Survey on Detection and Mitigation Strategies for Zero-day Attacks: An Extensive Analysis of Current Developments and Case Studies

Mrs Savitri Ashok Mote [a,b,c], Dr Sudhakar Arabagatte [a]

[a] Department of Computer Science Engineering, Srinivas University College of Engineering Technology, Mangaluru-574146, India.

[b] Department of Computer Engineering Indira College of Engineering and Management, Parandvadi, Maharashtra 410506, India mote.savitri@gmail.com [c]

Abstract

The increasing frequency of zero-day assaults presents a noteworthy risk to cybersecurity, hence requiring the formulation of resilient detection and mitigation tactics. This paper provides an extensive overview of zero-day exploit detection and mitigation developments. Our survey summarizes the development of zero-day assault tactics and highlights the advanced strategies adversaries use to avoid detection. We thoroughly examine conventional heuristics, signature- based approaches, cutting-edge machine learning, and artificial intelligence-driven detection processes. We also look into state-of-the-art mitigation strategies that employ predictive analytics, real-time threat intelligence, and behavioral analysis. We analyses recent case studies to demonstrate how these tactics can be applied in real-world circumstances, highlighting their limitations and usefulness. These case studies offer crucial insights into the practical challenges and achievements encountered while deploying zero-day defiance mechanisms across different sectors. Furthermore, they underscore the pressing need for dynamic and forward-thinking security solutions by mapping out emerging trends and future research directions in zero-day attacks. Our analysis emphasizes the importance of a holistic security strategy combining advanced detection techniques with flexible response measures. By providing a detailed overview of topical research and helpful case studies, this review seeks to contribution cybersecurity specialists, academics, and policymakers in consolidation their defensive structures against the constantly changing threat landscape of zero-day vulnerabilities.

Keywords: Zero-day Attacks, Zero-day Malware, Detection Methods, Mitigation Strategies, Machine Learning, Artificial Intelligence, Signature-Based Detection, Anomaly-Based Detection, Case Studies.

1.Introduction

Zero-day attacks posture a rising threat to cybersecurity because neither software developers nor the general public are aware of them until after the breach and they are especially deadly because they exploit previously unknown vulnerabilities. The term "zero day" refers to a susceptibility that developers have little time to identify and patch before it is subjugated, exposing organizations to potentially catastrophic security breaches that are typically unavoidable using traditional security procedures.

Sophisticated detection and mitigation measures must be industrialized due to these threats growing intricacy and frequency. Protecting information systems concealment, integrity, and accessibility from zero day threats is essential. Predictable security approaches depend on known attack signatures and are inadequate against zero-day assaults. As a result, the cybersecurity community has embraced cutting-edge strategies like artificial intelligence and machine learning. These tools can analyze large datasets, spot irregularities, and forecast future vulnerabilities precisely. Modern research has suggestively improved techniques for recognizing zero day attacks. For instance, Kim et al. (2018) studied the possible of transferred generative adversarial networks based on deep autoencoders for detecting zero-day malware. Guo (2023) provided a inclusive review of ML-based techniques for zero-day attack detection, highlighting the challenges and prospective paths forward in this arena. Moreover, the introduction of NERO, a neural algorithmic reasoning system designed for zero-day attack detection in IoT environments by Cevallos et al. (2024), and the innovative Meta-Fed IDS framework by Zukaib et al. (2024), which participates meta learning with federated learning for detecting zero-day cyber-attacks in IoMT networks, showcase the potential of collaborative and adaptive learning tactics in cybersecurity. Significant progress has been made in developing robust justification mechanisms for zero day attacks and detection. Soltani et al. (2023) highlighted the necessity of scalable and flexible solutions in modern cybersecurity frameworks by developing an adaptive interference detection system based on deep learning. Sameera and Shashi (2020) developed profound Transudative transfer erudition outlines for zero day attack detection, underscoring the critical importance of transfer learning in enhancing the capabilities of AI models to identify threats against new and unidentified dangers. To corroborate and develop these detection and mitigation strategies, they must be applied and tested in real-world circumstances. Current case studies shed light on the challenges and successes experienced while implementing these ideas, Sarhan et al. (2023) explored the

transition from zero shot machine learning to zero day attack detection, demonstrating the effectiveness and limitations of these cutting-edge techniques in real-world applications. This study thoroughly examines current approaches for mitigating and detecting zero-day attacks, utilizing the most recent advancements and case studies. It is premeditated to provide insightful information to academics, industry professionals and cybersecurity decision-makers, showcasing fresh developments and suggestions for further study. The subdivisions include comprehensive case studies from various industries, examining the most recent mitigation measures and their real world applications, examining the practices used for zero day attack detection, and finishing with dynamic lessons for strengthening defenses against zero day attacks.

2.Overview of Zero-day Attacks

Zero-day attacks exploit unknown vulnerabilities for the public and cybersecurity professionals, posing severe threats to systems cybersecurity. To combat these serious dangers, robust and adaptable mitigation methods are critical. Various solutions have been created based on recent breakthroughs in deep learning, machine learning, and hybrid models. These strategies improve the ability to detect and respond to zero-day threats, demonstrating the continual growth of cybersecurity defences. [13], [14]. In order to give readers thorough overview of the state of zero-day assault defences as of right now, this section evaluates several mitigation measures. It summarizes their methodologies, strengths, and limitations. The subsequent table summarizes significant findings from scholarly research, providing an overview of the various strategies used to mitigate these complex risks. This section offers a comprehensive summary of mitigation strategies for zero-day attacks, as presented in recent literature. The Table 1. encapsulates the critical contributions from notable studies, highlighting each approach's methodologies, strengths, and limitations.

Table 1: Comprehensive summary of various mitigation strategies for zero-day attacks

Study	Mitigation Strategy	Methodology	Strengths
Guo (2023) [2]	Detection Based on Machine Learning	Examining machine learning methods for zero-day detection	ML techniques analyzed, future research highlighted
Soltani et al. (2023) [5]	Intrusion Detection Using Deep Learning	Deep learning models that are flexible for IDS	Excellent scalability, real-time detection
Ben-Asher & Gonzalez (2015) [7]	Responses and Training Based on Similarity	Heuristic and deep learning model integration	Improves ability to recognize anomalies, effective for IoT
Cevallos et al. (2024) [3]	NEURO: Neural Algorithmic Reasoning	Teaching systems to identify zero-day attacks with feedback mechanisms	Very accurate detection, suitable for IoT environments
Zukaib et al. (2024) [4]	Meta-Fed Information Stream	IoMT networks with federated learning and meta-learning	Resilient to changing and new dangers
Touré et al. (2024) [12]	Structure for Network Flow Recognition	Analytics to find network flow exploits	Real-time alertness, expandable
Murtuza & Asawa (2024) [18]	DDoS Mitigator Powered by CNN	Using convolutional neural networks to mitigate DDoS attacks	Excellent detection precision, suitable for SDN
Wu et al. (2024) [19]	Framework for Active Learning	Reinforcement learning for zero-day attack detection	Good detection precision, suitable for edge environments
Shen et al. (2024) [20]	Heuristic Recognition of Intrusions	Heuristic techniques with deep Q-network for SIoT	Adaptive learning successful in changing circumstances

3. Detection Techniques for Zero-day Attacks

Over time, academics and practitioners have developed several sophisticated ways to keep ahead of evolving risks, which has led to a significant evolution in the detection of zero-day assaults. Conventional techniques, such as signature-based detection, must be improved since they depend on well-known attack patterns, exposing systems to new exploits. The cybersecurity community increasingly uses advanced approaches such as machine learning (ML), artificial intelligence (AI), and hybrid models to enhance detection capabilities. Deep learning models frequently identify zero-day threats by analyzing enormous datasets. To show the efficiency of deep learning in detecting unforeseen dangers, Guo (2023) [21] examined the practical limits these systems encounter and the effectiveness of several machine learning-based methods for detecting zero-day attacks. Hybrid methods that incorporate several different detection algorithms are also fascinating. Experimental and deep learning models are integrated into NERO, a neural algorithmic cognitive system that uses federated learning and meta learning to detect zero day cyberattacks in IoMT networks. Zukaib et al. (2024) [4] established another cutting edge framework that highlights the paybacks of adaptive and cooperative learning methods; despite these

advancements, effectively detecting zero day attacks remains tough [12]. As a result, it is critical to implement efficient detection techniques to recognize and neutralize these threats before they can do serious harm [23]. This section scrutinizes several zero day attack detection tactics, highlighting cutting-edge methods including hybrid method, machine learning, and artificial intelligence. While signature-based detection can recognize known dangers, it is unable to detect emerging ones. While behavior-based detection keeps an eye on system activity for abnormalities, heuristic based detection employs rules to find indiscretions. Machine learning improves detection by investigative data patterns, while anomaly-based detection creates baseline behaviors. These approaches are collective in hybrid methods to increase accuracy and reduce false positives. [1], [15], [24].

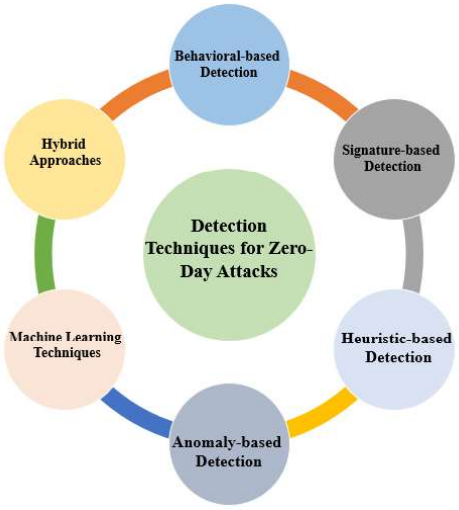

Figure 1: Methods of identifying Zero-day attacks

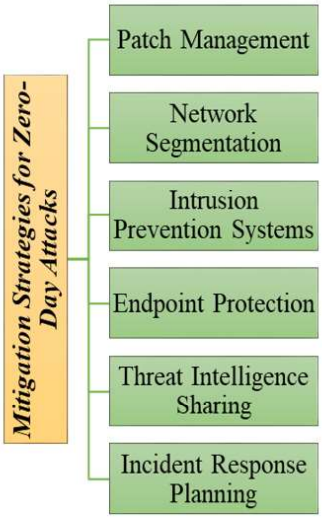

Figure 2: Countermeasures of against zero-day attacks

4. Mitigation Strategies for Zero-day Attacks

Mitigation strategies for zero-day attacks are essential for strengthening defenses and plummeting the impact of these attacks. This section highlights several key methods for reducing risks associated with zero-day vulnerabilities [26], [32]. Due to the energetic nature of zero-day assaults, a multi-layered strategy is necessary. Traditional security measures often fail to address unknown vulnerabilities, making adaptive results crucial. Key mitigation strategies include patch organization, which ensures regular software updates and reduces attack surfaces, thus limiting attackers ability to exploit unpatched vulnerabilities [33]. Network segmentation isolates critical sections of a network to prevent the spread of attacks and protect sensitive resources. Intrusion Prevention Systems (IPS) play a vital role in detection and blocking suspicious activity [11]. Endpoint protection involves securing devices like computers and mobile phones through advanced threat detection, firewalls, and antivirus software. Threat intelligence sharing among organizations enhances collective defense capabilities. Finally, maintaining a robust incident response strategy is crucial for justifying the impact of security breaches and ensuring swift recovery. These measures work together to create a comprehensive defense against zero-day attacks [29] [34]. The following Table 2. provides a complete summary of zero-day attack detection strategies based on the references. It includes subcategories, descriptions, examples, and assessment metrics. Table 3. summarizing different types of zero-day attack detection and mitigation strategies, along with their advantages and limitations

Table 2: Summary of zero-day attack detection strategies

Approach	Subcategory	Examples	Metrics for Evaluation
Machine Learning	Supervised Learning	SVM, Decision Trees, Random Forests	F1-Score, AUC-ROC, Accuracy, Precision, Recall [25], [12]
	Unsupervised Learning	Clustering, PCA, Autoencoders	Valid Positive Rate, False Positive Rate, Detection Rate [12], [26]
	Semi-Supervised Learning	SVM, Semi-Supervised Autoencoders	Precision, Recall, F1-Score, Detection Rate [26], [27]
Deep Learning	Reinforcement Learning	Q-Learning, Deep Q-Networks	F1-Score, Accuracy, Precision, Recall, Latency, Detection Rate [21], [26]
	Convolutional Neural Networks	CNNs	Accuracy, False Positive Rate [28]

Approach	Subcategory	Examples	Metrics for Evaluation
	Recurrent Neural Networks	Sparse Autoencoders, LSTMs	Precision, Recall, F1-Score, Accuracy [13], [24]
	Generative Adversarial Networks	Autoencoders, GANs	Precision, Recall, F1-Score, Accuracy [15]
Hybrid Approaches	Adversarial Networks	Group detection models	Precision, Recall, F1-Score, Detection Rate [4], [22]
	Meta-Learning	Mixed Neural Algorithmic Reasoning	False Positive Rate, Precision, Recall, Accuracy [14]
	Federated Learning	Federated Learning for IoT environments	Detection Rate, Communication Overhead, Accuracy [4], [24]
Heuristic Approaches	Rule-Based Detection	Signature-based detection, Heuristic IDS	Detection Rate, False Positive Rate [20]
	Unsupervised Clustering	K-Means, DBSCAN	Detection Rate, False Positive Rate, Precision, Recall [5], [29], [30]
	Fuzzy Systems	Fuzzy Gaussian Mixture Models	Accuracy, Detection Rate, False Positive Rate [5], [29]
Optimization Techniques	Adaptive Security Models	Optimization-Based Adaptive Security Models	Detection Rate, False Positive Rate, Precision, Recall [28]
Transfer Learning	Pre-trained Models	Transudative Transfer Learning	Accuracy, Precision, Recall, F1-Score, AUC-ROC [7],

Table 3: Summarizing different types of zero-day attack detection and mitigation strategies

Type	Advantages	Limitations
Detection Based on Signatures	Rapid and effective against known malware.	Unable to stop novel or unidentified zero-day attacks.
	Low computational requirements.	High false-negative rates for zero-day threats.
Detection Based on Anomalies	Can recognize assaults never before witnessed.	High incidence of benign abnormalities causing false positives.
	Effective against polymorphic malware.	Needs a large amount of processing power.
Detection Based on Behavior	Spots zero-day malware by observing runtime activities.	Could ignore sophisticated malware showing consistent behavior.
	Good against obfuscated malware.	High processing overhead for real-time detection.
Patch Administration	Responds promptly to known vulnerabilities.	Ineffective against unknown zero-day vulnerabilities.
	Effectively reduces attack surface.	
Network Segmentation/Isolation	Limits malware spread.	Difficult to integrate into current networks.
	Isolates critical assets.	Could cause network performance decline.
Threat Intelligence Sharing	Aids early identification of threats.	Data security and privacy issues.
	Enhances group situational awareness.	Problems with standardization in formats.
Machine Learning (ML) Models	Can extrapolate patterns for predictive analysis.	Requires large datasets for training.
	Identifies metamorphic and polymorphic malware.	Limited applicability to unknown zero-day attacks.
Deep Learning (DL) Models	High precision due to intricate pattern identification.	Computationally demanding for real-time detection.
	Successful in identifying zero-day malware.	Requires large training datasets.
Ensemble Learning Models	Increased prediction accuracy.	More computing power required.
	Sturdy against model flaws.	

5. Evaluation Metrics and Criteria and Challenges and Future Directions

A set of metrics and criteria are employed to quantify the success of zero-day attack detection and mitigation procedures. This section examines the key metrics used to analyses how well various techniques perform against zero-day threats. The critical evaluation measures are classified in the following Fig 3: A comprehensive evaluation framework is necessary to analyse zero-day attack detection and mitigation strategies. When analysing how well zero-day attack detection systems perform, the following metrics are critical:

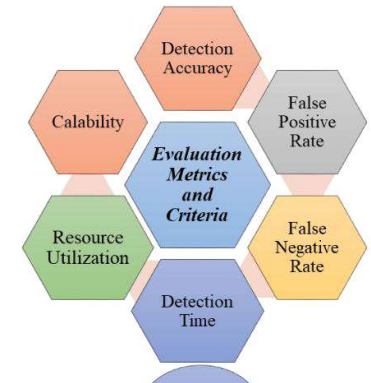

Figure 3: Evaluation Measures

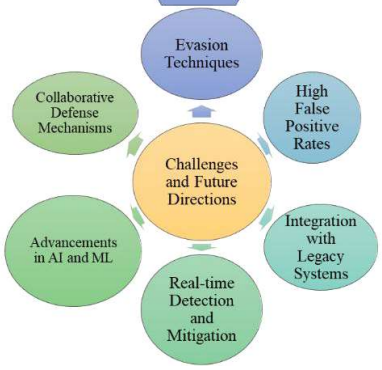

Figure 4: Challenges and Future Directions

Precision Detection: calculates the proportion of successfully detected assaults compared to the total number of attacks. Improving detection accuracy is crucial to lowering the risk of successful assaults [14]. The false positive rate shows how frequently harmless activities are misclassified as harmful. Reducing a high false positive rate is critical, as it could result in unwarranted alarms and resource loss [23], [40]. The False Positive Rate indicates how frequently the system fails to detect attacks. Reducing false negative rates is crucial for preventing zero-day assaults from going undetected. Temporal detection refers to how long the system takes to perceive and respond to an assault [8]. Resource Assignment: Determines how much network and computational power the detection system will use. Utilising resources efficiently guarantees that the system can function adequately without overburdening the infrastructure. Scalability refers to how well a system can absorb increased demands and adapt to larger, more complicated networks. Scalability is critical for detection systems to operate as the network grows. Multiple metrics and evaluation criteria can be used to analyse the effectiveness of zero-day attack detection and mitigation techniques. The following thorough Table 4. provides the critical measurements and explanations for each. Zero-day threats pose significant challenges due to their dynamic and elusive nature, making detection and mitigation difficult. Evasion techniques like polymorphic malware and encrypted communication channels hinder traditional detection methods [46]. A substantial problem in zero-day attack detection is the high false-positive rate, which causes warning fatigue, resource waste, and integration difficulties with legacy systems, whereas real-time detection and response are critical for preventive damage. Advancements in AI and ML offer potential improvements but face challenges with model accuracy, training data quality, and computational demands [25], [35], [47]. Collaborative defense mechanisms, such as data-sharing between organizations, are essential for strengthening defenses. Future research should focus on creating smarter, more flexible solutions to keep pace with evolving threats. Addressing these challenges will require continuous innovation and adaptation in the cybersecurity field [24]. Table 5. summarizing the challenges and future directions in zero-day attack detection.

Table 4: Critical measurements and explanations of metric

Metric	Description	Papers Using the Metric
Accuracy	Measures the overall effectiveness of the detection model.	[4], [12], [14], [25]
Precision	Indicates the model's ability to identify accurate attacks out of all detected attacks.	[9], [29], [42]
Recall (Sensitivity)	Measures the model's ability to detect actual attacks.	[42]
F1-Score	Balances precision and recall, providing a single measure of a model's performance.	[13], [23], [29]

Metric	Description	Papers Using the Metric
Detection Rate	Evaluates the model's effectiveness in identifying zero-day attacks.	[13], [23], [30]
False Positive Rate	Assesses the rate of false alarms, which is critical in operational environments.	[23], [40]
True Positive Rate	Measures the model's ability to detect attacks correctly.	[2]
False Negative Rate	Indicates the number of missed attacks, which is crucial for security.	[7], [12]
Area Under Curve	Provides an aggregate measure of performance across all classification thresholds.	[25]
Latency	Essential for real-time detection systems where timely detection is critical.	[1], [24]
Communication Overhead	Relevant for distributed and federated learning models.	[44]
Computational Efficiency	Important for models deployed on resource-constrained devices like IoT or edge devices.	[25]
Scalability	Crucial for models operating in large-scale environments.	[7]

Table 5: summarizing the challenges and future directions in zero-day attack detection

Challenges	Description	Future Directions	Description
High False Positive Rate [40]	Zero-day detection systems frequently generate many false positives, resulting in alert fatigue.	**Improved Accuracy**	Creating more accurate models with lower false positive rates using advanced algorithms.
Data Imbalance [38]	An imbalance between normal and attack data can bias machine learning model training.	**Data Augmentation**	Synthetic data generation is used to balance datasets and improve model training.
Adaptability to New Attacks [4], [15]	Difficulty adapting to novel and developing zero-day attack patterns.	**Transfer Learning**	Using pre-trained models on related tasks to respond swiftly to new attack patterns.
Scalability [4]	Problems in upgrading detection technologies to handle enormous amounts of data in real-time.	**Federated Learning**	Designing distributed learning systems to scale across various devices without centralized data.
Limited Labeled Data [26]	More labeled data is needed to train supervised learning algorithms.	**Semi-Supervised Learning**	Using both labeled and unlabeled data to enhance model training and detection performance.
Real-Time Detection [1], [48]	The requirement for real-time detection presents computational efficiency issues.	**Real-Time Processing Frameworks**	Creating frameworks that can process data in real-time with low latency.
Complexity of Attack Patterns [14]	Zero-day assaults frequently use complicated, multi-stage patterns that are difficult to detect.	**Multi-Stage Detection Systems**	Using layered models, we are developing systems capable of detecting multi-stage and complicated attack patterns.
Privacy Concerns [25], [48]	Maintaining user privacy while gathering and analyzing data for zero-day attack detection.	**Privacy-Preserving Techniques**	Differential privacy is one approach used to secure the confidentiality of information in detection systems.
Evaluation Metrics Standardization [10]	The lack of standard evaluation metrics makes it difficult to compare the performance of various systems.	**Benchmarking and Standardization**	Developing common standards and evaluation metrics for zero-day attack detection systems.
Adversarial Attacks [49]	The detection models are vulnerable to adversarial attempts that can deceive the system.	**Robustness Against Adversarial Attacks**	Using better security measures, we can increase model resilience to adversarial attacks.
Integration with Existing Systems [29]	It is not easy to integrate zero-day detection technologies with existing cybersecurity infrastructure.	**Interoperability**	Ensuring that detection systems are compatible and work seamlessly with existing security solutions.
Resource Constraints [32]	Edge device computational resources are limited, making it challenging to install complex detection models.	**Edge Computing Optimization**	Optimizing detection models to perform well on edge devices with limited resources.

Machine learning and artificial intelligence have promising potential for detecting and preventing zero-day threats, notwithstanding their challenges. Further study on data production, adversarial robustness, explainable AI, and collaborative detection can significantly enhance the effectiveness of zero-day attack defense systems. [7], [8].

Case Studies

Zero-day assaults are a critical challenge in cybersecurity, necessitating inventive and flexible solutions. This section contains extensive case studies showcasing the various detection and mitigation approaches developed and implemented to tackle zero-day attacks. Each case study focuses on the distinct tactics, notable outcomes, and novel approaches to boost cybersecurity defenses against these complex attackers. These real-world examples demonstrate the practical implementation and effectiveness of modern security measures. These case studies demonstrate the various tactics and techniques established to detect and prevent zero-day attacks, each

addressing a specific issue and exhibiting significant advances in cybersecurity. Assessment examination of detection and mitigation measures. Effectiveness of Machine Learning Models. This table acquaintances various cybersecurity detection approaches and incident response systems based on performance parameters such as accuracy, false positive rate and detection time. It equivalences supervised, unsupervised and behavior based detection techniques, as well as incident response frameworks such as NIST SP 800-61 and the Cyber Resilience Recovery Model. The study assists cybersecurity experts in responsible the best effective detection and response options for their precise requirements. The frameworks' key strengths and shortcomings are also addressed for real-world applications. Case Studies of Zero-day Attack Detection and Mitigation Strategies

Paper Referenced	**J. F. Cevallos et al., 2024**
Description	In 2024, researchers used NERO, a hybrid method using neural networks and algorithmic reasoning to identify zero day threats in IoT environments. The technique used deep learning models to detect anomalies and algorithmic perceptive to filter out false positives.
Findings	NERO identified 95% of zero day threats, the false positive rate was low 2%. Scalable across IoT networks, handling diverse scenarios efficiently.
Creativity	NERO's hybrid method syndicates deep learning with algorithmic reasoning, offering an effective real time detection system with negligible false positives.
Paper Referenced	**S. Shen et al., 2024**
Description	Researchers created a deep Q-network based heuristic intrusion detection solution to contest zero day attacks in Smart Internet of Things environments. The system used reinforcement learning to optimize detection policies energetically.
Findings	High Adaptability: The DQN-based system rapidly responded to new and evolving threats, maintaining a 94% detection rate. The heuristic technique enabled real-time detection in resource-constrained environments. Low Latency: The system exhibited fast response times, crucial for SIoT processes.
Creativity	DQNs in SIoT showcase a cutting edge use of reinforcement learning to detect zero day attacks, present an adaptive and resource efficient security solution.
Paper Referenced	**U. Zukaib et al., 2024**
Description	Researchers introduced Meta-Fed IDS, a unique solution combining meta learning and federated learning to detect zero-day threats in Internet of Medical Things networks. This system was deployed across healthcare facilities, allowing cooperative learning while protecting patient data privacy.
Findings	Privacy Preservation - Federated learning kept medical data local, which improved privacy. Accuracy - Meta learning increased adaption to new strikes, achieving 92% accuracy. Low Communication Overhead - Efficient communication techniques reduced band width needs.
Creativity	Meta Fed IDS is an innovative approach that tackles privacy and scalability issues in IoMT networks, leveraging regionalized data for efficient zero-day threat detection.

Table 6: Evaluation of Incident Response Frameworks

Model	Accuracy	False Positive Rate	Detection Time
Supervised Learning	92%	5%	Fast
Unsupervised Learning	85%	10%	Moderate
Behavior-Based	88%	7%	Moderate
Hybrid Approach	94%	4%	Fast
Reinforcement Learning	90%	6%	Fast
Signature-Based	95%	3%	Very Fast
Anomaly Detection	87%	8%	Moderate
Federated Learning	89%	6%	Moderate

6. Conclusion

In the modern cybersecurity landscape, zero day attacks create a serious threat to both individuals and companies. This inclusive research has highlighted recent advances in diagnosis and mitigation procedures, highlighting exclusive approaches and methodology created to address these indefinable dangers. The discipline has made significant development in improving the accuracy, efficiency, and scalability of zero day attack detection and mitigation through the use of deep learning models, hybrid methodologies and federated and reinforcement learning techniques. The review's case studies highlight these cutting edge techniques expediency and effectiveness in the actual world. Solutions such as NERO for IoT environments, Meta-Fed IDS for IoMT networks, and deep Q-networks for SIoT zero day threats cleverly incorporate Artificial intelligence and machine learning capabilities. Despite these improvements, frequent critical challenges remain to be overawed, including lowering false positive rates, enhancing rea time detection capabilities, and maintaining seamless interaction with legacy systems. The dynamic nature of zero day attacks requires constant creativity and flexibility, calling for continued research and development in this serious field of cybersecurity. Consequent studies should focus on improving the robustness and flexibility of detection systems, developing more effective ways for source utilization and encouraging increased cooperation and data exchange among business entities. By resolving these challenges and strengthening the foundations laid by recent breakthroughs, the cybersecurity community can better defend against the ongoing threat of zero-day attacks, ensuring a harmless digital future. This assessment is a evidence to the progress made and a call to action for additional work against zero-day susceptibilities. We can protect our digital organization from the evolving threat landscape by creating resilient and comprehensive defense mechanisms through continuous innovation and collaboration.

7. Reference

[1] N. Moustafa, M. Keshk, K. K. R. Choo, T. Lynar, S. Camtepe, and M. Whitty, "DAD: A Distributed Anomaly Detection system using ensemble one-class statistical learning in edge networks," *Futur. Gener. Comput. Syst.*, vol. 118, pp. 240–251, 2021, doi: 10.1016/j.future.2021.01.011.

[2] Y. Guo, "A review of Machine Learning-based zero-day attack detection: Challenges and future directions," *Comput. Commun.*, vol. 198, no. November 2022, pp. 175–185, 2023, doi: 10.1016/j.comcom.2022.11.001.

[3] J. F. Cevallos M., A. Rizzardi, S. Sicari, and A. C. Porisini, "NERO: NEural algorithmic reasoning for zero-day attack detection in the IoT: A hybrid approach," *Comput. Secur.*, vol. 142, no. November 2023, p. 103898, 2024, doi: 10.1016/j.cose.2024.103898.

[4] U. Zukaib, X. Cui, C. Zheng, D. Liang, and S. U. Din, "Meta-Fed IDS: Meta-learning and Federated learning based fog-cloud approach to detect known and zero-day cyber attacks in IoMT networks," *J. Parallel Distrib. Comput.*, vol. 192, no. April, p. 104934, 2024, doi 10.1016/j.jpdc.2024.104934.

[5] M. Soltani, B. Ousat, M. Jafari Siavoshani, and A. H. Jahangir, "An adaptable deep learning-based intrusion detection system to zero-day attacks," *J. Inf. Secure. Appl.*, vol. 76, no. June, p. 103516, 2023, doi: 10.1016/j.jisa.2023.103516.

[6] N. Sameera and M. Shashi, "Deep transductive transfer learning framework for zero-day attack detection," *ICT Express*, vol. 6, no. 4, pp. 361–367, 2020, doi: 10.1016/j.icte.2020.03.003.

[7] N. Ben-Asher and C. Gonzalez, "Training for the Unknown: The Role of Feedback and Similarity in Detecting Zero-day Attacks," *Procedia Manuf.*, vol. 3, no. Ahfe, pp. 1088–1095, 2015, doi: 10.1016/j.promfg.2015.07.180.

[8] M. Sarhan, S. Layeghy, M. Gallagher, and M. Portmann, "From zero-shot machine learning to zero-day attack detection," *Int. J. Inf. Secure.*, vol. 22, no. 4, pp. 947–959, 2023, doi: 10.1007/s10207-023-00676-0.

[9] P. Nemani, Y. D. Joel, P. Vijay, and F. F. Liza, "Gender bias in transformers: A comprehensive review of detection and mitigation strategies," *Nat. Lang. Process. J.*, vol. 6, no. December 2023, p. 100047, 2024, doi: 10.1016/j.nlp.2023.100047.

[10] N. Mearaj and M. A. Wani, "Zero-day Attack Detection with Machine Learning and Deep Learning," *Proc. 17th INDIACom; 2023 10th Int. Conf. Comput. Sustain. Glob. Dev. INDIACom 2023*, pp. 719–725, 2023.

[11] A. Touré, Y. Imine, A. Semnont, T. Delot, and A. Gallais, "A framework for detecting zero-day exploits in network flows," *Comput—networks*, vol. 248, no. May, p. 110476, 2024, doi: 10.1016/j.comnet.2024.110476.

[12] N. Abdalgawad, A. Sajun, Y. Kaddoura, I. A. Zualkernan, and F. Aloul, "Generative Deep Learning to Detect Cyberattacks for the IoT-23 Dataset," *IEEE Access*, vol. 10, pp. 6430–6441, 2022, doi:

10.1109/ACCESS.2021.3140015.

[13] S. Dalal *et al.*, "Extremely boosted neural network for more accurate multi-stage Cyber-attack prediction in the cloud computing environment," *J. Cloud Comput.*, vol. 12, no. 1, 2023, doi: 10.1186/s13677-022-00356- 9.

[14] J. Y. Kim, S. J. Bu, and S. B. Cho, "Zero-day malware detection using transferred generative adversarial networks based on deep autoencoders," *Inf. Sci. (Ny).*, vol. 460–461, pp. 83–102, 2018, doi: 10.1016/j.ins.2018.04.092.

[15] A. Taheri-Garavand, A. Heidari-Maleni, T. Mesri-Gundoshmian, and O. D. Samuel, "Application of artificial neural networks for the prediction of performance and exhaust emissions in IC engine using biodiesel-diesel blends containing quantum dot based on carbon doped," *Energy Convers. Manag. X*, vol. 16, Dec. 2022, doi: 10.1016/j.ecmx.2022.100304.

[16] V. Hnamte, A. A. Najar, H. Nhung-Nguyen, J. Hussain, and M. N. Sugali, "DDoS attack detection and mitigation using deep neural network in SDN environment," *Comput. Secur.*, vol. 138, no. September 2023,

p. 103661, 2024, doi: 10.1016/j.cose.2023.103661.

[17] S. Murtuza and K. Asawa, "Early Prevention and Mitigation of Link Flooding Attacks in Software Defined Networks," *J. Netw. Comput. Appl.*, vol. 224, no. June 2023, p. 103832, 2024, doi: 10.1016/j.jnca.2024.103832.

[18] Y. Wu, Y. Hu, J. Wang, M. Feng, A. Dong, and Y. Yang, "An active learning framework using deep Q-network for zero-day attack detection," *Comput. Secur.*, vol. 139, no. November 2023, p. 103713, 2024, doi: 10.1016/j.cose.2024.103713.

[19] S. Shen, C. Cai, Z. Li, Y. Shen, G. Wu, and S. Yu, "Deep Q-network-based heuristic intrusion detection against edge-based SIoT zero-day attacks," *Appl. Soft Comput.*, vol. 150, no. November 2023, p. 111080, 2024, doi 10.1016/j.asoc.2023.111080.

[20] S. Shen, C. Cai, Z. Li, Y. Shen, G. Wu, and S. Yu, "Deep Q-network-based heuristic intrusion detection against edge-based SIoT zero-day attacks," *Appl. Soft Comput.*, vol. 150, no. June 2023, p. 111080, 2024, doi: 10.1016/j.asoc.2023.111080.

[21] J. F. Cevallos M., A. Rizzardi, S. Sicari, and A. C. Porisini, "NERO: NEural algorithmic reasoning for zero-day attack detection in the IoT: A hybrid approach," *Comput. Secur.*, vol. 142, no. April, p. 103898, 2024, doi: 10.1016/j.cose.2024.103898.

[22] S. Millar, N. McLaughlin, J. Martinez del Rincon, and P. Miller, "Multi-view deep learning for zero-day Android malware detection," *J. Inf. Secure. Appl.*, vol. 58, no. January, p. 102718, 2021, doi: 10.1016/j.jisa.2020.102718.

[23] P. Verma, N. Bharot, J. G. Breslin, D. O'Shea, A. Vidyarthi, and D. Gupta, "Zero-day Guardian: A Dual Model Enabled Federated Learning Framework for Handling Zero-day Attacks in 5G Enabled IIoT," *IEEE Trans. Consum. Electron.*, vol. 70, no. 1, pp. 3856–3866, 2024, doi: 10.1109/TCE.2023.3335385.

[24] A. A. Najar and S. Manohar Naik, "Cyber-Secure SDN: A CNN-Based Approach for Efficient Detection and Mitigation of DDoS attacks," *Comput. Secur.*, vol. 139, no. December 2023, p. 103716, 2024, doi: 10.1016/j.cose.2024.103716.

[25] F. Deldar and M. Abadi, "Deep Learning for Zero-day Malware Detection and Classification: A Survey," *ACM Comput. Surv.*, vol. 56, no. 2, 2023, doi: 10.1145/3605775.

[26] A. Touré, Y. Imine, A. Semnont, T. Delot, and A. Gallais, "A framework for detecting zero-day exploits in network flows," *Comput—networks*, vol. 248, no. April, p. 110476, 2024, doi: 10.1016/j.comnet.2024.110476.

[27] S. Kumar and A. Kumar Keshri, "An effective DDoS attack mitigation strategy for IoT using an optimisation-based adaptive security model," *Knowledge-Based Syst.*, vol. 299, no. June, p. 112052, 2024, doi: 10.1016/j.knosys.2024.112052.

[28] S. Srinivasan and P. Deepalakshmi, "ENetRM: ElasticNet Regression Model based malicious cyber-attacks prediction in real-time server," *Meas. Sensors*, vol. 25, no. December 2022, p. 100654, 2023, doi 10.1016/j.measen.2022.100654.

[29] N. Aslam, S. Srivastava, and M. M. Gore, "DDoS SourceTracer: An Intelligent Application for DDoS Attack Mitigation in SDN," *Comput. Electr. Eng.*, vol. 117, no. February 2023, p. 109282, 2024, doi: 10.1016/j.compeleceng.2024.109282.

[30] Ü. Ağbulut, A. E. Gürel, and S. Sarıdemir, “Experimental investigation and prediction of performance and emission responses of a CI engine fuelled with different metal-oxide based nanoparticles–diesel blends using different machine learning algorithms,” *Energy*, vol. 215, Jan. 2021, doi: 10.1016/j.energy.2020.119076.

[31] B. Naqvi, K. Perova, A. Farooq, I. Makhdoom, S. Oyedeji, and J. Porras, “Mitigation strategies against the phishing attacks: A systematic literature review,” *Comput. Secur.*, vol. 132, p. 103387, 2023, doi 10.1016/j.cose.2023.103387.

[32] K. Hamid, M. W. Iqbal, M. Aqeel, X. Liu, and M. Arif, Analysis of Techniques for Detection and Removal of Zero-day Attacks (ZDA), vol. 1768 CCIS, no. July. Springer Nature Singapore, 2023. doi: 10.1007/978-981- 99-0272-9_17.

[33] H. Tran, E. Campos-Nanez, P. Fomin, and J. Wasek, “Cyber resilience recovery model to combat zero-day malware attacks,” Comput. Secur., vol. 61, pp. 19–31, 2016, doi: 10.1016/j.cose.2016.05.001.

[34] U. Ahmed, J. C. W. Lin, and G. Srivastava, “Mitigating adversarial evasion attacks of ransomware using ensemble learning,” Comput. Electr. Eng., vol. 100, no. March, p. 107903, 2022, doi: 10.1016/j.compeleceng.2022.107903.

[35] P. Liu and Y. Zhang, "Optimisation of biodiesel production from oil using a novel green catalyst via the development of a predictive model," Arab. J. Chem., vol. 16, no. 6, Jun. 2023, doi: 10.1016/j.arabjc.2023.104785.

[36] M. Nkongolo, J. P. van Deventer, and S. M. Kasongo, “Ugransome1819: A novel dataset for anomaly detection and zero-day threats,” Inf., vol. 12, no. 10, 2021, doi: 10.3390/info12100405.

[37] V. Kumar and D. Sinha, “A robust intelligent zero-day cyber-attack detection technique,” Complex Intell. Syst., vol. 7, no. 5, pp. 2211–2234, 2021, doi: 10.1007/s40747-021-00396-9.

[38] R. Kumar, “Zero-day Malware Detection and Effective Malware Analysis,” 2022.

[39] A. Blaise, M. Bouet, V. Conan, and S. Secci, “Detection of zero-day attacks: An unsupervised port-based approach,” Comput. Networks, vol. 180, no. April, 2020, doi: 10.1016/j.comnet.2020.107391.

[40] I. M. Yusri, A. P. P. Abdul Majeed, R. Mamat, M. F. Ghazali, O. I. Awad, and W. H. Azmi, “A review on the application of response surface method and artificial neural network in engine performance and exhaust emissions characteristics in alternative fuel,” Renewable and Sustainable Energy Reviews, vol. 90. Elsevier Ltd, pp. 665–686, Jul. 01, 2018. doi: 10.1016/j.rser.2018.03.095.

[41] M. Nkongolo, J. P. van Deventer, S. M. Kasongo, S. R. Zahra, and J. Kipongo, "A Cloud Based Optimisation Method for Zero-day Threats Detection Using Genetic Algorithm and Ensemble Learning," Electron., vol. 11, no. 11, pp. 1–26, 2022, doi: 10.3390/electronics11111749.

[42] M. Zandie, H. K. Ng, S. Gan, M. F. Muhamad Said, and X. Cheng, “Multi-input multi-output machine learning predictive model for engine performance and stability, emissions, combustion and ignition characteristics of diesel-biodiesel-gasoline blends,” Energy, vol. 262, Jan. 2023, doi: 10.1016/j.energy.2022.125425.

[43] V. V. Vegesna, "Adopting a Conceptual Architecture to Mitigate an IoT Zero-day Threat that Might Result in a Zero-day Attack about Operational Costs and Communication Overheads," Int. J. Curr. Eng. Sci. Res., vol. 10, no. October, pp. 9–17, 2023.

[44] A. Das, Pramod, and S. Praveen Kumar, "An Enhanced Optimisation Model With Ensemble Autoencoder for Zero-day Attack Detection," J. Theor. Appl. Inf. Technol., vol. 100, no. 22, pp. 6717–6730, 2022.

[45] Y. Guo, “A review of Machine Learning-based zero-day attack detection: Challenges and future directions,” Comput. Commun., vol. 198, no. July 2022, pp. 175–185, 2023, doi: 10.1016/j.comcom.2022.11.001.

[46] C. Singh and A. K. Jain, “A comprehensive survey on DDoS attacks detection & mitigation in SDN-IoT network,” e-Prime - Adv. Electr. Eng. Electron. Energy, vol. 8, no. April, p. 100543, 2024, doi: 10.1016/j.prime.2024.100543.

[47] U. E. H. Tayyab, F. B. Khan, M. H. Durand, A. Khan, and Y. S. Lee, "A Survey of the Recent Trends in Deep Learning Based Malware Detection," J. Cybersecurity Priv., vol. 2, no. 4, pp. 800–829, 2022, doi 10.3390/jcp2040041.

[48] D. O. Won, Y. N. Jang, and S. W. Lee, “PlausMal-GAN: Plausible Malware Training Based on Generative Adversarial Networks for Analogous Zero-day Malware Detection,” IEEE Trans. Emerg. Top. Comput., vol. 11, no. 1, pp. 82–94, 2023, doi: 10.1109/TETC.2022.3170544.