Proceedings of CONF-CDS 2025 Symposium: Data Visualization Methods for Evaluation
DOI: 10.54254/2755-2721/2025.PO25664

A Survey of AI-Based Zero-Day Attack Detection Methods

Xueli Lin

School of Cyber Engineering, Xidian University, Xi'an, China
a15860286886@163.com

Abstract. Low disclosure rate and strong destructive force Zero-day attacks endanger people's property security, privacy rights, network service quality, and other interests. Although there are advanced artificial intelligence-based anti-zero-day-attack methods, there are a series of problems, such as the data sparsity problem, poor generalization ability. Although much research on AI zero-day attack detection since 2019 exists, there is still a lack of systematic study across multiple dimensions. In this paper, the research results of AI-based cybersecurity research on zero-day attack recognition from 2019 to 2025 are chronologically compiled, and how different cooperation mechanisms could best perform between the few-shot-learning method and the adversary-training method. Inspired by cybersecurity, deep learning with game theory, economic incentive structure mechanisms, and social behavior law ideas, this study proposes a new hybrid mode detection adaptivity system for cybersecurity based on the analysis. which can provide countermeasures and experimental suggestions to improve the effectiveness of various detection practices, and played an effective role in improving the intelligence level of the field of cybersecurity.

Keywords: Zero-day attacks, artificial intelligence, cybersecurity, machine learning, anomaly detection

1. Introduction

As zero-day attacks have received more attention because of its advantage of using unknown vulnerabilities and some stealthy characteristics with terrible impact on people's lives, most experts have listed them among today's top cybersecurity threats. The data reported by MITRE ATTACK reveals that only around 18% of advanced persistent attacks (APT) used zero-day exploits in 2020, but the value has increased to 34% by 2023. Conventional methods of detecting intrusion patterns typically take more than 72 hours to react, resulting in a high probability of interception failure. In general terms, there exist two major methods for traditional detection, i.e., signature detection and anomaly behavior detection. Such techniques not only suffer from a lack of past relevant feature information and a high false positive rate but also rely heavily on the environment, so they prove almost ineffective against zero-day exploits [1,2]. New progress towards artificial intelligence introduces new paradigms while combining big data into various fields, so it brings multi-source heterogeneous data for online real-time analysis, leading from passive reaction to aggressive prediction during the initial phase of attack initiation.

© 2026 The Authors. This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (https://creativecommons.org/licenses/by/4.0/).

DOI: 10.54254/2755-2721/2025.PO25664

Against this background, this paper systematically reviews AI-based zero-day attack detection research from 2019 to 2025, with the literature focusing on four aspects: technological evolution, detection-paradigm optimization, systematic experimental comparison, and future development directions. By surveying emerging detection and defense paradigms such as multi-domain fusion, federated learning, and automated defense, it aims to leverage AI technologies to address the shortcomings of traditional detection techniques when confronting unknown attacks and to drive cybersecurity protection toward automation and intelligenc. It provides a technical roadmap for academia and industry, highlighting future research directions, including few-shot learning model optimization and dynamic adversarial training.

2. Challenge

Zero-day attack detection remains inherently challenging, as these attacks occur frequently when confronting new opponents or dynamic scenarios. Detecting attacks faces many challenges, mainly from the stealthy nature of attacks, limited data and models, and technical asymmetries.

2.1. Challenges of attack characteristics

Zero-day attacks are tough for AI detection tools because they’re super sneaky, spread quickly, and absence of preknown signs or labels. In the December 2020 Solar Winds incident, a highly stealthy APT conducted a long-term supply chain infiltration by exploiting unknown vulnerabilities and mimicking legitimate behavior, rendering traffic-statistics-based or rule-matching methods ineffective. Zero-day attacks also propagate rapidly, requiring detection systems to respond within millisecond-level windows. However, existing AI models struggle to meet real-time demands due to high computational complexity. The lack of preexisting labels necessitates reliance on unsupervised or self-supervised learning, yet these approaches are sensitive to benign activity noise, leading to a higher false alarm rate. Meanwhile, the early 2021 exploitation of Microsoft Exchange zero-day vulnerabilities (ProxyLogon series) affected more than 250,000 servers worldwide, causing detection rates of related systems to drop by over 30% in a short period. This emphasizes how the fast spread of zero-day attacks and label scarcity create critical challenges.

2.2. Challenges of data and models

At the data level, extreme scarcity of zero-day attack samples and class imbalance bias supervised learning models toward majority classes, necessitating generative data augmentation or transfer learning. However, their generalization degrades markedly in cross-domain scenarios. At the model level, adversarial attacks deceive detection models by injecting perturbations [3]. Research indicates that exposing models to adversarial samples can decrease accuracy drastically—from around 90.3% to 64.1%—highlighting the severse compromise of model effectiveness [4]. As illustrated in Figure 1, attackers consistently bypass static AI models using adaptive, real-time strategies, necessitating the adoption of online incremental learning methods [5].

DOI: 10.54254/2755-2721/2025.PO25664

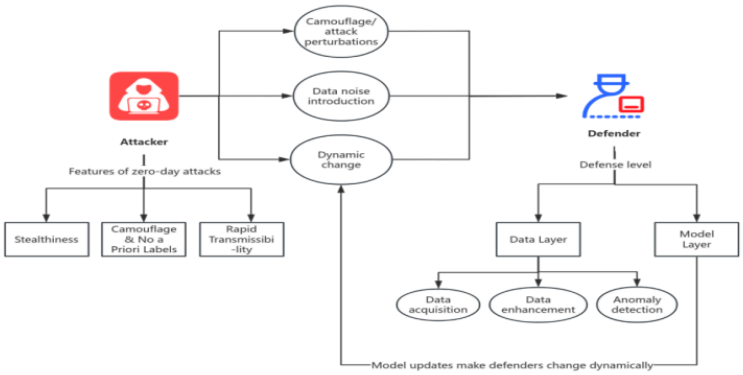


Figure 1. Schematic diagram of the “attack-defense game” framework

3. Ai-driven detection methods and technologies

The article summarizes a total of five categories of AI-based zero-day attack detection methods (including supervised learning, unsupervised learning, deep learning, reinforcement learning, and hybrid approaches) in terms of their advantages, disadvantages, and application scenarios.

3.1. Supervised learning

Supervised learning is a machine learning approach that trains models on labeled data to learn the mapping between inputs and outputs, with its hallmark reliance on large volumes of high-quality labeled samples. For example, in a zero-day attack detection study in an IoT environment using the MQTT-IoT-IDS2020 dataset, a deep Convolutional Neural Network (CNN) was employed to extract features from high-dimensional traffic data, followed by a multilayer fully-connected neural network for classification, achieving strong performance on known attacks. However, manual methods for labeling traffic attack types, like class-resampling or cost-sensitive strategies, tend to fall short when it comes to detecting new or unforeseen threats [7]. At the same time, training on extensive, well-labeled datasets enables fine-tuning models using methods like Stochastic Gradient Descent (SGD) and Adam, leading to high detection accuracy. However, the process involves considerable costs for data annotation, and there's always a risk of overfitting to familiar attack patterns, which can limit the model's ability to identify new threats [8]. In work using two mainstream IDS datasets (CICIDS2017 and NSL-KDD), Hindy et al. combined outlier detection with supervised learning to enhance anomalous traffic discrimination while extracting known features, yet still faced challenges of substantial labeled sample requirements and limited generalization [9]. Consequently, some studies have explored semi-supervised paradigms, where a small amount of labeled data guides the model to learn zero-day intrusion characteristics, thereby improving known-attack recognition and making the training process more transparent. Nevertheless,given the limited availability of zero-day samples, these models often find it challenging to effectively identify new types of attacks.

3.2. Unsupervised learning

Unsupervised learning is a method in machine learning where the system analyzes data independently to find underlying structures and patterns, without needing pre-labeled examples. In intrusion detection systems based on Generative Adversarial Networks (GANs), researchers have integrated temporal convolutional networks with self-attention mechanisms to capture both temporal

DOI: 10.54254/2755-2721/2025.PO25664

dependencies and global correlations in traffic data, thereby feature extraction modules that model unknown attack patterns. The advantage of unsupervised learning lies in its ability to discover anomalous patterns without large-scale annotated data; however, it is prone to mode collapse and instability during training [10]. A common remedy is the adoption of the Wasserstein GAN with gradient penalty (WGAN-GP), which has been shown experimentally to reduce the incidence of mode collapse by approximately 40% [35], while also enhancing sample diversity and stabilizing training. In zero-day malware detection, Mousa et al. used unsupervised methods like autoencoders to identify abnormal patterns in data, displaying notable flexibility and adaptability. However, this approach often results in a high false positives rate and requires extensive tuning to perform effectively. Unsupervised learning can also be used for zero-day attack detection and simulation by generating synthetic attack samples to improve predictive capability for novel threats, although simulation results may deviate from real-world scenarios [12]. During the construction of adaptive models, unsupervised strategies can dynamically adjust learning rates, apply adaptive regularization, and capture unknown threats in real time; nonetheless, the absence of explicit labels still poses challenges for model evaluation and debugging.

3.3. Deep learning

Deep learning is a machine learning method based on multi-layer neural networks that achieves complex pattern recognition and decision-making by automatically extracting deep features from data. For example, by constructing cross-category semantic relationships, zero-shot learning methods can effectively detect previously unseen vulnerabilities and exhibit strong generalization capabilities, but they also face high training complexity and heavy reliance on semantic descriptions [14]. Additionally, Redino et al. employed deep models built on graph and traffic data to effectively capture implicit structures in network communication, albeit with considerable preprocessing and graph construction overhead [15]. Using in-context learning (ICL) from Transformer models to introduce contextual information into the system, zero-day attack detection was achieved in digital substations, allowing rapid adaptation to environmental changes. In the domain of large language models, M et al. demonstrated the potential of LLMs for zero-day vulnerability detection—despite their rich pretraining knowledge and strong adaptability, high computational resource demands and explainability issues cannot be ignored [16]. Dahal et al. combined MLPs with explainable AI (XAI) to analyze zero-day attacks, a simple, efficient, and reasonably transparent approach, though it may underperform compared to deep architectures against complex attack patterns [17].

3.4. Reinforcement learning

Reinforcement learning is a machine learning method whereby an agent continuously explores its environment and optimizes its decision-making policy based on reward signals to achieve optimal behavior. In zero-day attack detection applications, reinforcement learning demonstrates strong adaptability and does not require full reliance on prior knowledge. For example, game theory–based reinforcement learning strategies can model the interaction between attacker and defender as a non-cooperative game, simulating various attack types through adversarial drills to optimize defense strategies and issue rewards according to the effectiveness of system defenses. Although this approach enhances detection flexibility, the complexity of attack modeling is high and may affect real-time deployment [18]. Moreover, Ngo & Nguyen applied reinforcement learning to detect zero-day malware in IoT environments by simulating IoT botnet attack patterns during training, using system call features for detection and adjusting the reward function based on false-positive and

DOI: 10.54254/2755-2721/2025.PO25664

detection rates to improve model stability and generalization [19]. However, the introduction of adversarial learning increases computational cost and may impact model convergence speed. Therefore, He et al. explored hardware-accelerated reinforcement learning detection methods by implementing an adaptive decision-making system on FPGA or GPU accelerators. This system generates adversarial samples through attack simulation and optimizes resource utilization via a reward function balancing detection accuracy and computational cost, enabling better adaptability across different hardware environments [20].

3.5. Mixed methods

Hybrid methods refer to improving detection accuracy and adaptability in zero-day attack detection by combining multiple techniques. A system that integrates CNN and LSTM can effectively capture the spatial and temporal features of network traffic, but its computational resource requirements are high when processing high-dimensional data [21]. The integration of signature-based detection and behavior analysis can improve detection performance by matching known attack patterns and monitoring anomalous behaviors, but the signature database must be continuously updated to address new threats [22]. Combining explainable AI (XAI) with the Synthetic Minority Over-sampling Technique (SMOTE) can enhance model transparency and balance data distributions, although SMOTE may introduce noise that affects generalization [23]. In the AI learning paradigm, Mearaj and Wani combined machine learning and deep learning by performing feature selection before classification to improve detection efficiency, but feature selection may omit critical information [24]. Additionally, Jena et al. combined static and dynamic analysis in web application security detection to perform code structure inspection and runtime behavior monitoring simultaneously, though dynamic analysis may incur additional system overhead [25].

3.6. Model optimization directions

Under all detection paradigms, zero-day attack detection faces similar and complex challenges and issues. In zero-day attack detection, the scarcity of labeled data has made few-shot learning one of the primary optimization focuses. By introducing methods such as transfer learning, meta-learning, and deep metric learning, models can capture attack features from limited samples and achieve generalized recognition of novel threats. For example, the Malware-SMELL strategy uses deep metric learning to map malicious samples into a similarity space, providing strong support for zero-shot detection [14]. Yu et al. proposed a few-shot intrusion detection method that, when trained on less than 1% of the NSL-KDD KDDTrain+ dataset, achieved high accuracies of 92.34% on KDD-Test+ and 85.75% on KDD-Test-21 [26]. Therefore, future optimization should further explore the integration of self-supervised and semi-supervised techniques to construct an adaptive detection framework based on few-shot learning, enabling rapid response and precise identification of unknown attacks.

Adversarial training plays an essential role in improving the robustness of zero-day attack detection models. It's also an important area to explore further for optimizing these systems.By incorporating adversarial sample generation and designing adversarial loss functions, the model can proactively simulate attacker perturbations during training, thereby capturing more subtle anomalous features. Various studies use methods such as GANs and variational autoencoders to generate adversarial samples. These approaches help strengthen models against deliberately crafted malicious inputs and enhance the ability of detectors to perform reliably in unfamiliar attack situations [10] Therefore, focusing on multi-scale adversarial sample fusion strategies and the joint optimization of

DOI: 10.54254/2755-2721/2025.PO25664

generative-discriminative networks has become one of the approaches to building more robust cybersecurity defense systems.

4. Evaluation metrics and experimental comparison

4.1. Accuracy, recall and ROC curve

Accuracy and recall are core metrics for evaluating system performance, where accuracy reflects the model's ability to correctly identify attack samples, and recall measures the model's comprehensiveness in capturing all attack samples. Nhlapo & Nkongolo evaluated the zero-day attack detection capabilities of four machine learning models using accuracy and recall, with the ensemble model achieved an accuracy of 100% [8]. The receiver operating characteristic (ROC) curve and area under the curve (AUC) further provide an intuitive representation of the trade-off between true positive rate and false positive rate at different decision thresholds. A higher AUC indicates better overall performance of the detection model. Sarhan et al. evaluated an MLP model using ROC and AUC on two datasets, and the results indicate that for the MLP model, the AUC values for the main attack types generally range between 0.94 and 0.95 [28].

4.2. Public datasets

In this study, researchers used a variety of public datasets, such as CIC-IDS 2017, UNSW-NB15, WSN-DS, Bot-IoT, and CICD-DoS2019, among others [1,10,20-21]. Using public datasets offers a consistent way to fairly compare different methods, which helps drive progress in improving the accuracy and robustness of zero-day attack detection, especially across diverse scenarios and multimodal environments.However, these datasets also have limitations: for example, CIC-IDS 2017 contains a large volume of simulated traffic during data collection, and its generation process may not fully reflect the complex background of real network environments, while CICDDoS2019 focuses primarily on DDoS attacks and lacks coverage of other attack types, which may not meet the needs of comprehensive security defense. Therefore, dataset selection will become an important factor to consider in future research.

5. Limitations and future directions

5.1. Limitations

Technically, AI-driven zero-day attack detection faces a series of bottlenecks, including the scarcity of zero-day attack samples, insufficient interpretability of models, inadequate generalization, and limited robustness in adversarial environments. The extremely low frequency of zero-day attacks, the difficulty of capturing and labelling them in advance, and the extremely high cost of acquiring and accurately labelling them render it difficult to construct high-quality, representative datasets, which directly undermines the reliability of model training and evaluation. Moreover, although deep learning models have achieved remarkable results in automatic feature extraction and detection accuracy, their "black-box" nature means that the decision process lacks sufficient interpretability. In scenarios where adversaries are actively changing tactics, many detection techniques struggle to keep up. This often results in either missing genuine threats or flagging harmless activity as dangerous, thus hampering the effectiveness of zero-day detection systems. Maintaining consistent performance in complex and rapidly changing network environments is difficult and requently comes with increased costs of deploying and maintaining the solution.

DOI: 10.54254/2755-2721/2025.PO25664

Furthermore, data privacy issues represent another urgent challenge in zero-day attack detection research. Detection systems often rely on large volumes of sensitive data, such as network traffic, user behavior logs, and medical images, which are potentially at risk of privacy leakage during collection, storage, and processing [31]. Although some public datasets have been anonymized, protecting user privacy while ensuring data quality and representativeness in real applications remains a complex task. Privacy-preserving techniques like federated learning offer new avenues for secure data sharing, but their robustness and effectiveness in complex adversarial scenarios still require thorough validation [32]. Privacy concerns not only impact the security and credibility of detection systems but may also introduce legal and ethical risks, imposing additional constraints on the deployment and adoption of zero-day attack detection technologies.

5.2. Future directions

Because most researchers conduct their work in specific and diverse application scenarios, the future evolution of zero-day attack detection technologies will increasingly rely on deep integration across multiple domains. Future research can further incorporate multidisciplinary approaches such as game theory, economic-incentive mechanisms, and socio-behavioral analysis. In the vulnerability-crowdsourcing domain, formal governance and relational governance mechanisms can motivate white-hat hackers to disclose and remediate zero-day flaws more proactively, thereby accelerating the identification and response to zero-day attacks [33]. Cross-modal data fusion offers a compelling approach, such as integrating static code analysis, energetic behavior monitoring, and natural-language processing. This combination allows for a more thorough extraction of hidden attack features, eventually improving both detection accuracy and the clarity of results [16].

As adversarial attack techniques continue to evolve, existing AI-based detectors face mounting challenges, making the development of novel defense paradigms a critical research priority.Zero-day detection benefits from existing patch management systems by optimizing remediation processes, which helps boost system responsiveness and strengthen overall security [34]. High-complexity vulnerabilities with widespread impact are typically addressed more quickly, whereas those involving higher privileges or sensitive data are more challenging to fix. Consequently, future defense frameworks can adopt data-driven methods such as survival analysis to predict and optimize patch-deployment timelines for different vulnerability classes, enabling more proactive security management.

6. Conclusion

This paper reviews the research advancements of AI in zero-day attack detection from 2019 to 2025, analyzes the advantages and disadvantages of different AI-driven detection methods, and explores corresponding optimization strategies. Although deep learning and reinforcement learning have exhibited strong potential in zero-day attack detection, critical challenges persist, including high data dependency, excessive computational cost, and lack of explainability. Moreover, the evolution of adversarial attacks rendered existing detection models vulnerable to perturbations, resulting in insufficient generalization. To enhance the practical effectiveness of AI-based zero-day attack detection, future research may focus on four directions: integrating multimodal data and cross-domain methods to improve model adaptability and generalization, exploring efficient few-shot learning and adaptive optimization strategies to reduce the reliance on large-scale labeled data, refining the adversarial training mechanisms to strengthen robustness in complex adversarial environments, and developing privacy-preserving approaches to ensure the security of data sharing.

DOI: 10.54254/2755-2721/2025.PO25664

As AI technology continues to advance, zero-day attack detection systems will move towards greater intelligence, efficiency, and security.

References

[1] Holm, H. (2014). Signature Based Intrusion Detection for Zero-Day Attacks: (Not) A Closed Chapter?. 47th Hawaii International Conference on System Sciences, Waikoloa, HI, USA, pp. 4895-4904, doi: 10.1109/HICSS.2014.600.

[2] AlEroud A. & Karabatis, G. (2012).A Contextual Anomaly Detection Approach to Discover Zero-Day Attacks, 2012 International Conference on Cyber Security, Alexandria, VA, USA, 2012, pp. 40-45, doi: 10.1109/CyberSecurity.2012.12.

[3] Croce F & Hein M (2020). Reliable evaluation of adversarial robustness with an ensemble of diverse parameter-free attacks. International conference on machine learning. PMLR, 2020: 2206-2216.

[4] Du X.H., et al. (2021). Text Adversarial Example Attack and Defense Techniques: A Survey. Journal of Chinese Information Processing .35.8: 1-15.

[5] Adhithya R. & Revathi M. (2024). Exploring the Efficacy of Federated-Continual Learning Nodes with Attention-Based Classifier for Robust Web Phishing Detection: An Empirical Investigation. 2024 International Conference on Advancements in Power, Communication and Intelligent Systems (APCI). IEEE, 2024: 1-7.

[6] Mbona, I. & Eloff, J.H.P. (2022). Detecting Zero-Day Intrusion Attacks Using Semi-Supervised Machine Learning Approaches. IEEE Access, vol. 10, pp. 69822-69838, doi: 10.1109/ACCESS.2022.3187116.

[7] Reardon, S., Hssayeni M. D. & Mahgoub, I. (2024). Detection of Zero-Day Attacks on IoT. 2024 International Conference on Smart Applications, Communications and Networking (SmartNets), Harrisonburg, VA, USA, pp. 1-5, doi: 10.1109/SmartNets61466.2024.10577735.

[8] Nhlapo, S.J., & Nkongolo, MNW. (2024). Zero-day attack and ransomware detection. arXiv: 2408.05244.

[9] Hindy H, Atkinson R, Tachtatzis C, et al. Towards an effective zero-day attack detection using outlier-based deep learning techniques [J]. ArXiv, vol. abs/2006.15344, 2020.

[10] P.F. de Araujo-Filho, M. Naili, G. Kaddoum, E. T. Fapi and Z. Zhu, "Unsupervised GAN-Based Intrusion Detection System Using Temporal Convolutional Networks and Self-Attention, " in IEEE Transactions on Network and Service Management, vol. 20, no. 4, pp. 4951-4963, Dec. 2023, doi: 10.1109/TNSM.2023.3260039.

[11] A.Arun, A. S. Nair and A. G. Sreedevi, "Zero Day Attack Detection and Simulation through Deep Learning Techniques, " 2024 14th International Conference on Cloud Computing, Data Science & Engineering(Confluence), Noida, India, 2024, pp.852-857, doi: 10.1109/Confluence60223.2024.10463429.

[12] Barros, P. H., Chagas, E. T., Oliveira, L. B., Queiroz, F., & Ramos, H. S. (2022). Malware-SMELL: A zero-shot learning strategy for detecting zero-day vulnerabilities. Computers & Security, 120, 102785.

[13] C.Redino et al., "Zero Day Threat Detection Using Graph and Flow Based Security Telemetry, " 2022 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS), Greater Noida, India, 2022, pp. 655-662, doi: 10.1109/ICCCIS56430.2022.10037596.

[14] L.M, V. Agarwal, S. Kamthania, P. Vutkur and M. Chari S, "Benchmarking LLM for Zero-day Vulnerabilities, " 2024 IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT), Bangalore, India, 2024, pp. 1-6, doi: 10.1109/CONECCT62155.2024.10677338.

[15] Dahal, Ashim, Prabin Bajgai, and Nick Rahimi. "Analysis of Zero Day Attack Detection Using MLP and XAI." arXiv preprint arXiv: 2501.16638 (2025).

[16] 18Hu, Z., Chen, P., Zhu, M., Liu, P. (2019). Reinforcement Learning for Adaptive Cyber Defense Against Zero-Day Attacks. In: Jajodia, S., Cybenko, G., Liu, P., Wang, C., Wellman, M. (eds) Adversarial and Uncertain Reasoning for Adaptive Cyber Defense. Lecture Notes in Computer Science(), vol 11830. Springer, Cham. https: //doi.org/10.1007/978-3-030-30719-6_4

[17] Ngo, QD., Nguyen, QH. (2022). A Reinforcement Learning-Based Approach for Detection Zero-Day Malware Attacks on IoT System. In: Silhavy, R. (eds) Artificial Intelligence Trends in Systems. CSOC 2022. Lecture Notes in Networks and Systems, vol 502. Springer, Cham. https: //doi.org/10.1007/978-3-031-09076-9_34

[18] Z. He, H. M. Makrani, S. Rafatirad, H. Homayoun and H. Sayadi, "Breakthrough to Adaptive and Cost-Aware Hardware-Assisted Zero-Day Malware Detection: A Reinforcement Learning-Based Approach, " 2022 IEEE 40th International Conference on Computer Design (ICCD), Olympic Valley, CA, USA, 2022, pp. 231-238, doi: 10.1109/ICCD56317.2022.00042.

[19] Mahdi Soltani, Behzad Ousat, Mahdi Jafari Siavoshani, Amir Hossein Jahangir, An adaptable deep learning-based intrusion detection system to zero-day attacks, Journal of Information Security and Applications, Volume 76, 2023, 103516, ISSN 2214-2126, https: //doi.org/10.1016/j.jisa.2023.103516.

DOI: 10.54254/2755-2721/2025.PO25664

[20] Zero-day Attack Detection and Prevention S. S. Satam, A. A. Patil, D. B. Narkhede, S. Singh and N. Pulgam, "Zero-Day Attack Detection and Prevention, " 2023 7th International Conference On Computing, Communication, Control And Automation (ICCUBEA), Pune, India, 2023, pp. 1-6, doi: 10.1109/ICCUBEA58933.2023.10392272.
[21] C.K. Sruthi, A. Ravikumar and H. Sriraman, "Enhancing Zero-Day Attack Detection with XAI-Driven ML Models and SMOTE Analysis, " 2024 3rd International Conference on Artificial Intelligence For Internet of Things (AIIoT), Vellore, India, 2024, pp. 1-5, doi: 10.1109/AIIoT58432.2024.10574566.
[22] Mearaj N. & Wani, M.A. (2023). Zero-day Attack Detection with Machine Learning and Deep Learning. 2023 10th International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, pp. 719-725.
[23] S. Jena, A. Soni, J. Rout and S. K. Nanda, "Zero-Day Exploits in Web Applications: Detection, Response, and Prevention, " 2024 3rd International Conference for Advancement in Technology (ICONAT), GOA, India, 2024, pp. 1-6, doi: 10.1109/ICONAT61936.2024.10774961.
[24] Y. Yu and N. Bian, "An Intrusion Detection Method Using Few-Shot Learning, " in IEEE Access, vol. 8, pp. 49730-49740, 2020, doi: 10.1109/ACCESS.2020.2980136.
[25] Mohanad Sarhan, Siamak Layeghy, Marcus Gallagher, and Marius Portmann. 2023. From zero-shot machine learning to zero-day attack detection. Int. J. Inf. Secur. 22, 4 (Aug 2023), 947–959. https: //doi.org/10.1007/s10207-023-00676-0
[26] Tan Q, Li Q, Zhao Y, et al. Defending against data reconstruction attacks in federated learning: An information theory approach [C]//33rd USENIX Security Symposium (USENIX Security 24). 2024: 325-342.
[27] Lu S, Li R, Liu W. FedDAA: a robust federated learning framework to protect privacy and defend against adversarial attack [J]. Frontiers of Computer Science, 2024, 18(2): 182307.
[28] Li Y, Zhao L. Collaborating with bounty hunters: how to encourage white hat hackers' participation in vulnerability crowdsourcing programs through formal and relational governance [J]. Information & Management, 2022, 59(4): 103648.
[29] Roumani Y. (2021). Patching zero-day vulnerabilities: an empirical analysis. Journal of Cybersecurity, 7(1): tyab023.