Zero-day Attack Detection with Machine Learning and Deep Learning

Nowsheen Meraj
Department of Computer Science
University of Kashmir
Kashmir, India
nousheen.meraj60@gmail.com

M. Arif Wani
Department of Computer Science
University of Kashmir
Kashmir, India
awani@uok.edu.in

***Abstract*— The most serious risk to network security can arise from a zero-day attack. Zero-day attacks are challenging to identify as they exhibit unseen behavior. Intrusion detection systems (IDS) have gained considerable attention as an effective tool for detecting such attacks. IDS are deployed in network systems to monitor the network and to detect any potential threats. Recently, a lot of Machine learning (ML) and Deep Learning (DL) techniques have been employed in Intrusion Detection Systems, and it has been found that these techniques can detect zero-day attacks efficiently. This paper provides an overview of the background, importance, and different types of ML and DL techniques adopted for detecting zero-day attacks. Then it conducts a comprehensive review of recent ML and DL techniques for detecting zero-day attacks and discusses the associated issues. Further, we analyze the results and highlight the research challenges and future scope for improving the ML and DL approaches for zero-day attack detection.**

Keywords*— *Zero-day attacks, Intrusion Detection System, Machine Learning, Deep Learning

I. Introduction

Cyber security refers to the technologies and methods used for protecting data, computers, networks, and other inter-connected systems from attacks that could compromise system confidentiality, integrity, and availability [1][2]. Recently, many reports on cyber security incidents highlight a rise in cyber-attacks, particularly zero-day attacks. A zero-day attack is defined as a type of cyberattack that is unknown or has not yet been made public. Software systems often have vulnerabilities that could be exploited by the cybercriminals. If the cybercriminal is successful in exploiting the vulnerability before software developers can find a patch, that exploit becomes a "zero-day attack". Zero-day attack aims to exploit the system's known or unknown vulnerabilities [3], and the software developers have zero days to fix that vulnerability, hence the term "zero-day". According to the findings of [4], zero-day attack averagely takes 312 days to be detected and until then, the number of attacks continue to increase by as much as five times. In "Project zero" [5], Google publishes a record of previously detected zero-day attack instances and it is found that a typical zero-day attack is identified every 17 days, with 15 days required to find a solution to that zero-day vulnerability. The well-known zero-day vulnerability attacks include Aurora attacks, which targeted various companies like Google, Juniper Networks, Rackspace, Adobe Systems, etc. [6]. Stuxnet is one of the most sophisticated threats ever launched. To evade the detection, it uses stolen digital certificates [7] and replicates itself over networks until it arrives at the target system [8]. In the RSA Advanced Persistent Threat (APT) breach, the attackers stole information concerning two-factor authentication of RSA SecurID by utilizing an APT attack. The APT took an advantage of remote code execution vulnerability in Adobe Flash Player [7]. Malicious Excel files or Microsoft Word files were attached to emails addressed to the victims [7], [9]. Attacks using the DarkLeech malware were directed at web servers. The Darkleech campaign was able to successfully breach over 40,000 web servers. Majority of the victims used Apache web servers [9] and malware like the Nymaim ransomware had been distributed on infected systems. Zero-day attacks can result in significant financial losses, data breaches, system disruptions, privacy invasions, and legal consequences causing widespread harm to individuals and organizations.

Due to exponential rise in zero-day cyberthreats, it becomes essential to identify and counteract them [10][11], and Intrusion Detection Systems (IDS) are designed to protect against these growing threats. IDS monitor the network traffic and identify any kind of intrusive behaviour [12]. IDS are commonly used in combination with other security tools, like antivirus software and firewalls, to achieve a comprehensive security. The existing IDS show efficiency in detecting both known and unknown attacks. Researchers have been exploring the applicability of ML and DL methods for the detection of such unseen attacks [13], [14]. ML and DL models extract features, patterns, and relationships from network data and on the basis of learned patterns, normal and intrusive activities are identified [15]. A great deal of study has been conducted to make ML and DL based IDS efficient for detecting zero-day attacks. This study aims to present an overview of recent research on machine learning and deep learning-based security approaches designed for detecting zero-day attacks. The main contributions of this paper are: (i) to provide a comprehensive review of ML and DL based approaches focusing on the issues, challenges, and research gaps (ii) to discuss and analyse the results of novel techniques (iii) to highlight various challenges and research directions in this particular domain. Rest of the paper is structured as follows: Section II and III provide background, importance, and types of ML and DL algorithms. Section IV provides a comprehensive review of classification methods discussing challenges and research gaps. Section V provides details about the results on benchmark datasets and highlights the future directions. Section VI concludes the paper.

II. Machine Learning

Machine Learning (ML) is defined as a process that focusses on the automation of knowledge acquisition and the

978-93-80544-47-2/23/©BVICAM, New Delhi, India

development of algorithms that can learn from data [16]. The field of machine learning holds a great potential for detecting zero-day attacks. ML algorithms build models that automatically learn from training data, identify patterns, detect well-known attacks, and respond to the changes in attack behaviour. In recent years, ML algorithms have been extensively studied for their effectiveness in detecting zero-day attacks. ML techniques are based on either a single classifier or an ensemble of classifiers. Some of the popular types of ML algorithms used are:

A. *One-Class Support Vector Machine (OCSVM)*

OCSVM is a machine learning algorithm specifically used for novelty detection. It is designed to identify anomalies or outliers in data. This algorithm works by finding a decision boundary that maximizes the margin between the closest datapoints and the boundary itself, and then classifies new data points based on their proximity to this boundary. In OCSVM, only one class, which is a "benign" class here, is used for training. It constructs a hyper plane that finds a boundary to enclose all the benign data. If the data point falls outside the boundary, that point is considered as a "zero-day attack" [17].

B. *Density-based Spatial* Clustering *of Applications with Noise (DBSCAN)*

DBSCAN is a density-based clustering algorithm that has the ability to cluster densely packed data [18]. In general, the data points in the cluster have similar properties and are distinguished from those in other clusters. DBSCAN groups the data points that are close to each other based on distance metric, and density and separates them into high-density and low-density regions. The high-density feature space is considered to be normal data, while low-density features are classified as outliers. The main idea behind utilizing DBSCAN for detecting zero-day attacks is that most network traffic data is normal, and the attack data is rare and distinct from normal data.

C. *k-Means Clustering*

In the field of ML, k-means clustering algorithm is used for grouping similar data points into predefined "k" number of clusters. The clustering process takes place in an iterative manner until convergence is reached. The result is that each cluster contains data that is similar to each other. The cluster centroid is assigned as a mean value of data points in a cluster. In the case of zero-day attacks, k-means algorithm groups the data into two clusters i.e., Benign and Zero-day attacks.

III. Deep Learning

In recent years, deep learning has emerged as one of the widely used and most applicable technique in Intrusion detection systems. The deep learning model consists of many hidden layers that are designed to identify the best features for detecting patterns in raw data. DL has been applied to various applications like recognition and classification. This paper, however, focusses specifically on DL techniques for detecting zero-day attacks. Some of the DL approaches that have been used are:

A. *Artificial Neural Network(ANN)*

ANN is a type of deep learning model composed of multiple layers including an input layer, intermediate hidden layers, and an output layer. The layers consist of multiple processing nodes, called neurons, that process information and generate output based on learned patterns and relationships. For detecting zero-day attacks, ANN can be used as a pattern recognition. The output of ANN represents a benign or zero-day attack class. The parameters of a neural network are optimized during training, which is responsible for associating outputs with the corresponding inputs.

B. *Autoencoder*

An Autoencoder is trained to reconstruct its input by encoding the input data into a low-dimensional representation, known as a bottle neck, and then decoding it back to its original form. The model minimizes the reconstruction error during training. The architecture of an autoencoder consists of two components: an encoder and a decoder. The encoder takes the original input and transforms it into a compact latent representation. The decoder gives the final output by reconstructing the original input from the latent representation. The output should be same as input. Originally, autoencoders were intended to be used for feature learning and dimensionality reduction. Autoencoders are now a popular reconstruction technique and their application in the detection of zero-day attacks is based on the assumption that the 'normal data' will have a low reconstruction error. If the reconstruction error of an incoming sample is larger than a specified threshold, that sample is flagged as a "zero-day attack".

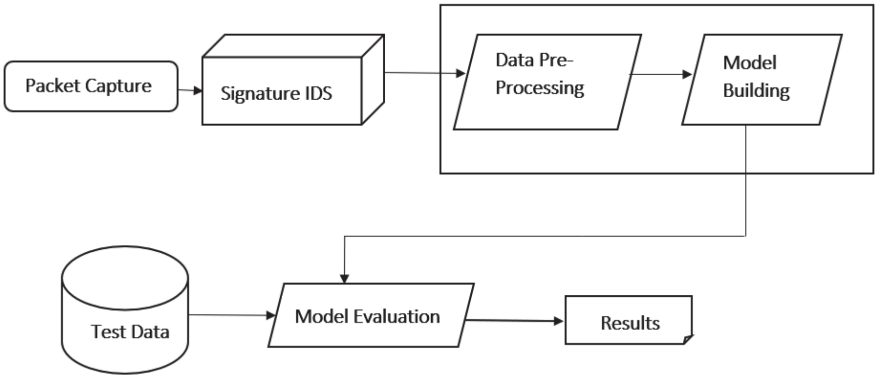

Fig. 1. Architecture of OCSVM Intrusion Detection System

C. Generative Adversarial Networks (GAN)

The architecture of GAN model is made up of a generator and discriminator that interact adversarially. The input of generator is a random variable, and its job is to generate the fake data similar to the training data. The discriminator is trained to differentiate the fake generated data from the real samples. After training, discriminator of a GAN should classify a testing sample either as “benign” or a “Zero-day attack”.

IV. Machine Learning and Deep Learning Techniques for Detection of Zero-Day Attacks

Zero-day attacks refer to previously undisclosed and novel form of attacks. Not only are new zero-day attacks being developed, but the existing attacks can also evolve by self- mutating or using encryption to evade detection. Hence, it remains a major challenge for cyber security practitioners to detect such evolving attacks. In [19], authors solved the problem of the polymorphic nature of attacks by implementing a framework based on OCSVM. Fig. 1 depicts the framework. The main aim of this technique is to identify and categorize an incoming traffic as a known attack, polymorphic attack, or a completely new developed zero-day attack. The classifier consists of several One-Class SVM modules, each of which categorizes the instances of specific attack classes. At the time of testing, when an incoming traffic sample is different from trained attacks, that incoming sample is detected as a “zero-day attack”. One-class SVM can perform better in terms of false positives, false negatives, true negatives, F-Measure, recall, accuracy, and specificity. In [20], the authors developed a lightweight IDS based on OCSVM to keep the detection rate high while minimizing false alarms. Pu et al. [21] utilized OCSVM to identify zero-day network intrusion threat and trained the model using a single class (benign network only). The authors in [22] evaluated various semi-supervised ML techniques. The experimental findings show that one-class SVMs have the highest performance in identifying zero-day attacks with F1 Score of 85%. OCSVM’s class-profiling technique is a good choice for the identification of zero-day attacks. However, as the attack classes increase in number, the detection phase gets expensive.

The ability of DBSCAN's to discover clusters, in any shape, has demonstrated its high detection rate for zero-day attacks. Fig. 2 illustrates the state-of-art framework proposed by [3] based on DBSCAN for zero-day attack detection in which detection process takes place using two separate engines. The model uses the live network traffic as an input. The first engine monitors the network behavior to identify any substantial changes that might be brought on by intrusions. The second engine traces zero-day attacks and blocks the communication that may cause future attacks against the monitored network. The proposed model achieves higher accuracy, recall and precision rates compared to well-known DBSCAN and K-means outlier detection techniques. One of the significant challenges in machine learning-based IDS is the imbalance in training data, which can lead to a bias towards normal behavior [23][24]. Therefore, the authors in [25] implement a hyper-clustering model based on DBSCAN for detecting zero-day attacks. To address the challenge of imbalance in datasets, the authors propose an extended DBSCAN (EDBSCAN) method, build upon the existing DBSCAN algorithm. This new method incorporates a new extended process based on measurement of distance between clusters. However, the density-based clustering algorithms perform better only in low-dimensional spaces and have poor detection accuracy in high-density spaces. In high dimensional spaces, the data are sparse, making it difficult to differentiate between high-density and low-density regions. Hence DBSCAN cannot be considered a reliable model for detecting zero-day attacks.

According to the definition of zero-day attack, it is a newly developed attack for which the labelled data is not available. Despite this, the models leverage supervised learning for detecting zero-day attacks. They use the labelled data of known attacks, based on the assumption that the feature vector of a zero-day attack may be similar to those of existing attacks. The efficiency of popular ML models like Quadratic Discriminant Analysis (QDA), Decision tree classifier, K-Nearest Neighbor (KNN) classifier, Gaussian Naïve Bayes (NB) classifier for detecting zero-day attacks was evaluated using CICIDS2018 dataset in a supervised manner [26]. To evaluate the models against zero-day cyber-attacks, eight novel attacks were collected from real-time environment. According to the results, the decision tree classifier performed the best in detecting zero-day attacks achieving a True Positive (TP) rate of 96% and False Positive (FP) of 5%.

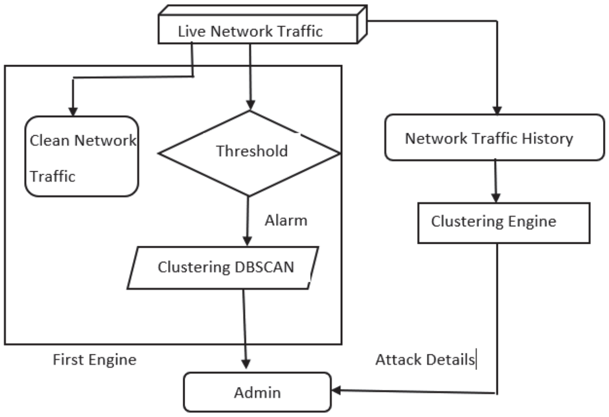

Fig. 2. Architecture of DBSCAN Intrusion Detection System

Therefore, it can be concluded that the detection of zero-day attacks can be accomplished by the use of supervised learning with labeled data of previously known attacks.

The effectiveness of several clustering techniques was investigated by [27] using different approaches including the k- Medoids, k-means, improved k-means and distance-based anomaly detection algorithms. Duong et al. [28] implemented a semi supervised ensemble model using K-means clustering algorithm for zero-day intrusion detection. The primary objective of this method is to train the system to identify normal behaviour, which will then be used to detect zero-day attacks. According to authors' evaluation on NSL KDD dataset, the model achieved 91% accuracy rate in detecting zero-day attacks.

Taher et al. [29] implemented a novel technique based on Artificial Neural Network (ANN) model to detect zero-day attacks. Fig 3 illustrates the architecture of proposed methodology. Their strategy combines feature selection with

ANN to train the model. Two models are created, one with 17 features and the other with 35 features. During the detection phase, the trained model is used to categorize the network traffic either as normal or a zero-day attack. The methodology was tested using the NSL-KDD dataset and compared with the Support Vector Machine (SVM) technique. As per the published results, comparatively better accuracy was attained, outperforming the SVM model with an accuracy of 94.02%. Likewise, Chiba et al. [30] built an IDS based on ANN and included all the performance metrics, including FP Rate, detection rate, and F-Score. This method had the advantage of an improved detection rate and lower FP Rate. One more work presented by [31] utilized a feed forward back propagation ANN technique to detect botnet attacks with an accuracy of 99.6%, outperforming the Naïve Bayes, SVM, and back propagation algorithms. ANN model focuses solely on signature-based attacks, leaving novel attacks undetected, resulting in a high false positive rate. The authors in [29] emphasize on evaluating the efficiency of ANN models using real-time network data. This is because obtaining a benchmark dataset that accurately represents a "true" zero-day attack is one of the potential challenges in detecting zero-day attacks.

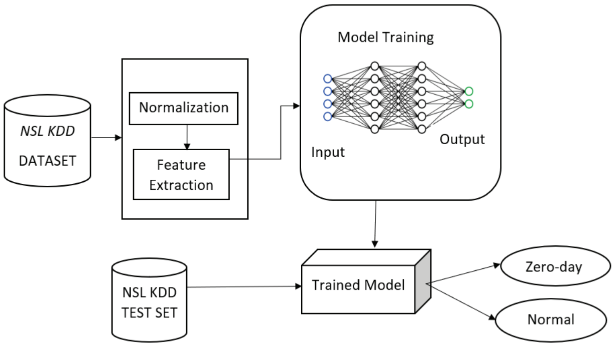

Fig. 3. Architecture of ANN Intrusion Detection System

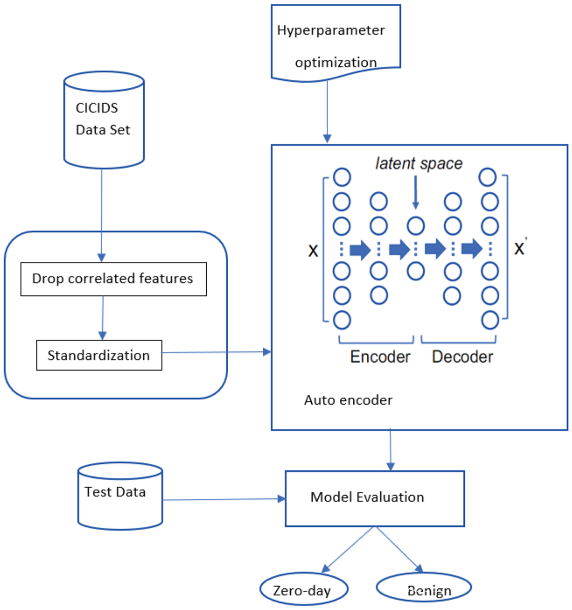

Fig. 4. Architecture of Auto encoder IDS

Auto encoders are a popular technique for reconstruction and their application for detecting zero-day attacks assumes that the "normal" data will be reconstructed with a small reconstruction error, while "anomalous data" will either have a high reconstruction error or cannot be reconstructed at all. Hindy et al. [32] aimed to develop an IDS for detecting zero-day attacks by introducing a novel technique utilizing autoencoder with improved recall rates and reduced false positive rates. The proposed approach was applied to two well-known IDS datasets NSLKDD and CIC-IDS 2017 to examine its effectiveness. Fig 4 illustrates the architecture of the suggested method, which includes a pre-processing stage where features having high correlation are eliminated to reduce model instability. The pre-processing phase selects 18 features, and the proposed auto encoder model is trained using benign samples only. The design of the auto encoder consists of three hidden layers with 15, 9, and 15 neurons each, along with an input layer and output layer, both having 18 neurons. Since an OCSVM has been successful in detecting zero-day intrusions, the results of this framework were compared to those of OCSVM. For the NSL KDD and CICIDS 2017 dataset, the suggested framework obtained detection accuracy of 89-99% and 75-98%, respectively. This proves that AE models are efficient in detecting sophisticated zero-day attacks and boast a high detection accuracy. Additionally, the false positive rates are minimized to a significant level. The auto encoder given in this technique outperforms the most recent implementation found in the current literature [33]. In order to identify zero-day intrusion threats, Zavrak et al. [34] also devised an auto encoder approach based on semi-supervised learning. It's interesting to note that these models perform better at identifying specific attacks. Since the models were trained with benign flow-based data, zero-day attacks that resemble benign activity remain undetected. Hence the models result in a very high false alarm rate. To address this challenge, the authors in [35] applied an AE approach using a technique called as Zero Shot Learning (ZSL). This technique simulates the "zero day" events and learns to distinguish between benign and attack classes by mapping the feature and sematic spaces. The results demonstrate that the lower False Alarm (FA) rate was maintained among all the attacks in the dataset.

Abdalgawad et al. [36] demonstrated that the Bidirectional Generative Adversarial Network (BiGAN) is an effective method for identifying zero-day network attacks. The proposed work applies the DL technique to IOT-23 dataset. The BiGAN architecture is composed of an encoder that transforms a feature space of 27 into a latent representation of 8. The generator (G) creates data from random noise (z) with the same size as the latent representation. The generated data and the actual data are fed to the discriminator. BiGAN is trained on both benign and anomalous samples. The authors tested the model using synthetic, unknown random samples that were created by changing the values of a subset of randomly selected features. The implementation of generative model resulted in detection rates that were higher than those achieved with traditional ML methods. However, the authors did not address the major problem of class imbalance, which requires further network analysis.

TABLE I. RESULTS ON NSL-KDD DATASET

Reference	Approach used	Descriptive Key Points	Performance Metrics	
Alazzam et al. [20]	OCSVM	• Light weight IDS based on OCSVM • Lowers the FA Rate • Improves the detection Rate	Accuracy FP Rate	0.998% 0.0001%
Duong et al. [28]	K-Means Clustering	• Builds normal profile of network traffic using clustering • Detect zero-day attacks using anomaly detection	Accuracy FP Rate	90.2% 10.5%
Zhang et al. [35]	AE	• Illustrate the feasibility of ZSL (zero Shot Learning) for unknown attack detection • ZSL method performs well in identification of unknown attacks	Accuracy FP Rate	88.3% 1.187%
Chiba et al. [30]	ANN	• Selects an optimal set of parameters • Generates all possible combinations of • IDS and compares their performance	Accuracy AUC	90.10% 98.73%
Taher et al. [29]	ANN	• Feature selection selects most relevant • Features • Outperforms SVM • False positive rate is high	Accuracy FP Rate	92% 15.2%

TABLE II. RESULTS ON CICIDS DATASET

Reference	Approach used	Descriptive Key Points	Performance Metrics	
Zavrak et al. [34]	AE, VAE	• Auto encoder based semi supervised learning • AE and VAE employed to identify zero-day attacks • Results demonstrate VAE outperforms AE and OCSVM	AUC	76%
Hindy et al. [32]	AE	• IDS with high recall rates and low false positive rates • Trained using benign Traffic only • Auto encoder has better detection accuracy than OCSVM	Accuracy	89-99%
Zhou and Pezarros [26]	KNN, RF, QDA,	• Five ML models are compared • Novel Attacks collected from Real-time • Decision tree performs the best	TP Rate FP Rate	96% 5%

V. ANALYSIS AND RESULTS

This section compares various ML and DL algorithms used for identifying zero-day attacks on the benchmark datasets NSL-KDD and CICIDS.

From Table I and Table II, it can be inferred that the OCSVM [20] and auto encoder [32] outperform in classifying known and zero-day attacks.

The FA rate in [20] has been reduced to a significant level. To measure the effectiveness of a classification model, the ROC- AUC is a more relevant metric. Area under the Curve (AUC) demonstrates the ability of ML algorithms to accurately distinguish different types of malicious attacks in a network. The Variational Auto-Encoder (VAE), Auto Encoder (AE), and OCSVM obtained AUC scores of 76%, 74%, and 66%, respectively. In [32], the performance comparison between OCSVM and autoencoder was made, and the detection accuracy of the system was found to vary significantly depending on the type of attack. The detection accuracy of attacks that have characteristics similar to normal samples is high, with a range of 92% to 99%. However, the accuracy of attacks that differ from normal samples is low, with a rate of 40%. It has been observed that although One-Class SVMs have good detection rates for zero-day attacks, autoencoders tend to perform better for complex unknown attacks. Both the models have a low False Positive (FP) rate. Furthermore, the authors in [29] attain a good level of accuracy but with a high rate of false positives, as their focus is solely on signature-based attacks, leaving novel attacks undetected. This results in a high FP and FN rates. In [26], authors compare the performance of five ML models for zero-Day attack detection using the CSE-CIC-IDS2018 data set for training.

To address the challenge of scarcity of comprehensive dataset for zero-day attack detection, eight novel attacks were included in the testing set which were collected from the live network. The results showed that the decision tree model was the most efficient, achieving the best TP rate of 96% and lowest FP rate of 5% among all the evaluated models.

Based on the observations in the evaluation results, several challenges and research directions can be highlighted:

- Lack of representative data set: It is essential to have a representative dataset for the accurate detection for ML/DL models. Currently, the datasets used for zero-day detection are not representative of typical zero-day attacks. The detection mechanisms often consider the behaviour of known attacks and zero-day attacks as similar. Hence, developing a new dataset that includes novel attacks will be a great contribution to this area.

- Large variation in detection accuracy: Despite the potential of the proposed detection schemes, none can detect different types of attacks at a uniform detection accuracy. There is a substantial difference in detection accuracy between various types of attacks.

- False Positives (FP) and False Negatives (FN) are prevalent in intrusion detection systems. Despite advancements in the development of IDS for zero-day attack detection, current systems appear to be prone to false negatives and false positives. False Negatives are particularly dangerous because the IDS may confuse the malicious traffic with a legitimate traffic. In the event of a false-negative, there is no warning that the attack has taken place, no alarm is raised, and attacks are frequently denied. Further research is needed to reduce FPs and FNs in order to achieve more effective results.

- Monitoring the traffic and identifying zero-day attacks in real time are challenging tasks. Most of the research conducted so far has focused on detection strategies utilizing pre-existing datasets, making them unsuitable for real-time monitoring. Developing a system for real-time detection of zero-day intrusions would be a significant step forward in this field.

VI. CONCLUSION

Zero-day attack detection continues to be an active research area due to its untapped potential. This paper presents a comprehensive review of ML/DL approaches for detecting zero-day attacks. These methods can identify unknown and previously unseen attacks, making them valuable tools in the fight against zero-day attacks. By utilizing the ML and DL techniques, it is possible to detect patterns and behaviors that indicate the occurrence of a zero-day attack. It should be noted, however, that these methods are not without limitations and challenges. Hence it is essential to continue to enhance and improve these methods to effectively defend against zero-day attacks in the future. For further research, we recommend development of a real-time detection framework with lower false positive and false negative rates. Additionally, creating a representative benchmark would be a significant advancement in improving the efficiency of ML/DL zero-day detection methods.

ACKNOWLEDGEMENT

The authors are thankful to the Artificial Intelligence Research Center at the Department of Computer Science, University of Kashmir for acquiring High-performance NIVIDA Server (DGX A100) under RUSA 2.0 grant and providing access to it for the smooth conduction of research.

REFERENCES

[1] I. H. Sarker, A. S. M. Kayes, S. Badsha, H. Alqahtani, P. Watters, and A. Ng, "Cybersecurity data science: an overview from machine learning perspective," J Big Data, vol. 7, no. 1, 2020, doi: 10.1186/s40537-020-00318-5.

[2] A. S. Ahanger, S. M. Khan, and F. Masoodi, "An Effective Intrusion Detection System using Supervised Machine Learning Techniques," Proceedings - 5th International Conference on Computing Methodologies and Communication, ICCMC 2021, no. May, pp. 1639–1644, 2021, doi: 10.1109/ICCMC51019.2021.9418291.

[3] P. V. Amoli, T. Hamalainen, G. David, M. Zolotukhin, and M. Mirzamohammad, "Unsupervised Network Intrusion Detection Systems for Zero-Day Fast-Spreading Attacks and Botnets." [Online]. Available: https://www.researchgate.net/publication/301549262

[4] L. Bilge and T. Dumitraş, "Before we knew it," in Proceedings of the 2012 ACM conference on Computer and communications security, Oct. 2012, pp. 833–844. doi: 10.1145/2382196.2382284.

[5] "Google, 'Project Zero.'" https://googleprojectzero.blogspot.com /p/about-project-zero.html (accessed Jan. 23, 2023).

[6] C. Tankard, "Advanced Persistent threats and how to monitor and deter them," Network Security, vol. 2011, no. 8, pp. 16–19, 2011, doi: 10.1016/S1353-4858(11)70086-1.

[7] G. Wangen, "The role of malware in reported cyber espionage: A review of the impact and mechanism," Information (Switzerland), vol. 6, no. 2, pp. 183–211, 2015, doi: 10.3390/info6020183.

[8] A. Matrosov, E. Rodionov, D. Harley, and J. Malcho, "Stuxnet under the microscope," ESET LLC (September 2010 …, pp. 1–85, 2010, [Online]. Available: http://www.eset.com/us/resources/white-papers/ Stuxnet_Under_the_Microscope.pdf

[9] A. Ghourabi, T. Abbes, and A. Bouhoula, "Data analyzer based on data mining for Honeypot Router," in ACS/IEEE International Conference on Computer Systems and Applications - AICCSA 2010, May 2010, pp. 1–6. doi: 10.1109/AICCSA.2010.5587041.

[10] N. Kaloudi and J. Li, "The AI-Based Cyber Threat Landscape," ACM Comput Surv, vol. 53, no. 1, pp. 1–34, Jan. 2021, doi: 10.1145/3372823.

[11] H. Hindy, E. Hodo, E. Bayne, A. Seeam, R. Atkinson, and X. Bellekens, "A Taxonomy of Malicious Traffic for Intrusion Detection Systems," in 2018 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA), Jun. 2018, pp. 1–4. doi: 10.1109/CyberSA.2018.8551386.

[12] Y. Hamid, F. A. Shah, and M. Sugumaran, "Wavelet neural network model for network intrusion detection system," International Journal of Information Technology (Singapore), vol. 11, no. 2, pp. 251–263, Jun. 2019, doi: 10.1007/s41870-018-0225-x.

[13] Y. Hamid and M. Sugumaran, "A t-SNE based non linear dimension reduction for network intrusion detection," International Journal of Information Technology (Singapore), vol. 12, no. 1, pp. 125–134, Mar. 2020, doi: 10.1007/s41870-019-00323-9.

[14] G. Kalnoor and S. Gowrishankar, "A model for intrusion detection system using hidden Markov and variational Bayesian model for IoT based wireless sensor network," International Journal of Information Technology (Singapore), vol. 14, no. 4, pp. 2021–2033, Jun. 2022, doi: 10.1007/s41870-021-00748-1.

[15] M. M. Najafabadi, F. Villanustre, T. M. Khoshgoftaar, N. Seliya, R. Wald, and E. Muharemagic, "Deep learning applications and challenges in big data analytics," J Big Data, vol. 2, no. 1, Dec. 2015, doi: 10.1186/s40537-014-0007-7.

[16] I. Bose and R. K. Mahapatra, "Business data mining - A machine learning perspective," Information and Management, vol. 39, no. 3, pp. 211–225, 2001, doi: 10.1016/S0378-7206(01)00091-X.

[17] B. Schölkopf, J. C. Platt, J. Shawe-Taylor, A. J. Smola, and R. C. Williamson, "Estimating the support of a high-dimensional distribution," Neural Comput, vol. 13, no. 7, pp. 1443–1471, 2001, doi: 10.1162/089976601750264965.

[18] M. Daszykowski, B. Walczak, and D. L. Massart, "Looking for natural patterns in data," Chemometrics and Intelligent Laboratory Systems, vol. 56, no. 2, pp. 83–92, May 2001, doi: 10.1016/S0169-7439(01)00111-3.

[19] P. M. Comar, L. Liu, S. Saha, P. N. Tan, and A. Nucci, "Combining supervised and unsupervised learning for zero-day malware detection," in Proceedings - IEEE INFOCOM, 2013, pp. 2022–2030. doi: 10.1109/INFCOM.2013.6567003.

[20] H. Alazzam, A. Sharieh, and K. E. Sabri, "A lightweight intelligent network intrusion detection system using OCSVM and Pigeon inspired optimizer," Applied Intelligence, vol. 52, no. 4, pp. 3527–3544, 2022, doi: 10.1007/s10489-021-02621-x.

[21] G. Pu, L. Wang, J. Shen, and F. Dong, "A hybrid unsupervised clustering-based anomaly detection method," Tsinghua Sci Technol, vol. 26, no. 2, pp. 146–153, 2021, doi: 10.26599/TST.2019.9010051.

[22] I. Mbona and J. H. P. Eloff, "Detecting Zero-Day Intrusion Attacks Using Semi-Supervised Machine Learning Approaches," IEEE

Access, vol. 10, pp. 69822–69838, 2022, doi: 10.1109/ACCESS.2022.3187116.

[23] Y. Yang, K. Zheng, C. Wu, X. Niu, and Y. Yang, “Building an effective intrusion detection system using the modified density peak clustering algorithm and deep belief networks,” Applied Sciences (Switzerland), vol. 9, no. 2, Jan. 2019, doi: 10.3390/app9020238.

[24] K. Jiang, W. Wang, A. Wang, and H. Wu, “Network Intrusion Detection Combined Hybrid Sampling with Deep Hierarchical Network,” IEEE Access, vol. 8, no. 3, pp. 32464–32476, 2020, doi: 10.1109/ACCESS.2020.2973730.

[25] A. S. Alfoudi et al., “Hyper clustering model for dynamic network intrusion detection,” IET Communications, no. August, pp. 1–13, 2022, doi: 10.1049/cmu2.12523.

[26] Q. Zhou and D. Pezaros, “Evaluation of Machine Learning Classifiers for Zero-Day Intrusion Detection -- An Analysis on CIC-AWS-2018 dataset,” May 2019, [Online]. Available: http://arxiv.org/abs/1905.03685

[27] I. Syarif, A. Prugel-Bennett, and G. Wills, “Unsupervised Clustering Approach for Network Anomaly Detection,” Communications in Computer and Information Science, vol. 293 PART 1, pp. 63–77, 2012, doi: 10.1007/978-3-642-30507-8_7.

[28] N. H. Duong and H. Dang Hai, “A semi-supervised model for network traffic anomaly detection,” in 2015 17th International Conference on Advanced Communication Technology (ICACT), Jul. 2015, pp. 70–75. doi: 10.1109/ICACT.2015.7224759.

[29] K. A. Taher, B. Mohammed Yasin Jisan, and M. M. Rahman, “Network intrusion detection using supervised machine learning technique with feature selection,” 1st International Conference on Robotics, Electrical and Signal Processing Techniques, ICREST 2019, pp. 643–646, 2019, doi: 10.1109/ICREST.2019.8644161.

[30] Z. Chiba, N. Abghour, K. Moussaid, A. el Omri, and M. Rida, “A novel architecture combined with optimal parameters for back propagation neural networks applied to anomaly network intrusion detection,” Comput Secur, vol. 75, pp. 36–58, 2018, doi: 10.1016/j.cose.2018.01.023.

[31] A. A. Ahmed, W. A. Jabbar, A. S. Sadiq, and H. Patel, “Deep learning-based classification model for botnet attack detection,” J Ambient Intell Humaniz Comput, vol. 13, no. 7, pp. 3457–3466, 2022, doi: 10.1007/s12652-020-01848-9.

[32] H. Hindy, R. Atkinson, C. Tachtatzis, J. N. Colin, E. Bayne, and X. Bellekens, “Utilising deep learning techniques for effective zero-day attack detection,” Electronics (Switzerland), vol. 9, no. 10, pp. 1–16, 2020, doi: 10.3390/electronics9101684.

[33] M. Gharib, B. Mohammadi, S. H. Dastgerdi, and M. Sabokrou, “AutoIDS: Auto-encoder Based Method for Intrusion Detection System,” pp. 1–9, 2019, [Online]. Available: http://arxiv.org/abs/1911.03306

[34] S. Zavrak and M. Iskefiyeli, “Anomaly-Based Intrusion Detection from Network Flow Features Using Variational Autoencoder,” IEEE Access, vol. 8, pp. 108346–108358, 2020, doi: 10.1109/ACCESS.2020.3001350.

[35] Z. Zhang, Q. Liu, S. Qiu, S. Zhou, and C. Zhang, “Unknown Attack Detection Based on Zero-Shot Learning,” IEEE Access, vol. 8, pp. 193981–193991, 2020, doi: 10.1109/ACCESS.2020.3033494.

[36] 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.