e-ISSN:2582-7219

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

Volume 7, Issue 13, April 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.521

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| | Monthly Peer Reviewed & Refereed Journal |

|| Volume 7, Issue 13, April 2024 ||

International Conference on Intelligent Computing & Information Technology (ICIT-24)

Organized by

Erode Sengunthar Engineering College, Erode, Tamilnadu, India

A Survey on Zero-Shot Learning Approach for Zero-Day Attack Detection on IoT Devices

N.Sakthipriya[1], V.Govindasamy [2], M.Haripriya[3], R.Rajesh[4], R.Ragul[5]

Department of Information Technology, Puducherry Technological University, Puducherry, India[1,2,3,4]

ABSTRACT: The security environment is facing unprecedented problems as a result of the rapid growth of IoT devices, primarily because of the large attack surface they provide. Even with more attention being paid to IoT device security, it is still difficult to identify unexpected threats. Conventional techniques such as heuristic methods and signature-based detection are unable to counter the wide range of assaults, including zero-day vulnerabilities. NIDS are essential for protecting network infrastructures, but attackers take advantage of holes in IoT devices with limited resources, opening up new channels for cyberattacks. This paper explores how intrusion detection methods and Internet of Things assaults are changing, emphasizing the growing danger of unidentified threats and the new strategy of zero-shot learning in identification. Hackers find it profitable to target Internet of Things (IoT) devices, which include household appliances and personal electronics, as they grow increasingly linked. Botnet attacks are particularly noteworthy among these dangers due to their advanced strategies for infiltrating IoT devices. Numerous intrusion detection methods, have been researched to strengthen IoT security and have demonstrated promise in detecting botnet activity. The effectiveness of zero-shot learning in identifying hitherto undetected attack patterns is evaluated in this study, providing insights into the changing IoT security environment and the steps that must be taken to counter new threats.

KEYWORDS: Internet of Things, Generative Adversarial Network, Zer-Shot Learning, Botnet, Zero-day attack

I. INTRODUCTION

The IoT network comprises interconnected smart devices, including sensors, household appliances, phones, vehicles, and computers, utilizing the global Internet. This network is progressively ingrained in our daily lives, offering diverse applications like smart home systems, efficient energy grids, advanced farming techniques, modern urban infrastructure, intelligent transportation solutions and many more [1]. An Internet of Things application is composed of three layers: the perception layer, the network layer, and the application layer. Sensing and obtaining environmental data, followed by transmission to the network layer, are the responsibilities of the perception layer. For example, security cameras are sensors that identify abnormalities like movement. The perception layer and the cloud are connected through the network/transport layer. It includes communication technologies including Wi-Fi, 5G, MQTT, Zigbee, and other internet protocols. For example, a security camera may use the home router and Wi-Fi to transmit a movement sensing signal to the main server. The application layer uses the data it gets from the network layer to perform user activities and provide services. For example, the cloud service may notify a homeowner when movement is detected from one of their surveillance cameras through a push notification to their mobile device [2]- [3].

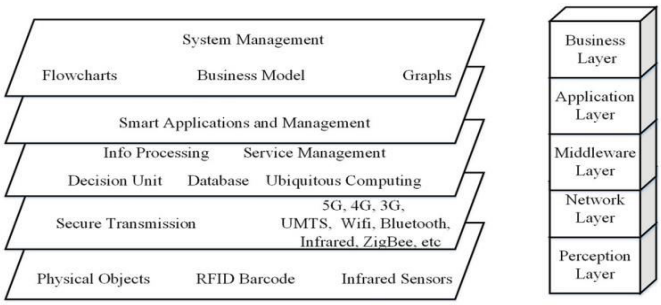

Fig. 1. OverallArchitecture of IoT

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| | Monthly Peer Reviewed & Refereed Journal |

|| Volume 7, Issue 13, April 2024 ||

International Conference on Intelligent Computing & Information Technology (ICIT-24)

Organized by

Erode Sengunthar Engineering College, Erode, Tamilnadu, India

IoT has faced security issues from its conception and continues to confront obstacles in this area across all architectural layers [4]. In their analysis of the many forms of assaults in Smart Health Systems, Butt et al. [5] identified the following: replay attacks, router attacks, select forwarding (SF) attacks, fingerprint and timing-based snooping (FATS), denial of service attacks (DoS), and sensor attacks. In general, threats like malicious code injection, eavesdropping, and interference might affect the perception layer [3, [6], [12]. In a similar vein, attacks such as spoofing, denial of service, man-in-the-middle, and routing information are common at the network layer [6]. Finally, malware, worms, and phishing attempts can infect the application layer [12]. These attacks were divided into four categories by Andrea et al. [7]: software, network, physical, and encryption. A physical assault occurs when the perpetrator is physically near the system, while a software attack occurs when a device has a defect that permits unauthorized access, potentially destroying the system. Network attacks occur when someone obtains entry to the IoT network with the intention of manipulating a device and causing harm, whereas encryption attacks occur when IoT authentication is compromised.

II. VULNERABILITY IN IOT NETWORKS

An IoT intrusion is any unauthorized activity or action that disrupts the IoT ecosystem. Put another way, an intrusion is any attack that jeopardizes the confidentiality, availability, or integrity of data. This would include an attack that stops authorized users from using computer services, for example. To safeguard system security, known as an intrusion detection framework, keeps an eye out for malicious activities on computer systems. Finding harmful network activity and illegal computer use is the primary objective of an intrusion detection system. Conventional firewalls are unable to do this duty. In doing so, computer systems are considerably strengthened against hostile acts that could compromise their confidentiality, availability, or integrity. IoT system security is a major concern due to the growing number of offerings and clients within IoT networks. The incorporation of IoT technologies into smart settings increases the effectiveness of smart products. However, vulnerabilities in IoT security are particularly dangerous in critical smart environments utilized in industries such as industry and health. Weak security measures in IoT-based intelligent settings expose applications and services to vulnerabilities. Secrecy, integrity, and availability are critical security concepts for apps and services that operate in Internet of Things (IoT)-based intelligent environments. Security issues in Internet of Things networks hence need more study focus in order to be resolved [9], [10]. For instance, concerns about security and privacy surface at every level of the Internet of Things architecture for Internet-based smart homes [11].

By utilizing a wide range of devices, including CPUs, sensors, and many other technologies, Internet of Things technology has successfully achieved its goal of exchanging data and establishing connections with other networks. Nevertheless, there may be a lack of security in the shared data due to the large number of linked devices, raising security issues. IoT security is about protecting the data that is transferred between various networks using IoT devices and IoT technology. By connecting to the internet, these gadgets create relationships with other people, creating security holes that hackers can use to obtain data. Inadequately secured data causes a great deal of worry and serious threats for many sectors and people, possibly leading to a large loss of data from their systems. [15].

III. OVERVIEW OF ZERO SHOT LEARNING AND GENERATIVE ADVERSARIAL NETWORK

A method known as "zero-shot learning" helps a model identify and categories items, patterns, or data points that it has never seen before. Zero-shot learning enables a model to generalize from known attack patterns to identify new and previously undetected attack types, which can be helpful in the context of detecting unexpected attacks. The model gains an understanding of the fundamental traits of assaults through training on a variety of known attacks. This increases the model's ability to identify patterns or anomalies linked to novel, unidentified attacks. By doing this, the system may be better able to adjust to changing threats without needing to be explicitly trained on every scenario of an attack. Zero-shot learning combined with Generative Adversarial Networks (GANs) can produce an effective framework for identifying unknown assaults.

Ian Goodfellow et al. [31] created Generative Adversarial Networks (GANs), a major development in unsupervised machine learning. Fundamentally, GANs are made up of two competing neural network models, known as a Discriminator (D) and a Generator (G), which are trained concurrently via a dynamic adversarial process. This creative framework makes it possible to produce incredibly realistic data. The main purpose of the Generator is to create synthetic data instances that closely resemble real data by mapping latent space vectors, or random noise, to the data

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| | Monthly Peer Reviewed & Refereed Journal |

|| Volume 7, Issue 13, April 2024 ||

International Conference on Intelligent Computing & Information Technology (ICIT-24)

Organized by

Erode Sengunthar Engineering College, Erode, Tamilnadu, India

space. At first, it is simple to tell G's outputs apart from the real data. But as training goes on, G gets better, producing data that is more realistic. In concert, the Discriminator's job is to assess data instances and decide which ones are real (from the dataset) and which ones are fake (made by G). With time, D's performance improves and he gets better at spotting G's lies. The following are steps in the GAN training process: Every iteration begins with the discriminator (D) being trained on a mixture of genuine and fake data. Maximizing D's capacity to accurately classify each instance as true or fraudulent is the goal. Generator (G) is then trained to trick D. This is accomplished by leading G to generate data that D is more likely to mistakenly identify as real by changing G's weights in response to D's input.

The accuracy with which GANs synthesize data from different distributions highlights the generalizability of the GANs methodology as well as its capacity to understand subtleties in data distributions. Greater precision can be achieved in addressing the problem of distributional imbalance between abnormal and normal data samples by utilizing the generating capabilities of GANs. Because there is inadequate training data on the anomaly distribution, model could result from an imbalanced ratio of abnormalities compared to standard data that is biased towards the greater class of normal data [19]. By generating real anomalous data, GANs help address data imbalance by giving the model more information to work with.

When anomalies happen infrequently or data generation is unaffordable, synthetic data generation works well. GANs are helpful for anomaly detection in IoT networks because routine occurrences generate more data than unexpected activities. However, it takes a lot of effort and money to generate different types of anomalous data in different ways. More devices are vulnerable to intrusion as a result of increased Internet usage, which calls for the creation of more advanced IoT device defense technologies and defined security procedures to ensure their safety. Numerous methods and resources are available for identifying anomalies in networks.

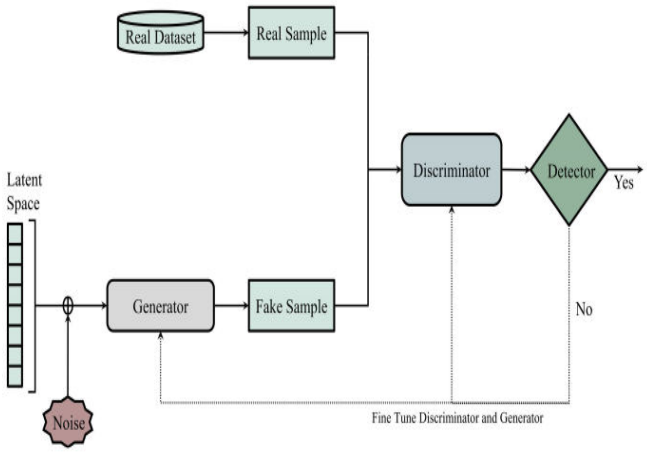

Fig. 2. General Architecture of GAN according to [26]

IV. DISCUSSION ON KEY CHALLENGES

In 2023, D. Y. Demirel et al. [20] addresses imbalanced data and false positive rates in web application security, proposing ZSL-CNN, a novel Zero-Shot Learning method utilizing Convolutional Neural Networks. Evaluation involves three datasets, including one from Yapı Kredi Teknoloji. Results show ZSL-CNN achieves a 99.29% true positive rate, surpassing Isolation Forest, Auto-encoder, De-noising Auto-encoder with Dropout, and One-Class SVM. Mohamed et al. propose a superior de-noising auto-encoder with dropout for network malware detection. One-Class SVM serves as a benchmark for anomaly detection in web-based attacks. The importance of CNN for web traffic feature extraction is emphasized for classification. While ZSL-CNN addresses imbalanced web security data, its generalizability is limited to specific datasets. Evaluation primarily compares it to traditional methods, neglecting hybrid approaches or deployment challenges. Further, while CNN's feature extraction importance is highlighted, interpretability and practical false positive impacts remain underexplored.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| | Monthly Peer Reviewed & Refereed Journal |

|| Volume 7, Issue 13, April 2024 ||

International Conference on Intelligent Computing & Information Technology (ICIT-24)

Organized by

Erode Sengunthar Engineering College, Erode, Tamilnadu, India

A unique zero-shot learning technique is presented by Sarhan et al. [21] in 2023 to assess the effectiveness of using NIDS with machine learning for the detection of zero-day attacks. During the characteristic learning phase, models translate the features of network data into semantic attributes, which enables them to distinguish among recognized assaults and benign behavior. Associations between known and zero-day attacks are built for harmful detection at the inference step. Zero-day Detection Rate (Z-DR), a novel metric, is used to assess how well the model detects unknown attacks. The system is tested using two algorithms for machine learning and NIDS datasets. The findings indicate that ML-based NIDSs face challenges from certain zero-day assault groups. Attacks with a low Z-DR have a higher Wasserstein Distance range and a different feature distribution. The Wasserstein Distance (WD) metric quantifies feature distribution distances between attack classes, identifying unique malicious patterns in certain groups. ML-based NIDSs need improvement to detect sophisticated attacks with unique behaviour.

In 2023, Regis Anne et al. [22] explores IoT device vulnerabilities like Botnets, identity, and data theft, stressing secure cyber-physical systems. It proposes ML and DL for Botnet detection, presenting a framework using real-time traffic analysis on the Aposemat IoT-23 dataset. The GRU model achieves 99.87% detection accuracy, verified via pcap file analysis with Wireshark, showcasing 99.89% malware detection and superior time complexity. Performance metrics—accuracy, precision, recall, F1-Score—are compared, with VM excelling in accuracy and precision, while decision tree and rain forest models show strong recall and F1 scores. Naive Bayes, evaluated with an accuracy of 0.862575, also offers promising results. Rain Forest, suitable for memory-constrained datasets, achieves an accuracy of 0.912443. The paper offers crucial insights into IoT security, proposing a robust Botnet detection framework. Limitations include dataset specificity (Aposemat IoT-23) and potentially narrow evaluation metrics that may not fully reflect real-world IoT challenges.

According to Waad Alhoshan et al. [23], the majority of deep learning and machine learning techniques now in use for requirements engineering (RE) activities rely on supervised learning and call for substantial volumes of labelled training data. This was discovered in 2023. The paper tackles the problem of insufficient data in RE and shows how ZSL can be used to classify requirements. The study's ZSL method uses transformer-based language models (LMs) and contextual word embeddings to accomplish three classification tasks: NFR identification, Security classification, and FR/NFR classification. The findings demonstrate that without any training efforts, the ZSL technique delivers good performance. It obtains an F1 value of 0.66 for FR/NFR classification, F1 scores ranging from 0.72 to 0.80 for NFR identification, and an F1 score of approximately 0.66 for Security classification. However, limitations exist in accurately classifying certain NFR classes.

Malware-SMELL is a novel zero-shot learning technique that Pedro et al. [24] propose in 2022 for the visual representation-based classification of malware. Malware-SMELL presents S-Space, a novel representation space that increases class separability and boosts classification process effectiveness. In a model for classification trained solely using good-ware code, the suggested strategy outperformed previous approaches by an average ratio of 9.58% and attained a rate of recall of 80%. The generalized Zero-shot Learning paradigm, Malware-SMELL's performance was assessed through tests done on the MaleViz dataset. The outcomes show how successful Malware-SMELL is in detecting unknown malware, even on the first day after a malicious release.

In 2021, Adversarial Auto-encoders (AAE) and Bidirectional Generative Adversarial Networks (BiGAN), two generative deep learning techniques, are investigated by Abdalgawad et al. [25] for the purpose of identifying cyberattacks on Internet of Things (IoT) devices. The IoT-23 dataset—which includes network flows from Amazon Echo, Philips Hue, and Somfy door locks—is used by the authors to train these models. With an F1-Score of 0.99, the results demonstrate that the generative algorithms perform better than conventional machine learning methods like Random Forests. Furthermore, a BiGAN model with an F1-Score ranging from 0.85 to 1 is developed to identify unknown attacks, which includes zero-day attacks. The study does, however, have certain shortcomings, including the failure to compare the suggested models with alternative machine learning methods and the results' limited applicability to different Internet of Things devices or network conditions.

In order to overcome data imbalance difficulties frequently encountered in anomaly detection algorithms trained on imbalanced data, Ullah and Mahmoud [26] offers a method for abnormality identification in IoT networks in 2021. This method uses conditional generative adversarial networks (cGANs). To improve and balance the dataset, the method

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| | Monthly Peer Reviewed & Refereed Journal |

|| Volume 7, Issue 13, April 2024 ||

International Conference on Intelligent Computing & Information Technology (ICIT-24)

Organized by

Erode Sengunthar Engineering College, Erode, Tamilnadu, India

makes use of one-class cGAN (ocGAN) and binary-class cGAN (bcGAN) models. The ocGAN focuses on comprehending the minority data class in order to balance the dataset, whereas the bcGAN generates greater information for the binary weighed dataset. In terms of accuracy, precision, recall, and F1 score, the findings of ocGAN and bcGAN model evaluation using a feed-forward neural network (FFN) on networks-based anomaly datasets demonstrate that these models outperform previous anomaly detection methods. The findings show encouraging detection rates in a range of contexts and datasets, with the bcGAN demonstrating an astounding accuracy of 98.10% on the KDD99 dataset. The need for a sufficient amount of training data to ensure model accuracy is highlighted by the constraints that occur when a model's training sample is less than 1000. These restrictions result in lower detection rates. Additionally, using balanced datasets during the development of the model is necessary to ensure the efficacy of the bcGAN model.

Zhang et al.'s 2020 study [27] focuses on the difficulty of identifying unidentified attacks in network attack detection. The two primary techniques, honeypot and clustering, are limited in their ability to identify attacks in real time and gather unknown assault samples. In order to identify unknown threats, the study suggests a Zero-Shot Learning (ZSL) technique that learns the mapping relations among feature space and semantic space. The ZSL classifier creates links between known and unknown attacks by extracting semantic information that is shared by all assaults. The suggested ZSL technique, which is based on a sparse auto-encoder, uses feature-to-semantic mapping to find attacks by mapping the features of recognized attacks to the semantic space. When tested on NSL_KDD dataset, strategy outperforms other approaches with an average accuracy of 88.3%.

A few-shot solution for detecting network intrusions based on the concept of meta- framework is proposed by Xu et al. [28] in 2020. The technique makes use of FC-Net, a deep neural network, or DNN, that is made up of a comparison network and a feature extraction network. Based on two datasets created from actual network traffic data sources, the suggested approach is assessed. When trained and evaluated on the same datasets, the findings demonstrate that the technique produces great detection rates, with a median detection rate of up to 98.88%. Additionally, the method's generalizability is demonstrated by how well it works with various datasets and attack kinds. When there are few harmful samples available, the approach can detect samples that are malicious with a mean detection rate of up to 99.62% in a few-shot situation. In situations where an adequate amount of training samples are unavailable, such as zero-day attacks, the article emphasizes the significance of few-shot detection.

For network security, Yu and Bian [29] propose an intrusion detection technique that uses Few-Shot Learning (FSL) in 2020. On the KDD-Test+ and KDDTest-21 datasets, the technique outperforms previous methods and achieves excellent accuracy. Additionally, the approach demonstrates enhanced detection rates for several assault types, particularly for R2L and U2R, with significant improvements in detection rates. Resampling approaches are mentioned in the paper as a way to balance the dataset and enhance classification performance. Promising outcomes are also observed in the evaluation on the UNSW-NB15 dataset; however, particular measures are not specified. Nevertheless, the study does not provide thorough justifications for the method's loss function, distance function, and embedding function. The report also lacks a detailed analysis of dataset properties and a thorough comparison with other approaches.

V. DISCUSSION ON KEY CHALLENGES

Conventionally, several models are designed to detect unknown threats, but their performance was not up to par. Here, Table 1 lists a few of them. In deep learning models, the choice of input features holds significant importance as it directly influences the model's ability to learn and generalize effectively. Additionally, the imbalance prevalent in cybersecurity datasets, where instances of normal behavior outnumber attack instances, poses a challenge. To mitigate this, techniques such as SMOTE (Synthetic Minority Over-Sampling Technique) or adjusting class weights are employed to address the class imbalance issue. Moreover, the opacity of deep learning models, often labeled as "black boxes," raises concerns regarding interpretability.

The significance of CNN is addressed through diverse feature extraction but it lacks in-depth discussion on the interpretability of learned features and their implications on false positive rates in practical scenarios [20]. Moreover, ML-driven NIDSs prove ineffective in identifying certain zero-day attacks, as those with low Z-DR exhibit distinct feature distributions and wider Wasserstein Distance ranges [21]. The deep learning model Gated Recurrent Unit

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| | Monthly Peer Reviewed & Refereed Journal |

|| Volume 7, Issue 13, April 2024 ||

International Conference on Intelligent Computing & Information Technology (ICIT-24)

Organized by

Erode Sengunthar Engineering College, Erode, Tamilnadu, India

centers on a specific dataset (Aposemat IoT-23), potentially limiting the evaluation metrics' ability to encapsulate the entirety of real-world challenges [22], and the dataset's limited nature questions the appropriateness of metrics for assessing the proposed work's performance [23]. Additionally, ZSL based on language models are confined to a specific dataset, reliance on visual representation, and the complexity involved in establishing and maintaining S-Space markers raise concerns [24]. Adversarial Auto-encoders and Bi-directional GANs overlooks the exploration of other traditional machine learning methods' performance, with no scalability and computational requirements [25]. Further, conditional GANs scope is limited, dataset constraints hamper generalizability, and computational demands pose challenges [26]. The reliability of ZSL with Sparse Auto-encoders is further undermined by its reliance on obsolete datasets, inability to rapidly detect attacks, and difficulties in gathering unknown attack samples [27].

TABLE I. ANALYSIS ON EXISTING UNKOWN ATTACK DETECTION MODELS.

No.	Author	Methodology	Dataset	Issues
1	D. Y. Demirel et al. [20]	Zero-Shot Learning with CNN	2010 CSIC HTTP dataset.	• CNN feature extraction significance underscored, • real-world impact unclear.
2	Sarhan et al. [21]	Zero-Shot Learning	UNSW-NB15, NF-UNSW-NB15-v2.	• Zero-day attacks evade ML-based NIDSs due to unique feature distributions.
3	Regis Anne et al. [22]	Gated Recurrent Unit (GRU)	Aposemat IoT-23 Dataset	• Aposemat IoT-23 dataset's evaluation metrics may miss real-world challenges.
4	Waad Alhoshan et al. [23]	Zero Shot Learning based on language models (LMs)	PROMISE NFR, SecReq	• Limited dataset. Metrics used is not appropriate for evaluating the performance.
5	Pedro et al. [24]	Zero-Shot Learning, Mini-Batch Stochastic Gradient Descent (SGD)	Malimg. MaleVis	• Dataset dependency, visual representation, • S-Space marker complexity limit.
6	Abdalgawad et al. [25]	Adversarial Auto-encoders (AAE) and Bidirectional Generative Adversarial Networks (BiGAN)	IoT-23 dataset	• Lacks exploration of traditional ML methods' performance, scalability, and computational needs.
7	Ullah and Mahmoud [26]	Conditional Generative Adversarial Networks (cGANs), Feed Forward Neural Network (FFN)	KDD99, NSLKDD, BoT-IoT, IoT Network Intrusion, MQTT-IoT-IDS2020, MQTTset and IoT-23.	• Limited Scope, Dataset Limitations, Generalizability, computational requirements
8	Zhang et al. [27]	Zero-Shot learning, Semantic mapping model, Sparse auto-encoder	NSL_KDD dataset	• Unknown attack sample collection is challenging, timely detection is not achieved, and the dataset is outdated.
9	Xu et al. [28]	Deep Neural Network	ISCX2012FS,	• No evaluation on

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| | Monthly Peer Reviewed & Refereed Journal |

|| Volume 7, Issue 13, April 2024 ||

International Conference on Intelligent Computing & Information Technology (ICIT-24)

Organized by

Erode Sengunthar Engineering College, Erode, Tamilnadu, India

		(DNN).	CICIDS2017FS	real-world traffic. The paper claims universality but lacks analysis to substantiate the claim.
10	Yu and Bian [29]	Few-Shot Learning (FSL)	NSL-KDD (KDD-Test+ and KDD-Test-21), UNSW-NB15	• Incomplete description of Few-Shot Learning (FSL) technique. Testing set disproportions noted.

VI. Conclusion and Future Work

The spread of IoT devices poses a serious danger to global security settings due to its large attack surface that is susceptible to many types of assaults. Even with the increased focus on Internet of Things security, conventional methods such as signature-based and heuristic-based detection are not effective in spotting new threats, such as zero-day vulnerabilities. Although network intrusion detection systems (NIDS) are essential for protecting network infrastructures, cybercriminals take advantage of weaknesses in IoT devices with limited resources to open up new attack vectors. This study explores how intrusion detection techniques and Internet of Things attacks are changing, emphasizing the growing threat that comes from unknowns and the use of cutting-edge approaches like zero-shot learning for identification. As IoT devices become more interconnected, hackers take advantage of these weaknesses. Because of their advanced penetration techniques, botnet assaults have become an especially dangerous menace. This study highlights the effectiveness of zero-shot learning in identifying hitherto unidentified attack patterns, even if several intrusion detection techniques show promise in strengthening IoT security. This research highlights the need for proactive actions to successfully manage developing IoT security concerns and minimize potential risks by throwing light on these developments.

REFERENCES

[1] A. Derhab et al.“Intrusion Detection System for Internet of Things Based on Temporal Convolution Neural Network and Efficient Feature Engineering” Wirel. Commun. Mob. Comput., vol. 2020, 1-16, 2020, doi:10.1155/2020/6689134.
[2] S. Fenanir et al., “A semi-supervised deep auto-encoder based intrusion detection for IoT,” Ingénierie Syst. Inf., vol. 25, no. 5, pp. 569-577, 2020, doi:10.18280/isi.250503.
[3] W. Yang, “Research on network security problems and countermea- sures based on the Internet of Things technology,” J. Phys. Conf. Ser., vol. 1744, no. 4, Feb., Art. no. 042010, 2021, doi:10.1088/1742-6596/1744/4/042010.
[4] C. Vorakulpipat et al., “Recent challenges, trends, and concerns related to IoT security: An evolutionary study,” 20th International Conference on Advanced Communication Technology (ICACT), Chuncheon, South Korea, 2018, 2018, pp. 405-410, doi:10.23919/ICACT.2018.8323774.
[5] S. A. Butt et al. 19th International Conference on Computational Science and Its Applications (ICCSA), St. Petersburg, Russia, 2019, 2019, pp. 26-31, doi:10.1109/ICCSA.2019.000-8.
[6] M. Burhan et al., “IoT elements, layered architectures and security issues: A comprehensive survey,” Sensors (Basel), vol. 18, no. 9, Sept., Art. no. 9, 2018, doi:10.3390/s18092796.
[7] I. Andrea et al., “Internet of Things: Security vulnerabilities and challenges,” IEEE Symposium on Computers and Communication (ISCC), Larnaca, Cyprus, 2015, 2015, pp. 180-187, doi:10.1109/ISCC.2015.7405513.
[8] A. Khraisat et al, “Survey of intrusion detection systems: Techniques, datasets and challenges,” Cybersecur., vol. 2, no. 1, p. 20, 2019, doi:10.1186/s42400-019-0038-7.
[9] H.-J. Liao et al., “Intrusion detection system: A comprehensive review,” J. Netw. Comput. Appl., vol. 36, no. 1, pp. 16-24, ISSN 1084-8045, 2013, doi:10.1016/j.jnca.2012.09.004.
[10] M. Weber and M. Boban, “Security challenges of the internet of things,” 39th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, Croatia, 2016, 2016, pp. 638-643, doi:10.1109/MIPRO.2016.7522219.
[11] B. Ali and A. I. Awad, “Cyber and physical security vulnerability assessment for IoT-based smart homes,” Sensors (Basel), vol. 18, no. 3, pp. 1-17, 2018, doi:10.3390/s18030817.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| | Monthly Peer Reviewed & Refereed Journal |

|| Volume 7, Issue 13, April 2024 ||

International Conference on Intelligent Computing & Information Technology (ICIT-24)

Organized by

Erode Sengunthar Engineering College, Erode, Tamilnadu, India

[12] S. A. Kumar et al., "Security in internet of things: Challenges, solutions and future directions" in 49th Hawaii International Conference on System Sciences (HICSS), Koloa, vol. 2016, 2016, pp. 5772-5781, doi:10.1109/HICSS.2016.714.
[13] A. A. Gendreau and M. Moorman, "Survey of intrusion detection systems towards an end to end secure internet of things" in Conference on Future Internet of Things and Cloud (FiCloud), vol. 2016, I. E. E. E. 4th International, Ed. Vienna: IEEE, 2016, pp. 84-90, doi:10.1109/FiCloud.2016.20.
[14] B. B. Zarpelão et al., "A survey of intrusion detection in internet of things," J. Netw. Comput. Appl., vol. 84, pp. 25-37, 2017, doi:10.1016/j.jnca.2017.02.009.
[15] A. Khraisat et al., "A novel ensemble of hybrid intrusion detection system for detecting Internet of things attacks," Electronics, vol. 8, no. 11, p. 1210, 2019, doi:10.3390/electronics8111210.
[16] G. Creech and J. Hu, "A semantic approach to host-based intrusion detection systems using contiguousand discontiguous system call patterns," IEEE Trans. Comput., vol. 63, no. 4, pp. 807-819, 2014, doi:10.1109/TC.2013.13.
[17] S. K. Gautam and H. Om, "Computational neural network regression model for host based intrusion detection system," Perspect. Sci., vol. 8, pp. 93-95, 2016, doi:10.1016/j.pisc.2016.04.005.
[18] Snort the Open Source Network Intrusion Detection System. Available at: https://www.snort.org.
[19] M. Salem et al., "Anomaly generation using generative adversarial networks in Host-Based Intrusion Detection" in Host-Based Intrusion Detect., Electronics & Mobile Communication Conference (UEMCON), New York, NY, USA, 2018, 2018, pp. 683-687, doi:10.1109/UEMCON.2018.8796769.
[20] D. Y. Demirel and M. T. Sandikkaya, "Web based anomaly detection using zero-shot learning with CNN" in IEEE Access, vol. 11, pp. 91511-91525, 2023, doi:10.1109/ACCESS.2023.3303845.
[21] M. Sarhan et al., "From zero-shot machine learning to zero-day attack detection," Int. J. Inf. Secur., vol. 22, no. 4, pp. 947-959, 2023, doi:10.1007/s10207-023-00676-0.
[22] W. Regis Anne et al, Detection of IoT Botnet Using Machine Learning and Deep Learning Techniques, Mar. 02 2023 [Preprint], 1st version available at Research Square, doi:10.21203/rs.3.rs-2630988/v1.
[23] W. Alhoshan et al., "Zero-shot learning for requirements classification: An exploratory study," Inf. Softw. Technol., vol. 159, p. 107202, ISSN 0950-5849, 2023, doi:10.1016/j.infsof.2023.107202.
[24] P. H. Barros et al., "A zero-shot learning strategy for detecting zero-day vulnerabilities, Computers & Security," vol. 120, p. 102785, ISSN 0167-4048, 2022, doi:10.1016/j.cose.2022.102785.
[25] N. Abdalgawad et al., "Generative deep learning to detect cyberattacks for the IoT-23 dataset" in IEEE Access, vol. 10, pp. 6430-6441, 2022, doi:10.1109/ACCESS.2021.3140015.
[26] I. Ullah and Q. H. Mahmoud, "A framework for anomaly detection in IoT networks using conditional generative adversarial networks" in IEEE Access, vol. 9, pp. 165907-165931, 2021, doi:10.1109/ACCESS.2021.3132127.
[27] Z. Zhang et al., "Unknown attack detection based on zero-shot learning" in IEEE Access, vol. 8, pp. 193981-193991, 2020, doi:10.1109/ACCESS.2020.3033494.
[28] C. Xu et al., "A method of few-shot network intrusion detection based on meta-learning framework" in IEEE Trans. Inf. Forensics Sec., vol. 15, pp. 3540-3552, 2020, doi:10.1109/TIFS.2020.2991876.
[29] Y. Yu and N. Bian, "An Intrusion Detection Method Using Few-Shot Learning", IEEE Access, vol. 8, pp. 49730-49740, 2020, doi:10.1109/ACCESS.2020.2980136.
[30] R. Khan et al., "Future internet: The internet of things architecture, possible applications and key challenges" in 10th International Conference on Frontiers of Information Technology, vol. 2012. Islamabad: IEEE, 2012, pp. 257-260, doi:10.1109/FIT.2012.53.
[31] I. Goodfellow et al., "Generative adversarial networks," Commun. ACM, vol. 63, no. 11, pp. 139-144, 2020, doi:10.1145/3422622.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com