NATURALISTA CAMPANO
ISSN: 1827-7160
Volume 28 Issue 1, 2024

A Survey on Different Methods for Zero-Day Attack Detection in IoT Edge Devices

Mrs. B. Praveena[1*], Dr. A. Devi[2]

[1*]Research Scholar, Department of Computer Science, Dr. SNS Rajalakshmi College of Arts and Science, Coimbatore,
Assistant Professor, Department of Computer Science with Data Analytics, Kongunadu Arts and Science College, Coimbatore.
[2]Research Supervisor & Associate Professor, Department of Computer Applications, Dr. SNS Rajalakshmi College of Arts and Science, Coimbatore.

Email: [1]praveenamtp@gmail.com, [2]devialagarsamy111@gmail.com

Abstract: An innovative idea with many potential uses of IoT, has assimilated into our way of existence. Many functions are made possible by complex networks made up of millions of intelligent devices, including infrastructure control and monitoring as well as communication. Due to limited bandwidth and resources, sophisticated centralized computing in the cloud architecture faced major obstacles as a result of the exponential proliferation of IoT devices and the massive data traffic they created at the network edge. With the emergence in the referred to as EC-assist IoT, Edge Computing (EC) is being recognized as a cutting-edge strategy that bridges the gap created by consumer's insufficient ability to access data to be processed and saved. The improved Quality of Service (also known as QoS) and distinctive aspects of this paradigm make data security more dangerous. Thus, this vulnerability makes a variety of assaults conceivable. Due to their explicit reliance on attack signature repositories, use of out-of-date datasets, or failure to take into account zero-day (unknown) assaults during model development, training, or testing, many of the newly presented solutions lack a comprehensive IDS strategy. If these aspects are ignored, the suggested IDS is not as reliable or useful in real-time situations. However, identifying zero-day attacks remains a difficult topic even with the numerous solutions that have been put out over the years. This article presents a thorough review of strategies for identifying zero-day attacks, comparing and contrasting their benefits and drawbacks. Potential research areas for the future have been addressed, along with the challenges that researchers have encountered in the past while trying to detect zero-day attacks.

Keywords: Internet of Things, Edge computing, Zero-day attack detection, Data traffic, Training, Testing and Review.

1. Introduction

The term ‘internet of things’ describes a group of entities that link together over the Internet to exchange and store data pertinent to a certain service or application. These entities may include smart gadgets, actuators, sensor technology, and any other devices with electronics incorporated [1,2]. IoT is able to facilitate and accelerate the introduction of new, creative services and applications due to the rapid advancement of information technology [3, 4]. IoT smart devices may also be used in a variety of complicated situations since they are always being updated with increasingly powerful processing, sensing, and computation capabilities. As per an analysis published by the International Data Corporation (IDC). By 2020, it is anticipated that there will be more than 200 billion IoT-capable smart devices and sensors worldwide, of which 30 billion will be Internet-connected. Examples of these include wearable technology, smart home appliances, smartphones and tablets, and more [5]. Figure 1 depicts common Internet of Things services and applications encountered in a variety of important industries.

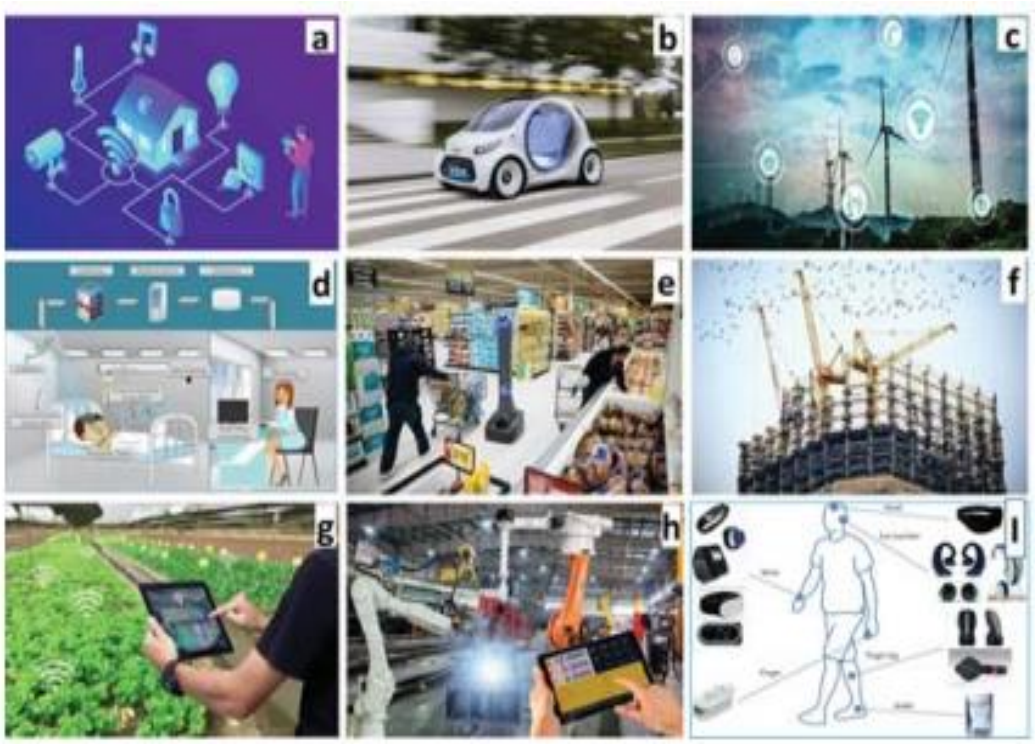

Figure 1: IoT applications include (a) smart homes, (b) smart cars, (c) optimization of energy, (d) wellness tracking, (e)FSC, (f) supervision of construction, (g) monitoring the environment, (h) monitoring production, and (i) gadgets that are wearable.

Based on research from Cisco Global Cloud Index (GCI) [6,7], it is anticipated that by 2020, the quantity of data generated and collected by these devices/sensors from the surrounding environment would surpass 500 Zettabytes (ZB). As part of the traditional cloud computing paradigm, each of such information will be routed to strong central servers situated in the cloud for extra processing, compute, and storage. The data has to be put back into the original devices after processing. For the following reasons, a method of this kind stresses the core network excessively and offers a subpar quality of service (QoS): 1) Underutilization of bandwidth as well as assets incurs additional expenses for data transmission; 2) Data size increases significantly impair network performance; 3) Networking communication and handling traffic are made more difficult by the quick growth of IoT devices; 4) Dependent on time IoT apps and services, such as smart towns, smart electricity grids, and intelligent transportation, may encounter unavoidable delays [8, 9].

Developing an IoT system with edge computing support might provide a solution to all of these problems and limitations. Through the integration of the edge computing (EC) concept using the current cloud computing infrastructure, this solution effectively resolves the previously listed difficulties. In order to do this, nodes and/or servers are positioned closer to network edges and data sources. Improved network security, reduced latency, and support for IoT services and apps will all result from doing this. In subsequent years, the Internet of Things (IoT) framework with EC assist, IDC predicts that the network edge will handle 40% of edge-originated data processing and storage. Smart building and health monitoring are only two of the areas where EC-assisted IoT systems handle and control enormous volumes of data related to critical and sensitive applications. Because of this, it has been a target for assaults from the government, hackers, and cybercriminals.

These "zero-day" assaults take use of undiscovered flaws to evade detection by cyber security monitoring systems. Thus, extensive studies as well as practical measures are required to counteract zero-day attacks within EC-supported IoT networks. With a consequence, new EC-compatible IoT services and applications will be able to create safe connected gadgets and sensors. This article describes the many methods to identify zero-day assaults along with their advantages and disadvantages. Researchers have talked about the difficulties they have had in the past while attempting to identify zero-day attacks and the potential directions they now have to pursue.

2. Litrature review

Sharma et al [2017] [10] offered a consensus-building architecture that reduces the danger of zero-day assaults on IoT networks. The suggested system leverages Internet of Things (IoT) gadget situational behavior, a notification protocol, and essential data exchange protocol to enable trustworthy communication while preventing assaults. According upon the numerical analysis, the proposed method may identify and eliminate zero-day risks from connected devices while maintaining network functionality.

Ngo and Nguyen[2022][11] introduced a reliable IoT botnet detection model that uses system call feature-based adversarial learning in conjunction with supervised learning to identify zero-day attacks. Dataset experiments show that it is possible to identify both zero-day attacks and Iot botnets. Using a somewhat well-known dataset, the suggested model achieves 88,94% accuracy, significantly improving its capacity to identify novel IoT botnet variations.

Kumar and Sinha [2021][12] formulated a novel, clever, and robust hacking monitoring model focused upon the heavy-hitter idea and graph technique to identify zero-day attacks with the aim address aforementioned issues. There are two phases to the desired task: evaluation and signature creation. This model uses the produced signatures to assess performance throughout the training phase. The suggested zero-day attack detection strategy surpasses existing techniques based on real-time attack data, with multi-class classification accuracy of 90.35% and binary classification accuracy of 91.33%. It is promising that this model performs 91.62% well in binary-class classification when compared to the benchmark data set CICIDS18. Consequently, the suggested method for sensing zero-day attacks functions effectively.

Lobato et al [2018][13] projected training an adaptive detection of threats architecture using a real-time detection model.The following are the suggested architecture's main contributions: i) collect data about the behavior of attackers and zero-day attacks using networked honeypots; ii) use stream processing technology to process data in real-time while maintaining an elevated throughput; iii) evaluate our detection plans on two real data sets, one compared to a major Brazilian network of things user and a different created in our lab; iv) create and design adaptive detection schemes that make use of online as well as trained, managed methods that resemble the actions of genuine users and refresh their requirements in real-time in response to zero-day threats.The performance experiments show that the proposed architecture achieves over 90% classification accuracy with a favorable trade-off between threat detection and false positive rates, even in the face of real-world behavioral changes and zero-day threats.

El-Sayed et al [2021][14] attempted to deliver novel automatic learning as well as deep neural network methodologies for identifying unknown threats in IoT photos, often known as anomaly detection. In order to pick the supervised machine or deep learning algorithm that would produce the best results, PCAP data are first represented as RGB pictures in order to facilitate better analysis. The purpose of this work is to pick the best supervised learning algorithm by testing and comparing seven of them with varying complexity levels. The sevens may be divided into two categories: conventional classifiers, The k-n Neighbours, SVM and Logistic Regression (LR) are among the CNN classifiers, as are 2-Layer and 4-Layer CNN, and VGG16. Based on MobileNetv2 characteristics, testing results indicated that the support vector machine classifier performed at a maximum level of 94%. Its quick and consistent training with less resources than both of the models might be the reason for this.

Seraphim and Poovammal [2022][15] offered machine learning methods for faster, more accurate detection of zero-day vulnerabilities with a lower false alarm rate. Zero-day assaults are included in the CICIDS dataset, which is streamed. Performance parameters including reliability, detection time, and utilization of memory are utilized to evaluate the system, it is built using methodologies such as random forest, random tree, Bayes's method, and Hoeffding tree. It was discovered that the Hoeffding tree requires 5.94 seconds and 0.08 MB of memory to provide an accuracy of 99.97%.

Roshan and Zafar [2021][16] suggested an intrusion detection system with the ability to identify unknown and zero-day cyberattacks. created a clever intrusion detection model using the autoencoder. The suggested approach is innovative in that it demonstrates the critical role threshold plays in the recall-efficient detection of zero-day cyberattacks. Furthermore, establishing a single criterion for a certain kind of assault might not be sufficient for other, less obvious cyberattacks. To demonstrate the importance of each assault, we have thus assessed accuracy independently for each one using various criteria. The most recent dataset, CICIDS2017, has been utilized for assessment. Regarding accuracy or recall, the model performs well both on an individual and aggregate level. On the CICIDS2017 dataset, the optimized version of the autoencoder (OPT_AE) has an overall accuracy of 99.29%.

Hu et al [2019][17] offered a structured framework that made it possible to create adaptive cyber defenses against zero-day threats based on reinforcement learning. Control theory and machine learning ideas are used in reinforcement learning. It's amazing how reward learning might eliminate the need for defenses to be aware of crucial details about attacks that are zero-day, such as the goals and spaces of vulnerability sites. Obtaining this

knowledge in advance is extremely hard, if not not possible, in order to ensure protection. Learning through reinforcement schemes defeat the following kinds of attacks: strategic attacks (in which the attacker and defender play a non-cooperative game), non-strategic random attacks (in which the attacker selects what it does according to a specified probability distribution), and Bayesian attack graphs (in which the attacker compromises network machines through the use of various known or zero-day vulnerabilities).

Priya and Annie Uthra [2021][18] presented a novel Variational Auto Encoder (VAE) model for reconnaissance of zero-day attacks using DL. Creating a novel IDS model with a high and low false-negative detection rate both are the goal of this project. Preparing unprocessed data for the DL-VAE model to understand requires pre-processing. The Variational Auto Encoder model is used to search the networking data for zero-day vulnerabilities following the entry of the pre-processed data. The efficacy of the DL-VAE model has been shown in several research, and the results are examined from various angles. Based on the gathered simulation data, the DL-VAE model was determined to have improved with a kappa of 0.973, F-score of 0.982, accuracy of 0.989, specificity of 0.977, and sensitivity of 0.985.

Kim et al [2018][19] developed the state-of-the-art technique known as the transferred deep-convolutional generative adversarial network (tDCGAN), which can differentiate between genuine and bogus malware. Although each vary because they possess different attributes, the data produced by distribution at random have numerous similarities to real data. Utilizing both true and false data generated by the tDCGAN—which is based around a deep autoencoder (DAE) that locates pertinent characteristics and stabilizes the GAN training—the detector learns about numerous aspects of malware.To enable the GAN to be gradually trained before it is ever given instructions, the DAE collects generic data, detects malware traits, and transmits this information to the GAN generator.The trained discriminator gives the detector the ability to identify malware characteristics through the procedure of transfer learning. Using an average rate of classification of 95.74%, we show that tDCGAN performs better than other models in terms of learning stability. It performs better than the rest when it comes to defense against simulated zero-day attacks.

Sameera and Shashi[2020][20] Marginal probability distributions across the domains and different feature spaces were addressed by applying the TL manifold alignment approach, which combines the initial and final domains into a single latent space. Using the cluster correspondence processes, a way is given to generate target soft labels on the modified space in order to make up for the absence of labeled target instances. Furthermore, DNN offers a framework for identifying zero-day threats. Through a series of trials, the authors assessed the effectiveness of the proposed structure using the data from the NSL-KDD and CIDD datasets. Experiments clearly demonstrate that the suggested method might identify zero- day assaults on unknown data.

Bu and Cho [2021][21] Using a deep Convolutional Auto Encoder (CAE) is advised in order to preserve character-level URL data and defend against zero-day attacks. Investigating 222,541 Websites across three actual-world data sets in detail revealed that the most advanced deep-learning algorithms were operating at peak performance. The receiver-operating characteristic (ROC) curve analysis and tenfold cross-validation demonstrate that the suggested method outperforms the most recent deep model by 3.98%.

Li, et al [2023][22] enabled the release of RETSINA, a cutting-edge meta-learning architecture that uses a small amount of training data to help a company identify zero-day Web attacks across several domains. More precisely, it applies meta-learning to effectively train detection models by utilizing cross-domain information transfer, or the connection across requests made via HTTP from several domains. Furthermore, we offer an adaptive preprocessing module and a multi-domain representation approach to capture cross-domain semantic correlations for cross-domain model training, to enable cross-domain semantic analysis of Web requests more easily. Analyze 4 real-world datasets with 293 million search across various subjects. The experimental results show that, despite having little training data, RETSINA performs better than current unsupervised Web detection of attacks methods. To reach detection performance comparable to current methods, that develop distinct models for different domains needing an entire day of data, RETSINA, for example, requires only a few minutes of data to train. In an Internet corporation, we also carry out real-world implementation. Within a month, RETSINA records 126 requests per day for zero-day attacks on one domain, and 218 requests per day on another.

Sara and Hossain [2023][23] ML and DL based models were trained to discriminate between authentic and fraudulent behavior using both single and multiple factors extracted from the static properties of mobile applications. We evaluate the performance of those models using a range of datasets (DREBIN), which encompass real-world Android application features together with samples of zero-day and benign malware. We achieved an F1 Score of 96% in the case of zero-day malware using the multi-view model (DL Model). Thus, this study might help lower the probability of unknown malware.

Soltani et al [2023][24] recommended managing emerging threats with IDSes by utilizing a deep learning-based strategy. Because it uses deep novelty-based classifiers in conjunction with classic clustering based on a particular layer of deep structures, this technology is unique to the security sector. Furthermore, DOC++ an improved

version of DOC is introduced as a deep novelty-based classifier. To further enhance the capacity of deep learning algorithms to identify content-based assaults, we additionally utilize the Deep Intrusion Detection (DID) framework during the preprocessing stage. The CIC-IDS2017 and CSE-CIC-IDS2018 datasets are used to evaluate the novelty classifier of the framework using four distinct approaches: DOC, DOC++, OpenMax, and AutoSVM. Our findings suggest that the best method for developing the open set recognition module is DOC++. The clustering and after training phases' completeness and homogeneity show that this model is robust enough for the automated labeling and updated step.

Table 1. Comparsion of existing zero attack detection methods

Author name	Methods	Merits	Demerits
Sharma et al [2017]	Consensus framework	Produces better detection accuracy	Time consuming nature
Ngo and Nguyen[2022]	Adversarial learning	Achieves 94% accuracy	Increases the computational complexity
Kumar and Sinha [2021]	Heavy-hitter and graph technique	obtaining a 91.62% outcome for this model's binary-class categorization	Need to identify ZA kinds whose actions are independent of current assaults in order to increase the resilience of our method.
Lobato et al [2018]	Online Support Vector Machine	Over 90% categorization accuracy is attained.	Does not perform well with high volume data
El-Sayed et al [2021] .	CNN classifiers include Support Vector Machine, 4-Layer CNN, Two-Layer CNN, K-Nearest Neighbors, and Logistic Regression.	Reached 94%	It's necessary to investigate more sophisticated optimization strategies, such feature selection.
Seraphim and Poovammal[2022]	Naïve Bayes, random trees, random forests, and hoeffding	Gives the accuracy of 99.97%	Does not focused on multi-class classification
Roshan and Zafar [2021]	Auto encoder	Obtains the accuracy 99.29 %	Very expensive
Hu et al [2019]	Reinforcement learning	Robust and efficient	It requires a lot of data
Priya and Annie Uthra [2021]	Variational Auto Encoder (VAE)	Feasible and reduces the time complexity	Does not implemented for other attack detection
Kim et al [2018]	Generative adversarial network with deep convolutional transfer	strongest defense against zero-day attacks in comparison to other	Increases the false positive rate
Sameera and Shashi[2020]	DNN	Could successfully detect zero-day attacks	Need to extend this work for specific attack type detection
Bu and Cho[2021]	Deep Convolutional Auto Encoder	Compared to the most recent deep model,	To enhance the detection performance, it is necessary to take into

		sensitivity increased by 3.98%.	account the extra exploitation of URL characteristics.
Li, et al [2023]	RETSINA	Achieve comparable detection performance	Increases the error rate
Sara and Hossain [2023]	SVM and CNN	Achieved f1 Score 96%	Does not implemented on real time data
Soltani et al [2023]	DOC, DOC++, OpenMax, and AutoSVM	Improves the true positive rate	Time complexity is very high

3. Inferences from the existing work

Prior research employed several techniques for detecting zero-day attacks, which are capable of handling substantial amounts of network traffic data and safeguarding communication networks from cyber threats. Nonetheless, scalability in current IoT networks is rapidly increasing. As a result, in practical use scenarios, it could be challenging to transfer large amounts of dispersed IoT network traffic data to a distant central cloud server for processing owing to network limitations. Additionally, certain works that employ the Centralized Deep Learning approach demand a large amount of memory space for data storage, a longer training period, and a significant communication overhead. Moreover, the locations of cloud data centers are frequently remote from the IoT device deployment sites. The botnet detection system based on Centralized Deep Learning has substantial latency as a result.

4. Solution

Future work in this area will mostly focus on enhancing algorithms for zero-day threats detection and classification. The initial feature selection process will employ the swarm intelligence technique. It significantly improves the model's accuracy and lengthens the training period required to create the model. The identification of zero-day attacks will be carried out using an enhanced deep learning technique.

5. Conclusion and future work

Zero-day attacks provide new security issues because to the Internet of Things' (IoT) fast rise in cyberattacks. Intrusion-detection systems (IDS) are often trained on targeted assaults to safeguard Internet of Things applications; However, zero-day attacks—attacks that an IDS has not yet discovered—continue to present challenges and raise concerns over the safety and confidentiality of user data within such applications. The present paper provided a review of the research on zero-day attack detection. After examining such approaches, it is determined that deep learning techniques are superior at identifying zero-day botnet attacks, and future study may concentrate on this area.

6. References

1. Saharkhizan, M., Azmoodeh, A., Dehghantanha, A., Choo, K.K.R. and Parizi, R.M., 2020. An ensemble of deep recurrent neural networks for detecting IoT cyber attacks using network traffic. IEEE Internet of Things Journal, 7(9), pp.8852-8859.
2. Huong, T.T., Bac, T.P., Long, D.M., Thang, B.D., Binh, N.T., Luong, T.D. and Phuc, T.K., 2021. Lockedge: Low-complexity cyberattack detection in iot edge computing. IEEE Access, 9, pp.29696-29710.
3. Eskandari, M., Janjua, Z.H., Vecchio, M. and Antonelli, F., 2020. Passban IDS: An intelligent anomaly-based intrusion detection system for IoT edge devices. IEEE Internet of Things Journal, 7(8), pp.6882-6897.
4. Diro, A.A. and Chilamkurti, N., 2018. Distributed attack detection scheme using deep learning approach for Internet of Things. Future Generation Computer Systems, 82, pp.761-768.

5. Becker, E., Gupta, M. and Aryal, K., 2023, July. Using Machine Learning for Detection and Classification of Cyber Attacks in Edge IoT. In 2023 IEEE International Conference on Edge Computing and Communications (EDGE) (pp. 400-410). IEEE.
6. Blaise, A., Bouet, M., Conan, V. and Secci, S., 2020. Detection of zero-day attacks: An unsupervised port-based approach. Computer Networks, 180, p.107391.
7. Sriram, S., Vinayakumar, R., Alazab, M. and Soman, K.P., 2020, July. Network flow based IoT botnet attack detection using deep learning. In IEEE INFOCOM 2020-IEEE conference on computer communications workshops (INFOCOM WKSHPS) (pp. 189-194). IEEE.
8. Alshamkhany, M., Alshamkhany, W., Mansour, M., Khan, M., Dhou, S. and Aloul, F., 2020, November. Botnet attack detection using machine learning. In 2020 14th International Conference on Innovations in Information Technology (IIT) (pp. 203-208). IEEE.
9. Ahmed, A.A., Jabbar, W.A., Sadiq, A.S. and Patel, H., 2020. Deep learning-based classification model for botnet attack detection. Journal of Ambient Intelligence and Humanized Computing, pp.1-10.
10. Sharma, V., Lee, K., Kwon, S., Kim, J., Park, H., Yim, K. and Lee, S.Y., 2017. A consensus framework for reliability and mitigation of zero-day attacks in IoT. Security and Communication Networks, 2017.
11. Ngo, Q.D. and Nguyen, Q.H., 2022, April. A Reinforcement Learning-Based Approach for Detection Zero-Day Malware Attacks on IoT System. In Computer Science On-line Conference (pp. 381-394). Cham: Springer International Publishing.
12. Kumar, V. and Sinha, D., 2021. A robust intelligent zero-day cyber-attack detection technique. Complex & Intelligent Systems, 7(5), pp.2211-2234.
13. Lobato, A.G.P., Lopez, M.A., Sanz, I.J., Cardenas, A.A., Duarte, O.C.M. and Pujolle, G., 2018, May. An adaptive real-time architecture for zero-day threat detection. In 2018 IEEE international conference on communications (ICC) (pp. 1-6). IEEE.
14. El-Sayed, R., El-Ghamry, A., Gaber, T. and Hassanien, A.E., 2021, December. Zero-day malware classification using deep features with support vector machines. In 2021 Tenth International Conference on Intelligent Computing and Information Systems (ICICIS) (pp. 311-317). IEEE.
15. Seraphim, B.I. and Poovammal, E., 2022. Zero-Day Attack Detection Analysis in Streaming Data Using Supervised Learning Techniques. In Intelligent Systems and Sustainable Computing: Proceedings of ICISSC 2021 (pp. 517-530). Singapore: Springer Nature Singapore.
16. Roshan, K. and Zafar, A., 2021, October. An Optimized Auto-Encoder based Approach for Detecting Zero-Day Cyber-Attacks in Computer Network. In 2021 5th International Conference on Information Systems and Computer Networks (ISCON) (pp. 1-6). IEEE.
17. Anand, P., Singh, Y. and Selwal, A., 2022. Learning-based techniques for assessing zero-day attacks and vulnerabilities in IoT. In Recent Innovations in Computing: Proceedings of ICRIC 2021, Volume 1 (pp. 497-504). Singapore: Springer Singapore.
18. Hu, Z., Chen, P., Zhu, M. and Liu, P., 2019. Reinforcement learning for adaptive cyber defense against zero-day attacks. Adversarial and Uncertain Reasoning for Adaptive Cyber Defense: Control-and Game-Theoretic Approaches to Cyber Security, pp.54-93.
19. Priya, S. and Annie Uthra, R., 2021. An Effective Deep Learning-Based Variational Autoencoder for Zero-Day Attack Detection Model. In Inventive Systems and Control: Proceedings of ICISC 2021 (pp. 205-212). Springer Singapore.
20. Kim, J.Y., Bu, S.J. and Cho, S.B., 2018. Zero-day malware detection using transferred generative adversarial networks based on deep auto encoders. Information Sciences, 460, pp.83-102.
21. Sameera, N. and Shashi, M., 2020. Deep transductive transfer learning framework for zero-day attack detection. ICT Express, 6(4), pp.361-367.
22. Bu, S.J. and Cho, S.B., 2021. Deep character-level anomaly detection based on a convolutional autoencoder for zero-day phishing URL detection. Electronics, 10(12), p.1492.
23. Li, P., Wang, Y., Li, Q., Liu, Z., Xu, K., Ren, J., Liu, Z. and Lin, R., 2023, November. Learning from Limited Heterogeneous Training Data: Meta-Learning for Unsupervised Zero-Day Web Attack Detection across Web Domains. In Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security (pp. 1020-1034).
24. Sara, J.J. and Hossain, S., 2023, September. Static Analysis Based Malware Detection for Zero-Day Attacks in Android Applications. In 2023 International Conference on Information and Communication Technology for Sustainable Development (ICICT4SD) (pp. 169-173). IEEE.
25. Soltani, M., Ousat, B., Siavoshani, M.J. and Jahangir, A.H., 2023. An adaptable deep learning-based Intrusion Detection System to zero-day attacks. Journal of Information Security and Applications, 76, p.103516.