2025 12th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)
Amity University, Noida, India. Sep 18-19, 2025

2025 12th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO) | 979-8-3315-5421-7/25/$31.00 ©2025 IEEE | DOI: 10.1109/ICRITO66076.2025.11241728

A Review Study on Zero-Day Attacks in Intrusion Detection System

Urvashi Sangwan
School of computer Applications
MRIIRS,
Faridabad
urvashibaswana.84@gmail.com

Suhail Javed Quraishi
School of computer Applications
MRIIRS,
Faridabad
suhailjaved.sca@mriu.edu.in

Abstract **- In this contemporary world, cyber threats and vulnerabilities are growing exponentially with the growing network, thereby emphasizing the need for a strong defense mechanism. Zero-day attacks (ZDA) is one of the crucial ones with catastrophic impact, including monetary losses and data breaches compromising essential infrastructure and, in certain cases, even threats to national security. The review paper focuses on effective techniques for the detection of zero-day attacks. For this review paper, we have studied various Research papers, Articles, and Reports by various security service stakeholders between 2020 to 2025. By evaluating the existing literature, we understand the patterns of the cyberattacks and various Artificial Intelligence (AI) techniques used by cybersecurity analysts to detect and mitigate the threats. According to the findings, investment in AI approaches for the detection of zero-day attacks has improved attack identification efficiency and decreased overall handling costs. Moreover, the hybrid ensemble models using Machine Learning (ML) & Deep Learning (DL) techniques are used for the zero-day detection with the highest efficacy to strengthen the security in the cyber world. The paper assists in integrating the ML and DL techniques to create a multi-powered model for zero-day attack detection.**

Keywords: Anomalies, Breaches, Cybersecurity, Intrusion Detection System, Zero-day attack

I. INTRODUCTION

Cyber security encloses the technologies and methods for safeguarding data, computers, networks, and interconnected systems from any potential attacks that may endanger system's confidentiality, integrity, and availability. Among these threats, zero-day assaults are extremely nimble and pose a serious risk to the security of both hardware and software systems[1]. Although, security patches and mitigation strategies can address known vulnerabilities, zero-day vulnerabilities remain unidentified. These attacks come from the fact that they take use of flaws in the targeted system or network infrastructures that software developers were previously unaware of. ZDA are extremely difficult for both modern and conventional security solutions to detect because of their novelty. It is crucial to address them to ensure comprehensive security.

The CrowdStrike event of July 19, 2024, made it clear how urgent it is to stop zero-day attacks. A boot loop occurred on Windows devices as a result of CrowdsStrike's automated content validator failing to detect problematic content data in a configuration update. This incident impacted almost 8.5 million Windows devices globally either by crashing or stuck in boot, and affected companies from a variety of industries, including media, healthcare, banking, and airlines, highlighting serious operational hazard[2].

During 2024, more than half (53%), of newly discovered widespread threat vulnerabilities were exploited before software developers could publish updates[3]. Thereby, it is extremely important to strengthen the cybersecurity against such an unpredictable and baffling threat of zero-day attacks. An intrusion detection system (IDS) is one of the most important defenses in the cyber system for identifying irregularities[4].

In this paper, Section II provided the detailed study about various ML and DL algorithms used for the detection mechanism. Section III illustrates cost of data breaches and attacks pattern since 2018 on the basis of various reports from security service providers. Section IV concludes the paper and future scope.

II. LITERATURE REVIEW

For thorough threat management, a multi-layered strategy incorporating behavior analysis, pattern matching, and anomaly detection is necessary for zero-day attacks(ZDA) protection. ML and DL have emerged as a promising technique for bolstering cybersecurity defenses in recent years [17]. As it offers automated detection and response mechanisms, that are adaptable enough to change with evolving threat landscapes.

A. Detection using supervised learning

Traditionally, the supervised learning techniques of ML and DL were used on labeled input data which has corresponding expected results, to find out signature or pattern of the network or the host. When given high-quality labeled data and a clear prediction task, supervised learning works quite well. However, it requires detailed information on each type of attacks upfront during the training time.

Ibraheem, I. O. et al.[5] studied and compared four ML algorithms: Gradient Boosting, Decision Trees, Random Forests, and Support Vector Machines (SVM). The results demonstrated Random Forest to detect ZDA with highest accuracy of 92% due to its ability of continuously enhancing performance by learning from previous mistakes. In another Review, Ahanger, A. S. et al.[19] proposed an IDS system by integrating Supervised Machine learning algorithms to detect the known and unknown attacks. The four ML algorithms Random Forest, Decision Tree (DT), Multi layer perceptron (MLP) and SVM are used for the data classification as normal and abnormal. The model gives an precision score of more than

99% when trained and tested with three feature subsets randomly chosen from NSL-KDD dataset.

Fevid, E. et al.[6] has put forward an efficient framework for ransomware ZDA detection in real time environment. The author used assembly language bytecode analysis, a static analysis techniques, which provides logical characteristics of ransomware. By integrating it with Random Forest (RF) classifier, a ML technique's capability of handling complicated feature spaces and big datasets with ease.

Zaki, R. M. et al.[7] suggested a hybrid IDS using ensemble stacking of the three classifiers - XGBoost, K-Nearest-Neighbors (KNN), and Stochastic Gradient Descent (SGD) on Internet of Things (IoT) networks to detect cyber attacks. The model provides an accuracy of 99.91% when tested on CIC-IDS2017 and CICDDoS2019 datasets. Grid Search CV mechanism encouraged to get best hyper-parameters for each classifiers at each classification stage and the feature selection was performed by Random Projection. The model was capable to detect the DDoS ZDA in 0.22sec.

When given high-quality labeled data and a clear prediction task, supervised learning works quite well. However, in practice, it's dependence on labeled data and tendency toward over-fitting, can present serious difficulties. The high number of false positives and negatives caused by supervised learning makes it difficult to distinguish between malicious and benign data, which makes it difficult to detect ZDA. Therefore, it is typically used in conjunction with other methods rather than alone to identify Zero-Day threats[8].

B. Detection using unsupervised or semi-supervised learning

Anomaly based detection is featured by unsupervised learning which focuses on learning from unlabeled data. Which comes out to be more effective solution to detect the fresh attacks with little prior knowledge and self-training feature. However, fall short from high false positives[4]. This leads to wrongly identify the legitimate as malicious one. Consequently, their performance and practical utility are limited. Semi-supervised learning combines the benefits of supervised and unsupervised learning and train the model with small labeled and large unlabeled data and provides better results in detection novel attacks compared to traditional signature-based approach [25][18].

The authors [25] proposed an unsupervised hybrid ensemble model for detecting DDoS attack in IoT network. Comprising unsupervised feature reduction by Gaussian Random Projection(GRP) and hard voting techniques among the three classification algorithm - Gaussian mixture model (GMM) , the Stochastic Gradient Descent One class SVM (SGDoneclass) classifier, and k-means. The model provided an accuracy of 94.5% when tested on CIC-DDoS2019.

A model utilizing DL techinques, encoding-decoding features of autoencoders, i.e. excellent at identifying intricate ZDA was suggested by Hindy, H. et al.[9]. The results shows the reduced miss rate (false-positives), better recall rates and a higher detection accuracy of 89-99% when tested on MSL-KDD and 75-98% on CIC-IDS2017 datasets. Autoencoder was found superior on comparative analysis of proposed model and outlier based ML technique - One-class SVM (OCSVM).

Touré, A. et al.[10] proposed a hybrid learning approach utilizing significance of integrating supervised and unsupervised learning in classification. While unsupervised algorithms like K-Means is used to reveal hidden patterns in the data. CNN, a supervised algorithm, helps classify known network flows. In order to maximize the detection model's precision some supervised algorithms are coupled with boosting methods. The effectiveness of the method is in detecting abnormalities related to the flow of ZDA is validated by an online supervised learning process.

Shen, S et al.[11] developed a proposal for DQN-HIDS, a heuristic learning intrusion detection system using Deep Q-Networks (DQN) for edge-based SIoT networks in the midst of a lack of training samples. By incorporating deep neural networks into Q-learning, the Deep Q-Network (DQN) can operate in a wide state space and interpret environmental observations to pursue optimal strategies even in the absence of knowledge about the environment's state.

Comar, P. M. et al.[12] introduces a two-level malware detection system, firstly to identify between malicious and benign flow and then uses a class-based profiling technique to distinguish between new and existing malware. Additionally, it creates a tree-based kernel for one-class SVM (OCSVM) classifiers to address the problems with data imperfection that occur in network flow data.

Siregar, S. M[13] utilized the potential of semi supervised algorithm One-class SVM on CIC-IDS2017 dataset for anomaly detection. During the preprocessing phase KBest techniques is also integrated for feature selection process. It illustrated how the feature selection technique improved the overall efficiency of OCSVM algorithm. Moreover, it focused how a unsupervised or semi-supervised would be better to detect out anomalies.

C. Detection using Meta learning

Meta learning is another advance technique which revolutionized the ZDA detection by optimizing hyper-parameters across tasks and adapts to new environments quickly. The concept is built by mimicking human problem-solving techniques, where people can swiftly draw up new information based on what they already know during learning. Its goal is to use less data training to rapidly produce a model with great generalization and high accuracy.

Zoppi, T et al.[4] compared and found that meta learning with unsupervised algorithm is better than the unsupervised algorithm in detecting the anomalies. Yang, A.et al.[14] has utilized the meta-optimizer based on Online Met Learning (OML) and Long Short-Term Memory that exhibits remarkable versatility in addressing real-world issues by modifying the basic learners' parameters. It also showcase its application in IDS, spam detection, anomaly detection,network traffic analysis and many more areas other than cyber security. Table 1. summarizes the ML and DL techniques utilized for ZDA detection approaches with their findings and limitations.

TABLE I. Summary of ML & DL Based Zero-Day Attack detection approaches

Reference	Dataset used	Algorithm Implemented	Accuracy	Research Finding	Research Gap
Ibraheem et al. 2024 [5]	CIC-IDS2018	Gradient Boosting classifiers, RF, DT, and SVM	(DT) 85% (RF) 92% (RF) 88% (GB) 90%	Comparative analysis of the various ML algorithms used for detection of ZDA ,where random forest achieved more accuracy than any others.	Only detection is focused, mitigation is missing.
Siregaret al. 2023 [13]	CIC-IDS2017 and CIC-DDoS2019	XGBoost, KNN, and Stochastic Gradient, SGD, Random projection	Accuracy 99.91 %, Precesion 99.83 % Recall 99.70 % F1 score 99.84 %	Hybrid IDS which achieved a very high accuracy in detecting attacks, significantly reduce false alarms and improve the detection time and reduce the computational complexity using ML techniques on IOT n/w.	Detect more types of attack and reduce detection time.
Roopaeet al. 2024 [10]	CIC-DDoS2019	Clustering algorithms: combining K-means, Gaussian mixture model(GMM), and OCSVM with a hard voting technique for classification.	Accuracy of 94.5%, Precision 93.3 % Recall 95.3 % F1 score 94.3 %	ZDA detection using unsupervised ML algorithm for DDoS attack.	Automated mitigation beyond mere detection. Regularize the Upgradation of model as per novelty.
Hindy et al 2020 [9]	CICIDS2017, NSL-KDD	DL - Autoencoder , ML - OCSVM	89-99% (NSL-KDD) 75-98% (CICIDS2017)	ZDA detection, using Deep learning by an autoencoder model. Encoding-decoding capability is used and also found it superior to OCSVM.	Model do not account for attack behavior, and many attacks and false alarms
Zhang et al.2020 [20]	NSL_KDD	Encoder, Sementic Encoder (SAE), New ZSL	67% (SAE) 86% (Encoder) 88.3% (Novel ZSL)	Feature descriptions of unknown attacks is sufficient rather than detailed sample using zero-short learning .	Updated Datasets required. Moreover, semantic description should be taken from various network security BBS.
Sarhan et al. 2023 [21]	UNSW-NB15, NF-UNSW-NB15-v2 (synthetic DS)	Random Forest(RF) Multi-Layer Perceptron (MLP)		Zero short ML based model is evaluated on 2 datasets for 2 algorithms and results are analyzed using the Wasserstein Distance (WD) technique.	To enhance its generality to new attack types.
Kumar et al. [22]	CICIDS18	Heavy-hitter , Graph techniques	91.33% - binary classification 90.35% - multi-class classification	The model for detecting ZDA works in two phases- signature generation and evaluation, where heavy-hitter for high volume attacks and graph technique for low volume attacks are used.	accuracy and time complexity needs to be optimized.
Aru et al. 2024 [23]	CICIDS2017 ,NSL -KDD	Dynamic LSTM based Anomaly Detection (DLAD).	99.50% (Validation) Accuracy 99.25% precision 98.88% Recall 98.78% F1 score 98.76%.	Detecting anomalies and adapt to change network behaviors to detect ZDA using DL	Existing analyses conducted against known datasets, need for datasets that include instances of zero-day malware.
Ibrahim et al. 2023 [24]	TON-IoT	DL-CNN ML-NB,LR,AdaBoost	CNN+Regularization = 98% CNN +Non-regularization = 83% Classical ML 32 - 61%	Anomaly detection using CNN, with and without regularization methods, and classical ML algorithms. These DL-based methods are able to decrease the over-fitting issue.	Accuracy needs to be improved.

III. Methodology

The methodology for this review paper is designed by exploring research papers, articles and the latest data breach investigations reports by security service provider. Exploring the possible techniques utilized for detecting the Zero-Day Attacks.

A. Search Methodology

We developed a search method by combining keywords and controlled vocabulary terms related to threat, anomaly, and intrusion detection with the study questions and objectives. We utilized boolean operators, such as AND and OR, along with various combinations of the search phrases. The following search phrases have been selected for this study:

(“Zero-day attack” OR “zero-day” OR “0-day” OR “vulnerabilities”) AND (“intrusion detection” OR “anomaly detection” OR “threat detection”) AND (“ Mitigation” OR)

B. Survey

The IBM 2024 Data Breach Report states that the average global cost of a data breach in 2024 was 4.88 million dollars, which is the largest amount ever after the pandemic and a 10% rise over the previous year as shown in Fig 1. The Healthcare sector is the most affected one with 9.77 million dollars this year, though little lesser then last year [15].

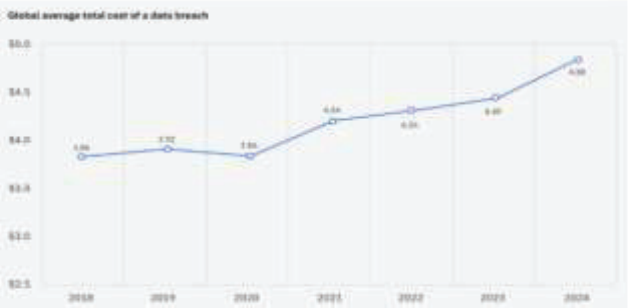

Fig. 1. Total Cost of data breach measured in USD Million [15]

The another most significant finding of the report was the organizations who used AI in their preventative procedures saw an average reduction in breach costs of USD 2.2 million [15]. AI driven detection technique has reduced the response time, both Mean time to Identify (MTTI) & Mean time to Contain(MTTC). However, Fig 2. shows that zero-day vulnerabilities detection is faster using ML & DL techniques but still struggling to mitigate the impact of an exploit due to unknown vulnerabilities.

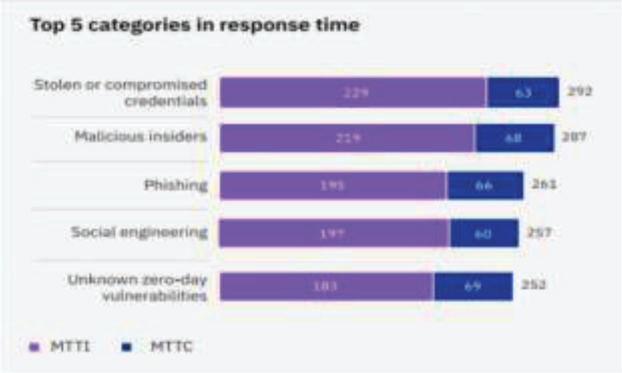

Fig. 2. Response time measured in days [15]

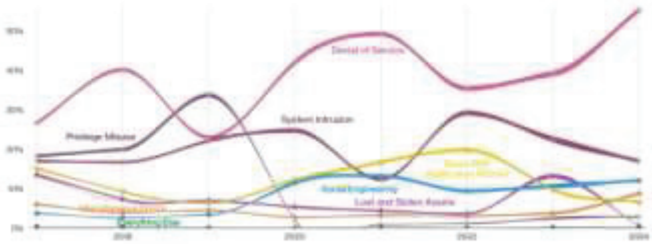

Fig. 3. Attack Patterns over time in incidence [16]

The different patterns in breaches changed over the past few years has been demonstrated in Fig 3. DoS attack continues to rule, and system intrusion remains most common. Since last year, there has been a noticeable increase in both the Social Engineering and Miscellaneous Errors patterns, especially the latter. On the other hand, the Basic Web Application Attacks pattern has significantly decreased since it was included in the 2023 DBIR [16].

C. Limitation & Challenges

Traditional detection techniques are inadequate because ZDA are inherently unique, and ML models frequently lack relevant datasets. Furthermore, current models cannot be modified in real time because they are constructed using attack data from the past. The models continuously needs to updated for effectively and efficient detection.

Challenges faced by current models :

- High False Positives and Negatives
- Dataset for training needs to be timely updated
- For ZDA detection the model needs to be updated continuously

IV. Conclusion

The cyber attacks are increasing at an alarming rate and proportionally the cost involved in data breaches. Simultaneously the need of the security tools to detect and mitigate them. AI has tremendously reduced the costing by automating detection and incidence response techniques, taken to combat the impact of attack. ML techniques utilized for detection where the static structure of signature repositories is used, faces challenges to adjust to new attack patterns, and is also time-consuming to obtain such a vast amount of labeled data. Thereby, supervised learning method is likely to result in a large number of false positives and negatives, and struggling to identifying between benign and malicious data. Ensemble model created using Semi-supervised ML algorithm outperforms by integrating the power of both supervised and. Mostly model firstly distinguish between the legitimate and the anomalies followed by classification model to categorize the attacks using various ML and DL algorithms. Moreover, few models focuses on feature reduction algorithms which is critically important to enhance the overall efficiency by reducing the data dimensional of the dataset.

This review will help the researcher to further identifying the best ensemble hybrid model for there IDS to detect the abnormalities in the system to strengthen the security by considering the provided approaches. Moreover, regular updates and improvements to the model is required for a robust and secure real-time IDS.

V. ReferenceS

[1] Kaloudi, N., & Li, J. (2020). The ai-based cyber threat landscape: A survey. ACM Computing Surveys (CSUR), 53(1), 1-34.

[2] https://www.computerweekly.com/feature/CrowdStrike-update-chaos-explained-What-you-need-to-know

[3] Rapid7 2024 Attack Intelligence Report https://www.rapid7.com/globalassets/_pdfs/research/rapid7_2024_attack_intelligence_report.pdf?utm_source=chatgpt.com

[4] Zoppi, T., Ceccarelli, A., & Bondavalli, A. (2021). Unsupervised algorithms to detect zero-day attacks: Strategy and application. Ieee Access, 9, 90603-90615.

[5] Ibraheem, I. O., & Tosho, A. U. Zero day attack vulnerabilities: mitigation using machine learning for performance evaluation. Journal of Computers for Society, 5(1), 43-58.

[6] Fevid, E., Walsh, C., & Russo, L. (2024). Zero-day ransomware detection via assembly language bytecode analysis and random forest classification. Authorea Preprints.

[7] Zaki, R. M., & Naser, I. S. (2024). Hybrid Classifier for Detecting Zero-Day Attacks on IoT Networks. Mesopotamian Journal of CyberSecurity, 4(3), 59-74.

[8] Mbona, I., & Eloff, J. H. (2022). Detecting zero-day intrusion attacks using semi-supervised machine learning approaches. IEEE Access, 10, 69822-69838.

[9] Hindy, H., Atkinson, R., Tachtatzis, C., Colin, J. N., Bayne, E., & Bellekens, X. (2020). Utilising deep learning techniques for effective zero-day attack detection. Electronics, 9(10), 1684.

[10] Touré, A., Imine, Y., Semnont, A., Delot, T., & Gallais, A. (2024). A framework for detecting zero-day exploits in network flows. Computer Networks, 248, 110476

[11] Shen, S., Cai, C., Li, Z., Shen, Y., Wu, G., & Yu, S. (2024). Deep Q-network-based heuristic intrusion detection against edge-based SIoT zero-day attacks. Applied Soft Computing, 150, 111080.

[12] Comar, P. M., Liu, L., Saha, S., Tan, P. N., & Nucci, A. (2013, April). Combining supervised and unsupervised learning for zero-day malware detection. In 2013 Proceedings IEEE INFOCOM (pp. 2022-2030). IEEE.

[13] Siregar, S. M., Purwanto, Y., & Wibowo, S. A. (2023, December). Enhancing Network Anomaly Detection with Optimized One-Class SVM (OCSVM). In 2023 3rd International Conference on Intelligent Cybernetics Technology & Applications (ICICyTA) (pp. 84-88). IEEE.

[14] Yang, A., Lu, C., Li, J., Huang, X., Ji, T., Li, X., & Sheng, Y. (2023). Application of meta-learning in cyberspace security: A survey. Digital Communications and Networks, 9(1), 67-78.

[15] IBM security report: Data breach cost 2024, https://www.ibm.com/reports/data-breach

[16] “Verizon data breach investigations report,” 2024, [online] https://www.verizon.com/business/resources/Tc43/reports/2024-dbir-data-breach-investigations-report.pdf

[17] Zhou, Q., & Pezaros, D. (2019). Evaluation of machine learning classifiers for zero-day intrusion detection--an analysis on CIC-AWS-2018 dataset. arXiv preprint arXiv:1905.03685.

[18] Alrassan, I., & Alqahtani, A. (2023, June). Detection of ddos attacks on clouds computing environments using machine learning techniques. In 2023 International Conference on Intelligent Computing, Communication, Networking and Services (ICCNS) (pp. 190-196). IEEE.

[19] Ahanger, A. S., Khan, S. M., & Masoodi, F. (2021, April). An effective intrusion detection system using supervised machine learning techniques. In 2021 5th International Conference on Computing Methodologies and Communication (ICCMC) (pp. 1639-1644). IEEE.

[20] Zhang, Z., Liu, Q., Qiu, S., Zhou, S., & Zhang, C. (2020). Unknown attack detection based on zero-shot learning. IEEE Access, 8, 193981-193991.

[21] Sarhan, M., Layeghy, S., Gallagher, M., & Portmann, M. (2023). From zero-shot machine learning to zero-day attack detection. International Journal of Information Security, 22(4), 947-959.

[22] Kumar, V., Sinha, D.: A robust intelligent zero-day cyber-attack detection technique. Complex Intell. Syst. 7(5), 2211–2234 (2021)

[23] Arun, A., Nair, A. S., & Sreedevi, A. G. (2024, January). Zero Day Attack Detection and Simulation through Deep Learning Techniques. In 2024 14th International Conference on Cloud Computing, Data Science & Engineering (Confluence) (pp. 852-857). IEEE.

[24] Ibrahim Hairab, B., Aslan, H. K., Elsayed, M. S., Jurcut, A. D., & Azer, M. A. (2023). Anomaly detection of zero-day attacks based on CNN and regularization techniques. Electronics, 12(3), 573.

[25] Roopak, M., Parkinson, S., Tian, G. Y., Ran, Y., Khan, S., & Chandrasekaran, B. (2024). An unsupervised approach for the detection of zero-day distributed denial of service attacks in Internet of Things networks. IET Networks, 13(5-6), 513-527.