i. Empirical Review on machine learning based models for Zero-Day management
ii. Empirical Review on deception based models for Zero-Day management
iii. Recommendation of solution to help solve the problem

## 2. Methodology of research

The methodology of this work is the systematic literature review approach which began with the empirical review of machine learning based models for management of zero-day attack. Secondly the study review machine learning based solutions for zero day management. From each review, findings were made and recommendation was provided to help improved reliability of zero day attack management.

### 2.1.1 Empirical Review on machine learning based models for Zero-Day management

[5] Proposed a hybrid model combining deep learning with an autoencoder for detecting zero-day vulnerabilities. The model was tested on CICIDS2017 and NSL-KDD datasets, and compared against a one-class SVM. It used three hidden layers and optimized parameters including a 1024 batch size and L2 regularization. Results showed strong anomaly detection with minimized classification loss. The approach proved effective in identifying zero-day attacks. [6] Extended CyberBattleSim to integrate cyber deception techniques like decoys, honeypots, and honeytokens. The study evaluated attacker behaviour using reinforcement learning under deceptive environments. Metrics included attacker wins, wasted resources, and defender detections. The results confirmed that deception influences attacker strategies. The study suggested adding autonomous defenders for real-world applicability. [7] Implemented autoencoders to build a deep learning-based intrusion detection system for zero-day attacks. They benchmarked performance against one-class SVM using CICIDS2017 and NSL-KDD datasets. The model achieved up to 99% accuracy on NSL-KDD and 98% on CICIDS2017. Autoencoders effectively distinguished anomalies from normal patterns. The approach proved scalable and robust. [8] reviewed the state-of-the-art in deception-based intrusion detection systems. The study explored psychological, legal, and technical aspects of deception in cybersecurity. It highlighted deception as a proactive defense to detect and analyze attacker behaviour. Risks associated with deception use were also discussed. The review emphasized careful deployment to avoid unintended consequences. [2] Examined the impact of zero-day attacks on ML and DL models, focusing on model stealing, data poisoning, and adversarial inputs. The study presented mitigation strategies like federated learning, anomaly detection, and model verification. It

Corresponding Author Tel: +2348037448051

warned of threats to ML reliability across domains. The research stressed privacy-preserving and robust model development. It offered a comprehensive threat-defense analysis. [9] applied machine learning using TensorFlow to detect social media-based zero-day attacks via Twitter data. The study combined word classification with NLTK for multilingual text processing. It achieved an 80% detection success rate. Results demonstrated real-time detection potential using public data. The system allowed timely alerts to security providers. [10] proposed a cyber deception system using honeypots and honeynets for industrial IoT security. The model simulated IoT attack surfaces in Ukraine to study attacker behaviour. It planned to use ML for generating realistic traffic and detecting deception-aware tools. The approach aimed to build a believable honeynet environment. The study reinforced deception as a strategic detection layer.

Table 1: Summary of the Review

| **Author** | **Method** | **Limitation** | **Application** |
|---|---|---|---|
| [5] | Hybrid deep learning + autoencoder for zero-day detection; tested on CICIDS2017 & NSL-KDD; optimized with 3 hidden layers, batch size 1024, L2 regularization | Requires large computational resources for training; performance dependent on parameter tuning | Network intrusion detection with focus on zero-day attacks |
| [6] | Extended CyberBattleSim with cyber deception (decoys, honeypots, honeytokens) using reinforcement learning; metrics: attacker wins, wasted resources, detections | Lacks autonomous defenders for full real-world simulation | Evaluating attacker behaviour under deceptive cybersecurity environments |
| [7] | Autoencoder-based intrusion detection for zero-day attacks; compared to one-class SVM; achieved 99% (NSL-KDD) & 98% (CICIDS2017) | May require dataset-specific tuning; limited validation on real-world streaming data | Scalable and robust anomaly detection in networks |
| [8] | Review of deception-based intrusion detection systems covering technical, legal, and psychological aspects | Potential legal/ethical concerns; risk of unintended consequences in deployment | Proactive defense to detect and analyze attacker behaviour |
| [2] | Analysis of ML/DL vulnerability to zero-day attacks (model stealing, data poisoning, | Implementation complexity; trade-off between privacy and | Strengthening ML model robustness across domains |

| | | | |
|---|---|---|---|
| | adversarial inputs) and mitigation via federated learning, anomaly detection, model verification | accuracy | |
| [9] | ML-based detection of social media zero-day attacks using Twitter data, TensorFlow, and NLTK; 80% success rate | Limited to Twitter-based indicators; accuracy may drop for unseen attack patterns | Real-time detection of social media-originated zero-day attacks |
| [10] | Cyber deception for industrial IoT using honeypots/honeynets; simulating Ukraine IoT attack surfaces; plans to integrate ML for realistic traffic | ML integration not yet implemented; focuses on simulation phase | Industrial IoT threat analysis and deception-based defense |

### 2.1.2 Identified challenges of machine learning based solutions

Despite the promising performance of machine learning models in zero-day vulnerability detection, several limitations persist across existing studies. [5] and [7] highlight that although autoencoders and one-class SVMs achieve good accuracy, they face difficulties in minimizing false positives and maintaining performance across diverse datasets. The static nature of their training also limits real-time adaptability to unseen threats. [6] demonstrate that reinforcement learning-based attackers can be misled using deception, but the absence of autonomous defenders and realistic attacker modeling restricts the simulation's applicability to real-world scenarios. [8] emphasize the conceptual potential of deception-based intrusion detection but point out practical deployment challenges, including attacker evasion, ethical concerns, and the lack of dynamic response mechanisms. [2] notes that machine learning models are vulnerable to model stealing, data poisoning, and adversarial inputs, which can degrade model integrity and create new attack surfaces. Additionally, [9] show that while social media data enhances early detection, language diversity, noise in unstructured data, and reliance on public platforms can affect detection accuracy. Lastly, [10] stress that while honeypots aid in attacker profiling, building believable IoT honeynets and generating realistic traffic patterns remain technically challenging. These findings reveal a pressing need for more robust, adaptive, and secure ML-based frameworks for managing zero-day threats.

### 2.1.3 Review on deception approach for zero-day management

[11] Proposed a game-theoretic model for cyber deception in mitigating zero-day attacks by strategically allocating honeypots under a constrained deception budget. Their approach mapped honeypot placement onto an attack

graph and analyzed the resulting impact on attacker and defender rewards. The model considered unknown zero-day vulnerabilities, focusing on their influence on game dynamics. It identified critical vulnerability nodes and proposed mitigation techniques. Simulation results showed improved attacker capture rates across different deception budgets. [4] Conducted a broad evaluation of deception techniques aimed at enhancing honeypot effectiveness. The study categorized methods such as optimization, diversification, dynamization, and sculpting based on their deployment strategies. Simulation-based comparisons highlighted performance trade-offs among approaches. The review excluded anti-honeypot detection methods but provided a strategic outlook on deception deployment. Recommendations were made for improving honeynet systems and addressing unresolved research gaps. [12] Reviewed 30 years of cyber deception practices through a novel two-dimensional taxonomy based on a four-layer deception stack and the cyber kill chain model. The taxonomy linked deception techniques to specific attack stages and layers, aiding strategic planning. Emphasis was placed on deception lifecycle and layered defenses for stronger cyber resilience. Future directions highlighted include human-centric deception design and hardware-supported mechanisms. This framework offers a comprehensive guide for both researchers and practitioners. [13] Examined the deployment of deception strategies in enterprise environments, focusing on threat assessment and security design. Techniques like breadcrumbs, obfuscation, perturbation, and the honey-x method were discussed for protecting assets. The study incorporated game-theoretic frameworks such as signaling and Stackelberg games. These models helped guide deception responses tailored to organizational needs. The paper emphasized aligning security strategies with dynamic adversarial behaviour. [14] Emphasized the role of game theory in introducing uncertainty into cyber defense through deception. The work expanded classical models by allowing defenders to manipulate game payoffs using misinformation and decoys. It introduced a hypergamy model to quantify the effects of deception on attacker decision-making. Unlike previous assumptions, the attacker was not presumed fully informed. The study called for adaptive learning models to better predict attacker behaviour and optimize deception deployment.

### 2.1.4 Challenges identified from the studies

Despite their valuable contributions, these works reveal several critical limitations. The game-theoretic honeypot allocation model in [11] assumes a static attack graph and does not consider adaptive attacker behaviour or dynamic changes in system topology, which may limit its real-world applicability. The review in [4] provides extensive coverage of deception strategies but omits anti-honeypot detection techniques, leaving a gap in addressing adversaries' counter-deception tactics. While [12] offers a comprehensive taxonomy of cyber deception linked to the cyber kill chain, it lacks empirical validation and focuses more on classification than on operational deployment. The study in [13] highlights deception strategies tailored to enterprise systems using game theory but does not account for the resource constraints and deployment overhead in large-scale

Corresponding Author Tel: +2348037448051

environments. Finally, [14] introduces a hypergamy model for dynamic deception, yet it lacks real-time adaptability and still requires the development of attacker profiling and learning mechanisms to enhance decision-making under uncertainty. These gaps suggest the need for a more integrated, adaptive, and resource-aware stochastic framework that can respond to evolving threats in complex cyber environments.

## 3. The proposed deception technique for zero-day attack management

The proposed system is made of three different approaches which are an improved game theory approach, honeypot and honeytoken. The improved game theory optimizes decision making to differentiate between attacker and legitimate user. Upon attacker identification, access to decoy facility is granted which looks exactly like the main network facility and developed using honeypot techniques. To ensure that the attacker remains on the decoy facility, decoy vulnerabilities are strategically placed on the network environment using honeytoken technique. This ensures that the attacker remains on the fake network facility, while the threat intelligence and response are automatically initiated. The figure 1 presents the proposed system block diagram.

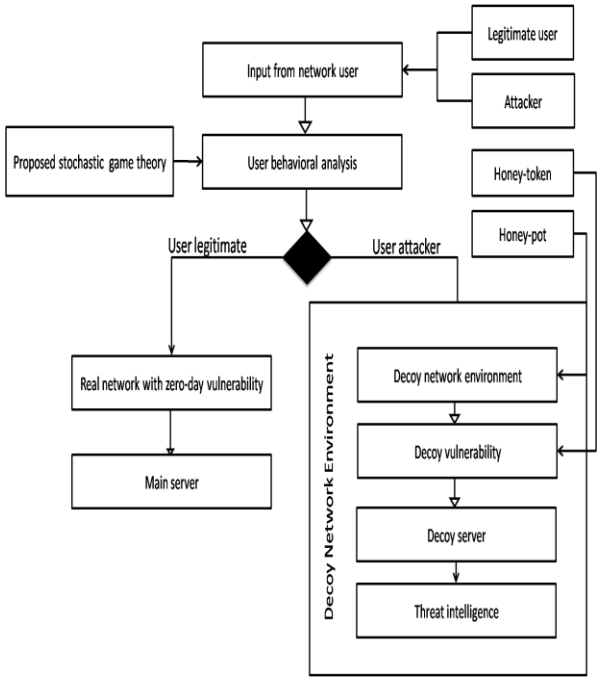


Figure 1: Proposed deception technique for zero day attack management

From the illustration in Figure 1, the mathematical models from Equations 1-3, where Equation 1 is the Trust Score Calculation model

$$T_i = \frac{\sum_{j=1}^{n} w_j f_j(x_i)}{\sum_{j=1}^{n} w_j} \quad (1)$$

Where $T_i$ = trust score of agent i; $f_j(x_i)$ = normalized feature j for agent i(e.g., detection rate, false alarm rate); $w_j$ = weight of feature j based on importance

Then, the model for Utility function is presented in Equation 2 as:

$$U_i(s_i, s_{i-1}) = \alpha \cdot P_i - \beta \cdot C_i + \gamma \cdot T_i \quad (2)$$

$U_i$ = utility of agent i; $P_i$ = payoff from successful detection/mitigation; $C_i$ = cost of defense or false positives; $T$ = trust score from Eq. 1; α,β,γ = scaling factors

Finally, Nash Equilibrium Condition model is presented in Equation 3 as

$$U_i(s_i^*, s_{-1}^*) \geq U_i(s_i, , s_{-i}^*) \forall s_i \in S_i \quad (3)$$

- $s_i^*$ = optimal strategy for agent i

- $S_i$ = set of all possible strategies for agent i
- The system is in equilibrium if no agent can improve its utility by unilaterally changing strategy.

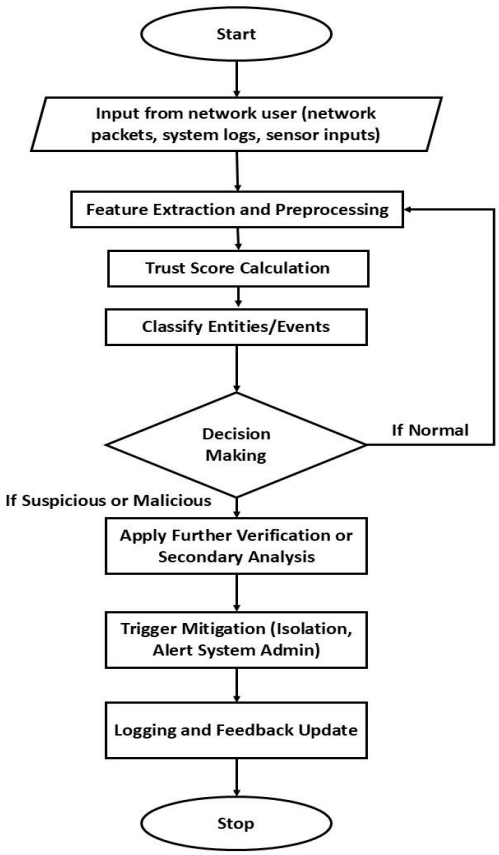


Figure 2: Flowchart of the Behavioural Model

The flowchart in Figure 2 presents the network approach to threat detection and response, beginning with the intake of various data sources such as network packets, system logs and sensor inputs. These inputs undergo feature extraction and pre-processing, followed by trust score calculation to assess their credibility and based on this score, the system classifies the input as either normal or suspicious/malicious. Normal inputs put the process on a loop, while suspicious ones trigger further verification or secondary analysis. If confirmed as threats, mitigation actions such as isolation or alerting administrators are executed and the process concludes with logging and feedback updates, reinforcing an adaptive and dynamic security framework that continuously learns and improves its threat response capabilities.

Figure 3 presents the architecture which showed the management of zero-day vulnerability through stochastic game theory, adaptive honeypot and honeytoken. When users (attacker or legitimate normal user) tries to access the network, based on their behaviour the stochastic game theory was applied to analyze user activity and upon classification as normal user is granted access to the real network with zero day vulnerability. However, upon classified as attacker is granted access to the deception network developed with honeypot techniques. To ensure that the attacker is trapped on the network, honeytoken was applied to create vulnerabilities, which the attacker keep on exploiting while wasting time and their threat information collected at the back end as the threat intelligence.

### 3.1 Simulation of the deception based zero-day attack management system

Python environment was used to implement the deception model for zero-day vulnerability. This was achieved using libraries such as NumPy, Matplotlib, and NetworkX for effective data processing, statistical analysis, and network visualization, respectively. The decoy network environment was first created using a graph-based technique, in which nodes were color-coded balls to represent honeypots, legitimate users,

and zero-day vulnerabilities. Stochastic game theory was used in the behavioural analysis to model interactions between attackers and authorized users. This allowed for the management of zero-day vulnerabilities with the use of honeytokens and the redirection of possible threats toward honeypots. The study employed simulations to quantitatively assess several performance metrics, such as Attack Diversion Rate (ADR), Honeytoken Activation Rate (HAR), Mean Time to Detect (MTTD), Mean Time to Respond (MTTR), and False Positive Rate (FPR).

## 4. Results And Discussions

This section begins with the result of the behavioral analysis, showing the cumulative number of feature classified by the Stochastic Game Theory (SGT) as attacker reward and as legitimate user reward. Then the next results discussed the performance evaluation of the deception based network with integrated SGT, honeypot and honeytoken technique made of adaptive honeypot and honeytoken, against zero-day attack. Experiments were performed on the network using several threat features and results were evaluated.

### 4.1 Results of the features behavioural analysis with SGT

In order to optimise the choice of the conventional game theory technique in the categorisation of attackers and genuine users, the SGT model in equation 3.10 was suggested. to assess the model following integration with the dynamic state transition state in equation 3.7 in the network environment. To assess the efficacy of the SGT during behavioural analysis, 200,000 feature vectors of cumulative attackers and regular users were introduced through simulation over 100 seconds. Figure 7 presented the findings. The findings revealed the accumulation of rewards for normal users and reward for attackers over the number of iterations rounds for attack. The findings showed that although the benefits for attackers declined those for genuine users and defenders grew considerably. Furthermore, the results of the legitimate user behavioural analysis demonstrated that the SGT correctly grants access to the user and consistently rewards them, while the attacker's declining results suggest that the masquerading attempt was unsuccessful because the SGT sent the user to a decoy facility, incurring costs rather than rewards, which led to the graph's steady decline in rewards.

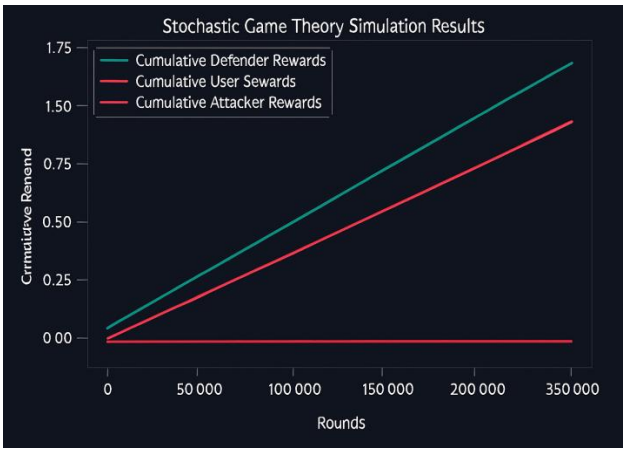


Figure 3: Result of the behavioural analytical model with SGT

Figure 3 demonstrated that the SGT model could accurately categorise the actions of attackers, defenders, and authorised users and provide them the proper access. The dynamic user actions were represented as a stochastic process, and its Nash equilibrium was then chosen as the ideal threshold for making

decisions and classifying users according to their activities, which produced excellent results.

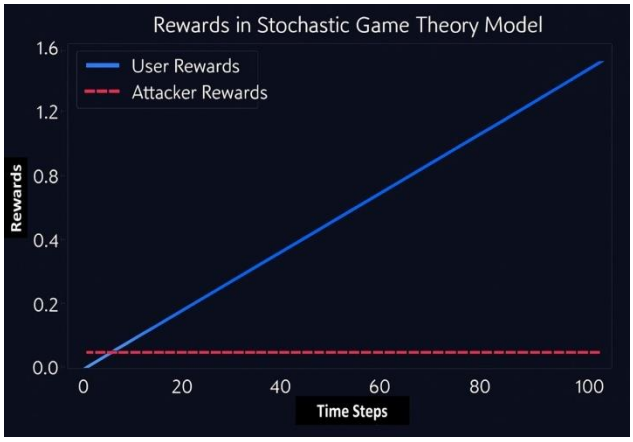


Figure 4: Result of the SGT during zero-day attack

The behavioural analysis's performance following a 100-second simulation with a zero-day assault was shown in Figure 4. According to the results, each user's behaviour was recognised and categorised as either that of an attacker or a legal user. In order to assess the efficacy of the methodology, incentives were given for each successful right action. While the awards for regular users constantly grew, it was found that the rewards for attackers consistently declined. This suggested that although the legal user succeeded in achieving its objective since it was categorised as a regular user and granted access to the network, the attacker was unable to do so because the SGT discovered it and classed it as a decoy facility. The heat map chart in Figure 6 was also applied to evaluate the SGT model for behavioural analysis.

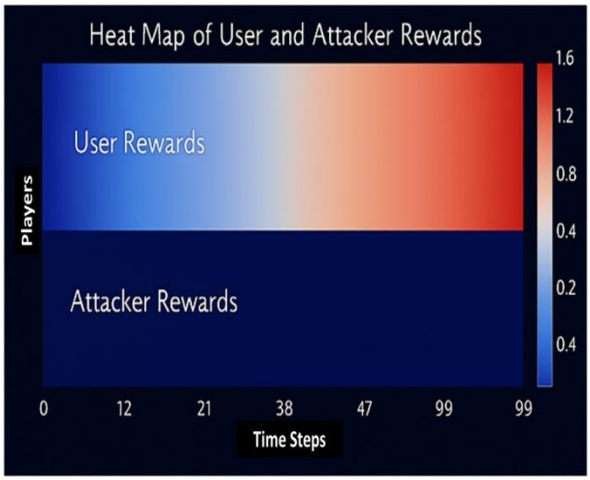


Figure 5: Heat map of the SGT behavioural analytical performance

Two of the primary actors in this heat map of attackers and authorised users were taken into account for the analysis. The colour candle range of 0 to 1.6 was used to calculate the reward score. According to the results, the heat map was entirely deep blue in the attacker reward context, with score values ranging from 0-0.6. The bad heat map data suggested that the attacker had a very low reward since it continuously failed to accomplish its goal, which led to the low reward being recorded. It was noted that, in the context of the genuine user reward heat map, the rewards were consistently extremely good with the heat map of rewards at the ideal level after the first few seconds of being here. This suggested that our algorithm could accurately identify a typical user who could access the network without any restrictions or diversion to pose as a danger. Figure 7 shows the mean rewards for the attacker and user engagement as determined by the behavioural study based on SGT.

Corresponding Author Tel: +2348037448051

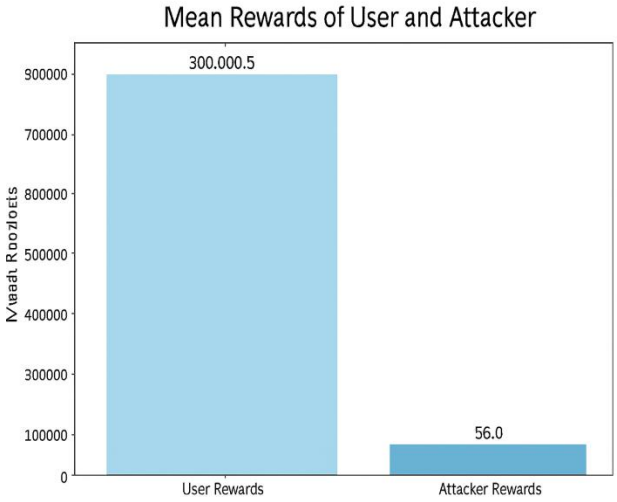


Figure 6: Mean reward evaluation score

The user rewards over 900,000 features of the zero-day assault were measured using the mean reward assessment result in Figure 6, with the attacker reward recording 56 awards and the user reward recording 800000.5 score. This outcome suggests that acceptable user conduct was appropriately categorised as typical, granting the defender access to the network. Additionally, it demonstrated that legitimate users were not mistakenly sent to a decoy facility in order to pose as attackers. The notably low attacker rewards score indicated that the attacker was unable to accomplish its objective of penetrating as a regular user to take advantage of the network vulnerability.

## 4.2 Simulation of the network environment with SGT based deception technique

Attackers are granted access to a decoy facility after being classified by the SGT in the preceding section, whilst authorised users are granted access to a regular network server for data administration. A combination of honeypot and honeytoken was used to create the deception strategy. The genuine network was recreated as a decoy system using the adaptive honeypot architecture in Equation 1, and the honeytoken was utilised as the decoy vulnerability that traps the attacker on the network while safeguarding the primary infrastructure. A 100-second zero-day assault was used to test the deception model in the network environment, and the results are shown in Figure 7.

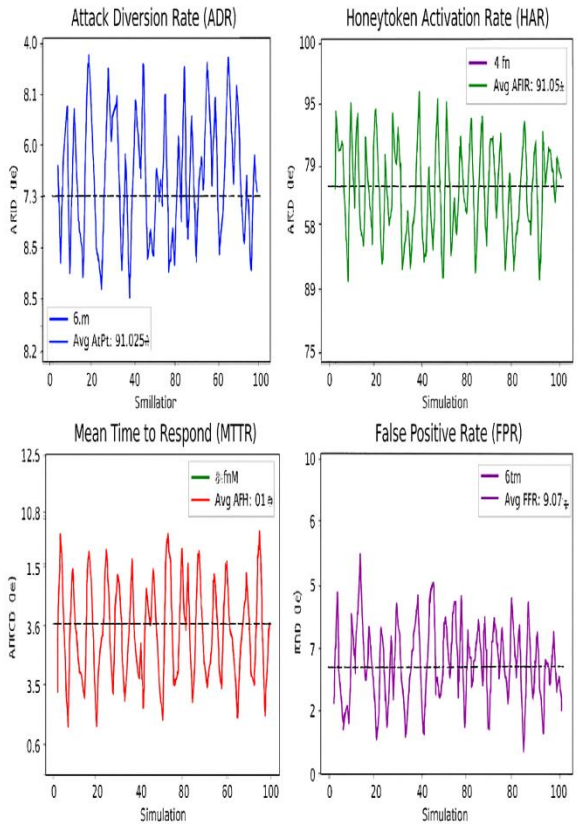


Figure 7: Result of the deception solution against zero-day vulnerability

The outcome of the deception strategy was shown in Figure 8. The SGT classified the player's conduct during the zero-day attack and redirected it to the decoy facility. According to the reported ADT of 91.56%, the SGT successfully identified the player activity ac threat and redirected to the fake network throughout the network's 100-second zero-day

attack scenario. The rate of honeypot activation was measured at 87.45%, and the average detection speed of the SGT, which is the MTTD, was 5.96s. The evaluation of the deception solution's performance against zero-day attacks also took into account the mean reaction time, which was 10.04 seconds, and the average false-positive rate, which was 3.07%. The MTTR reported the response time of the zero-day attack by the SGT, while the FPR measures the percentage of legitimate activities classified as attack.

## 5. Conclusion

This study has recommended an approach to managing zero-day vulnerabilities in cyber systems through stochastic game theory **and** cyber deception mechanisms**.** By modelling attacker-defender interactions as probabilistic sequential games, the framework accommodates uncertainty, adaptive strategies, and multi-layer threat dynamics. The integration of deception through honeypots, honeytokens, and decoys was strategically optimized under limited resource constraints, enhancing the defender's capacity to mislead, delay, and detect sophisticated adversaries. The stochastic nature of the model enables continuous state transitions and rewards computation based on evolving attack surfaces, which traditional static models fail to capture. Recommendation is made to implement and test the recommended solution through experiments. Overall, this research contributes to the body of cybersecurity by introducing a dynamic, intelligent, and proactive defense framework tailored to the unpredictable and evolving threat of zero-day attacks.

## REFERENCE


1. Sarhan M., Layeghy S., Gallagher M., & Portmann M., (2022) From zero-shot machine learning to zero-day attack detection. International Journal of Information Security (2022) 22:947–959 https://doi.org/10.1007/s10207-023-00676-0
2. Kovářová M., (2024) Exploring Zero-Day Attacks on Machine Learning and Deep Learning Algorithms. Proceedings of the 23rd European Conference on Cyber Warfare and Security, ECCWS 2024
3. Sayed A., Anwar A., Kiekintveld C., Bosansky B., &Kamhoua C., (2023) Cyber Deception Against Zero-Day Attacks: A Game Theoretic Approach. Springer Nature Switzerland AG 2023https://doi.org/10.1007/978-3-031-26369-9_3
4. Javadpour A., Jafari F., Taleb T., ShojafarM., & Benzaid C., (2024) A comprehensive survey on cyber deception techniques to improve honeypot performance. Computers & Security 140 (2024) 103792https://doi.org/10.1016/j.cose.2024.103792
5. SakthiMurugan S., Sanjay K., Vishnu V.,& Santhi P., (2023) Assessment of Zero-Day Vulnerability using Machine Learning Approach. EAI Endorsed Transactions on Internet of Things
6. Walter, E., Ferguson-Walter, K., & Ridley, A. (2021). Incorporating deception into cyberbattlesim for autonomous defense. arXiv preprint arXiv:2108.13980.
7. Hindy H., Atkinson R., Tachlatzis C., Colin J., Bayne E., &Bellekens X., (2020) Utilising Deep Learning Techniques for Effective Zero-Day Attack Detection. Electronics 2020, 9, 1684; doi:10.3390/electronics9101684
8. Oluoha, O.U., Yange, T.S., Okereke, G.E. and Bakpo, F.S. (2021) Cutting Edge


Corresponding Author Tel: +2348037448051

Trends in Deception Based Intrusion Detection Systems A Survey. Journal of Information Security, 12, 250-269. https://doi.org/10.4236/jis.2021.124014

9. Topcu, A.E.; Alzoubi, Y.I.; Elbasi, E.; Camalan, E. Social Media Zero-Day Attack Detection Using TensorFlow. Electronics 2023, 12, 3554. https://doi.org/10.3390/electronics12173554
10. Morozov D., Vakaliuk T., Yefimenko A., Nikitchuk T., &Kolomilets R., (2023) Honeypot and cyber deception as a tool for detecting cyber attacks on critical infrastructure. doors-2023: 3rd Edge Computing Workshop, April 7, 2023, Zhytomyr, Ukraine
11. Sayed A., Anwar A., Kiekintveld C., Bosansky B., &Kamhoua C., (2023) Cyber Deception Against Zero-Day Attacks: A Game Theoretic Approach. Springer Nature Switzerland AG 2023https://doi.org/10.1007/978-3-031-26369-9_3
12. Zhanh L., & Thing V., (2021) Three Decades of Deception Techniques in Active Cyber Defense - Retrospect and Outlook. arXiv:2104.03594v1
13. Alshammari, A., Rawat, D. B., Garuba, M., Kamhoua, C. A., &Njilla, L. L. (2020). Deception for cyber adversaries: status, challenges, and perspectives. Modeling and Design of Secure Internet of Things, 141-160.
14. Ferguson-Walter, K., Fugate, S., Mauger, J., and Major, M. (2019). Game theory for adaptive defensive cyber deception. In Proceedings of the 6th Annual Symposium on Hot Topics in the Science of Security (pp. 1-8).
15. Singh U., Joshi C., & Kanellopoulos D., (2019) A framework for zero-day vulnerabilities detection and prioritization. Journal of Information Security and Applications 46 (2019) 164–172https://doi.org/10.1016/j.jisa.2019.03.011
16. Roumani Y., (2021) Patching zero-day vulnerabilities: an empirical analysis. Journal of Cybersecurity, 2021, 1–13 https://doi.org/10.1093/cybsec/tyab023
17. Reddy B., Shaik S., & Gaddam V., (2024) Reinforcement Learning for Zero-Day Vulnerability Detection in IoT Devices: A Proactive Approach. Research Square: https://doi.org/10.21203/rs.3.rs-4086508/v1
18. Perkins, R. C., & Howell, C. J. (2021). Honeypots for cybercrime research. Researching Cybercrimes: Methodologies, Ethics, and Critical Approaches, 233-261. FErguson-M
19. Zahoora U., Rajarajan M., Pan Z., & Khan A., (2022) Zero-day Ransomware Attack Detection using Deep Contractive Autoencoder and Voting based Ensemble Classifier. Applied Intelligence https://doi.org/10.1007/s10489-022-03244-6
20. Sivamohan, S., Sridhar, S.S., Krishnaveni, S. (2022). Efficient Multi-platform Honeypot for Capturing Real-time Cyber Attacks. In: Hemanth, D.J., Pelusi, D., Vuppalapati, C. (eds) Intelligent Data Communication Technologies and Internet of Things. Lecture Notes on Data Engineering and Communications Technologies, vol 101. Springer, Singapore. https://doi.org/10.1007/978-981-16-7610-9_21
21. Tan, F., Zhou, L., and Xia, J. (2022). “Adaptive quantitative exponential synchronization in multiplex Cohen-Grossberg neural networks under deception attacks”. ElSevier. Journal of the Franklin Institute 359 (2022) 10558–10577 www.elsevier.com/locate/jfranklin.