Abhilasha Sinha, et. al. International Journal of Engineering Research and Applications
www.ijera.com
ISSN: 2248-9622, Vol. 14, Issue 10, October 2024, pp 79-83

RESEARCH ARTICLE OPEN ACCESS

Survey on Types of Attacks and Models of Intrusion Detection System

[1]Abhilasha Sinha, [2]Prof. Rakesh Kumar Tiwari, [3]Prof.Onkar Nath Thakur,
Department of Computer Science and Engineering,
Technocrats Institute of Technology & Science, Bhopal, India

ABSTRACT
Networks are becoming increasingly dynamic due to the widespread use of portable wireless devices. Consequently, the Internet of Things (IoT) networks are able to adapt to diverse environments and applications, enhancing their flexibility. However, this increased flexibility also heightens the risk of attacks on such networks. This paper provides a comprehensive summary of the research conducted in the field of intrusion detection for securing various types of networks. The paper discusses the architecture of Intrusion Detection Systems (IDS) and categorizes them according to the specific networks they protect. It details the models proposed by various authors, elaborating on the techniques employed for detecting intrusions in different environments. Furthermore, the paper lists the strengths and limitations of various techniques used for intrusion detection. Lastly, it presents the evaluation parameters used to compare these models, offering a thorough comparison to understand their effectiveness and areas for improvement.
Keywords- Deep Learning, Intrusion Detection, Feature Optimization, Genetic Algorithm, Soft Computing.

Date of Submission: 12-10-2024 Date of acceptance: 25-10-2024

I. INTRODUCTION

The rapid development of embedded systems has significantly contributed to the growth of the communication network. This technology allows a diverse array of electronic devices, each equipped with transmitters, receivers, or both, to seamlessly connect to the global network. Through precise configurations of hardware and software, these devices can be remotely managed within IoT networks, with each device uniquely identified using IPv6 addresses. This ability to control devices remotely offers substantial cost savings across various applications, including research projects, surveillance operations, and data collection efforts. IoT networks facilitate communication among household appliances, industrial controls, scientific research sensors, and more [1]. This interconnectedness alleviates the burden on traditional servers, routers, and switches, thereby enhancing overall system flexibility and efficiency.

Nevertheless, the extensive global access provided by IoT networks necessitates stringent security measures to protect devices, services, and data from unauthorized access and potential attacks [2]. The ubiquity of internet-based threats poses significant risks, potentially incapacitating devices, especially under weak communication channels. Such vulnerabilities can lead to system failures in services that rely on IoT infrastructure.

The successful deployment of IoT networks in various application domains depends on their resilience against a wide array of threats and intrusions. This underscores the importance of adhering to CIA (Confidentiality, Integrity, and Availability) standards and implementing robust security defense mechanisms. Intrusion Detection Systems (IDS) play a vital role in this context [3, 4]. IDS use agent-based techniques to continuously monitor the network for signs of attacks, and when an intrusion is detected, they generate alarms to trigger appropriate responses.

The primary objective of IDS is to detect activities that threaten the confidentiality and integrity of the IoT environment. IDS are typically divided into two main types: misuse-based and anomaly-based. Misuse-based IDS identify threats by comparing network activity against a database of known attack patterns [5]. These systems often utilize machine learning models such as Convolutional Neural Networks (CNN) and Feedforward Neural Networks (FFNN) to enhance their detection capabilities [6]. Researchers are also exploring improvements in feature sets to optimize the learning process of these models.

Anomaly-based IDS, on the other hand, focus on detecting unusual behavior by establishing a baseline of normal network activity and identifying deviations from this baseline. These systems employ various learning models to distinguish between normal and abnormal activities [7]. The goal is to detect novel attacks that do not match any known patterns. This paper also suggests that integrating machine learning models with feature selection techniques can further improve the efficiency and accuracy of IDS.

In summary, the paper highlights the importance of Intrusion Detection Systems in safeguarding IoT networks. By leveraging advanced machine learning techniques and continuously refining feature sets, IDS can effectively detect and respond to security threats, ensuring the confidentiality, integrity, and availability of IoT systems.

II. RELATED WORK

In this section IDS models proposed by other scholars are detailed where first few work gives an detail of normal network IDS system further IOT networks IDS's proposed by authors were detailed with their techniques.

YueJin et. al. [8], 2018 for home level intrusion detection system, using Wifi-Enabled IOT devices. Authors implemented a RSSI (Received signal strength indicator) based identification router that incorporate with a detection algorithm and visualize the whole home security through IOT. This kind of work is highly depends on equipment efficiency and single parameter (signal strength). Such an implementation was done on static network only, for mobile network where device come as guest for communication.

E.Anthiet. al.[9] ,Oct 2019 proposed a three layer intrusion detection system (IDS) that uses a supervised approach to detect a range of popular network based cyber-attacks on IoT networks. The system consists of three main functions: 1) classify the type and profile the normal behavior of each IoT device connected to the network; 2) identifies malicious packets on the network when an attack is occurring; and 3) classifies the type of the attack that has been deployed. Model uses all dataset feature which increases confusion while learning.

Ullah I , Mahmood Q.H [10], 2020 examines a novel scheme for generating datasets tailored for anomalous activity detection in IOT networks. By investigating methodologies and implementations , it sheds light on the efficacy of this approach in simulating real world scenarios and enhancing the accuracy of intrusion detection systems. This synopsis offers a glimpse into the innovative techniques shaping the future of IOT security.

J. Liu. Et. al.[11], 2021 proposed a particle swarm optimization-based gradient descent (PSO-LightGBM) for the intrusion detection. In this method, PSO-LightGBM is used to extract the features of the data and inputs it into one-class SVM (OCSVM) to discover and identify malicious data. The UNSW-NB15 dataset is applied to verify the intrusion detection model. SVM is limited to two class identification only.

X.Zhou , W. Liang [12] , investigates hierarchial adversarial attacks targeting graph neural networks within IOT network intrusion detection systems. By analyzing methodologies and advancements , it illuminates the evolving landscape of cybersecurity threats in IOT environments. 9

J.Liu ,D. Yang, [13] Proposed enhancing intrusion detection system within IOT environments . It delves into methodologies , implementation , and challenges , providing insights into the effectiveness of PSO in optimizing feature selection rule generation , and anamoly detection . The synthesis of existing research offers valuable insights for enhancing security in IOT networks.

Using a Dense Random Neural Network (DnRaNN), Latif et al. [14], 2021 suggested a unique lightweight approach for IoT network intrusion detection. The authors ran extensive trials on the ToNIoT dataset, including both binary and multi-class classification situations, to assess their technique.

S.W. Azumah , N. Elsayed [15] ,2021 examines a deep long term memory [LSTM] based approach for intrusion detection in IOT device networks within smart homes. By exploring methodologies and implementations , it highlights the effectiveness of deep learning techniques in detecting anomalous behaviour and enhancing the security of smart home environments.

J. Liu, D. Yang, M. Lian [16], 2021 the authors analyze and evaluate contemporary methods that make use of different types of data. For intrusion detection in ICS, a hybrid deep learning approach is deployed. Normal and abnormal network traffic are distinguished by LSTM and CNN models.

XiuKanet. al. [17] , 2021 proposed a novel IoT network intrusion detection approach based on Adaptive Particle Swarm Optimization Convolutional Neural Network (APSO-CNN). In particular, the PSO

algorithm with change of inertia weight is used to adaptively optimize the structure parameters of one-dimensional CNN. The cross-entropy loss function value of the validation set, which is obtained from the first training of CNN, is taken as the fitness value of PSO. This work has not utilize IOT dataset or environment. Adding new artificial session increase work complex.

By comparing characteristics from the UNSWNB15 and Bot-IoT data-sets based on flow and Transmission Control Protocol (TCP), we were able to generate a data-set of packets from IoT traffic for use in [18]'s, 2022 proposed Protocol Based Deep Intrusion Detection (PB-DID) architecture. We solve issues like unbalanced and over-fitting to properly categorize normal, DoS, and DDoS traffic.

In M. Mohy-Eddine [19],2023 the authors create a model for IoT security intrusion detection using feature engineering and machine learning. To cut down on computational cost and prediction time, we integrate Isolation Forest (IF) with Pearson's Correlation Coefficient (PCC). IF is used to find and eliminate anomalies in data sets. To choose the best characteristics, we use the PCC algorithm. In both cases (PCCIF and IFPCC), PCC and IF can be used interchangeably. Improved IDS functionality is achieved by the use of the Random Forest (RF) classifier.

In [20], 2023 the authors investigate identification and discriminative deep learning methods for detecting malware used in cyberattacks. The study did a nice job of summarizing the seven techniques, which included three types of deep learning (RNN, CNN, and DNN) and four types of generative models/methods (RBN, DBN, DBM., and DA). This study also pays special attention to the reliability and availability of research-related dictionaries. This study's experiments show that IDS and Cybersecurity threats may be detected in a collaborative technological setting.

IV. TYPES OF NETWORK ATTACKS

Different network based attacks were categorized into following classes [21,22]:

1. Insider attack

Sometimes people having the authorization to use the cloud service, though choose to gone through the insider way. This mainly done with the intention of using the unauthorized privileges and revealing the information to other clients or in market. An insider attack has been planned mostly by the employees of the competitors or the cloud administrator in the domain client company having right to access those. They also had hand in modifying the company's information and documents.

The best-known example to clear about this insider attack is the Amazon Elastic Compute Cloud (EC2) (Slaviero, 2002) – an internal attack of DoS.

2. Cloud malware injection attack

In this attack, the attacker has the motive of not only accessing the information but also get control over it of the client data. For this attacker creates its own service implementation module for setting it into a client cloud system. For this uses SaaS/PaaS method or the virtual machine instance into the IaaS solution. To result in a performing malicious activity, attacker if gets succeed in his work of cloud fouling, the cloud will automatically accept and sends the hacker module information to the user. Due to which the begins of malicious activities performing by the attacker.

Types of attacks under this category:

Cross site scripting attack: XSS uses the HTML for the attack in which malicious code is injected into the data by using the Flash, JavaScript or others.

SQL injection attack: In this attack the attacker uses the input field of the database of the user. The most common example for such types of attacks are the attack occurred on the Sony play station in the year 2008 website.

Command injection attack: the name of this attack is given as per its role, because it injects the command and those commands are run according to the runtime environment or may create shell.

3. Abuse and Nefarious use of cloud services

The main difference in this attack than the insider is the attackers background, otherwise all is in common. In the insider attack the attacker is the authorised user of the data while in this attacker is the hacker which attacks the less secured database or poor clouds. As due to this no need of using expensive DoS and did brute forced attacks on the target.

4. Denial of service attack

This type of attacksis mainly done by the flooded networks having many packets like TCP, UDP, ICMP or their combinations.due to the risk of the intruder attack on the distributed services of the computer, some of them are not even available to the authorised users also. As this attack overloads all the systems, due to which legal users are unable to used them.These types of attacksprove very dangerous for the single cloud data and servers as many users depends on that cloud distributed network.

5. Side channel attack

This type of attack done with the cryptographic algorithm of the system. For this they used the special VMM service which is virtual machine manger which guides the user attack for the creation of virtualization layer. They placed a physical virtual machine on the

targeted system, while VMM helps other users and supervises known as hypervisor.

6. User to root attack

In this attack, the attacker uses the sniffing password for the authentication of the targeted user's system. So, by combining traditional various methods for the raising of the privileges to the super user access acceptance. An example of such escalation technique is the smashing stack, in which a packet of the set-UID- root program that corrupts the address space, so that returning information from the instruction to subshell space.

7. A remote to Local attack

In this attacker takes the advantages of the targeted user local privileges. This attack is also known as remote to user attack. In this attacker sends packets to the user host and close the exposures of the access of asxlock, guest, xnsnoop, phf and sendmail.

8. Scanning Attacks A scanning attack [27] is an attack that attempts to send packets of information to a network system to gather information about the topology. It involves looking for ports which are either open or closed, what type of traffic is permitted and not permitted, which hosts are active or even the type of hardware running on different devices. For instance, a type of attack that finds weak points in a network is Blind SQL injection attacks. A Blind SQL injection attack is an attempt to ask a database questions that make it respond by a Boolean value to find vulnerabilities. These types of attacks often attempt to find open ports to be exploited by injecting malicious code or malware.

9. Asymmetric Routing When packets take a specific route to the destination, and a different route back to the source, this behaviour is called asymmetric routing [27]. This behaviour is normal in general, but it is unwanted. The reason behind that is adversaries can benefit from asymmetric routing by sending malicious data through particular parts of the network to bypass security systems, depending on firewalls configuration. If the network is allowed to perform asymmetric routing, then it is exposed to attacks such as SYN flood attacks. An SYN flood attack is an attack that attempts to open many connections without closing them (half-open attack), which leads to a total consumption of system or server resources so that it becomes unresponsive. This attack is a DDoS attack type, and one reason to deactivate asymmetric routing in the network.

10. Buffer Overflow Attacks Buffer overflow [27] attacks attempt to replace normal data with malicious data in penetrated memory parts, such that a malicious code gets executed later on. In generic terms, a buffer overflow attack writes more data in the memory's buffer than it can handle; performing this action results in making the data overflow into the neighbouring memory.

III. EVALUATION PARAMETER

In order to evaluate results there are many parameter [20] such as accuracy, precision, recall, F-score, etc. Obtaining values can be put in the mention parameter formula to get results.

$$\text{Precision} = \frac{\text{True\_Positive}}{\text{True\_Positive} + \text{False\_Positive}}$$

$$\text{Recall} = \frac{\text{True\_Positive}}{\text{True\_Positive} + \text{False\_Negative}}$$

$$F\_Score = \frac{2 * \text{Precision} * \text{Recall}}{\text{Precision} + \text{Recall}}$$

$$Accuracy = \frac{Correct\_Classification}{Correct\_Classification + Incorrect\_Classification}$$

IV. CONCLUSIONS

Wireless network enhances human life's adaptability, drawing numerous intruders who seek unauthorized access to data, compromising privacy. This paper compiles various methods proposed by scholars for intrusion detection in networks, clouds, IoT, and other domains. It was observed that many researchers focus on feature optimization using genetic algorithms. Additionally, the application of feature reduction techniques has improved the accuracy of intrusion class detection in many machine learning models. In the future, scholars could explore different neural network models, such as spiking neural networks.

REFERENCES

[1]. D. Denning and P. G. Neumann, Requirements and model for IDES-a realtime intrusion- detection expert system. SRI International, 1985.

[2]. D. E. Denning, "An intrusion-detection model," Software Engineering, IEEE Transactions on, no. 2, pp. 222–232, 1987.

[3]. M. M. Sebring, "Expert systems in intrusion detection: A case study," in Proc. 11th National Computer Security Conference, Baltimore, Maryland, Oct. 1988, 1988, pp. 74–81

[4]. R. Jagannathan, T. Lunt, D. Anderson, C. Dodd, F. Gilham, C. Jalali, H. Javitz, P. Neumann, A. Tamaru, and A. Valdes, "System design document: Next-generation intrusion detection expert system (nides)," Technical Report, Tech. Rep., 1993.

[5]. R. Maxion, K. Tan et al., "Anomaly detection in embedded systems," Computers, IEEE Transactions on, vol. 51, no. 2, pp. 108–120, 2002.

[6]. Zegzhda P., Kort S. (2007) Host-Based Intrusion Detection System: Model And Design Features. In: Gorodetsky V., Kotenko I., Skormin V.A. (Eds) Computer Network Security. MMM-ACNS 2007. Communications In Computer And Information Science, Vol 1. Springer, Berlin, Heidelberg.+

[7]. N. Moustaf and J. Slay, ''Creating novel features to anomaly network detection using DARPA-2009 data set,'' in Proc. 4th Eur. Conf. Cyber Warfare Secur. Academic Conf. Limited, 2015, pp. 204–212.

[8]. Yue Jin, Zengshan Tian, Mu Zhou, Ze Li and Zhenyuan Zhang. A Whole-Home Level Intrusion Detection System using WiFi-enabled IoT International Wireless Communications & Mobile Computing Conference (IWCMC), ISSN: 2376-6506, Published Year 2018 .

[9]. E. Anthi, L. Williams, M. Słowińska, G. Theodorakopoulos and P. Burnap, "A Supervised Intrusion Detection System for Smart Home IoT Devices," in IEEE Internet of Things Journal, vol. 6, no. 5, pp. 9042-9053, Oct. 2019.

[10]. Ullah I., Mahmoud Q.H. (2020) A Scheme for Generating a Dataset for Anomalous Activity Detection in IoT Networks. In: Goutte C., Zhu X. (eds) Advances in Artificial Intelligence. Canadian AI 2020.

[11]. J. Liu, D. Yang, M. Lian and M. Li, "Research on Intrusion Detection Based on Particle Swarm Optimization in IoT," in IEEE Access, vol. 9, pp. 38254-38268, 2021.

[12]. X. Zhou, W. Liang, W. Li, K. Yan, S. Shimizu and K. I. -K. Wang, "Hierarchical Adversarial Attacks Against Graph-Neural-Network-Based IoT Network Intrusion Detection System," in IEEE Internet of Things Journal, vol. 9, no. 12, pp.

[13]. J. Liu, D. Yang, M. Lian and M. Li, "Research on Intrusion Detection Based on Particle Swarm Optimization in IoT," in IEEE Access, vol. 9, pp. 38254-38268, 2021.

[14]. S. Latif, Z. e. Huma, S. S. Jamal, F. Ahmed, J. Ahmad, A. Zahid, K. Dashtipour, M. Umar Aftab, M. Ahmad, Q. H. Abbasi, Intrusion Detection Framework for the Internet of Things using a Dense Random Neural Network, IEEE Transactions on Industrial Informatics (2021).

[15]. S. W. Azumah, N. Elsayed, V. Adewopo, Z. S. Zaghloul, C. Li, A Deep LSTM based Approach for Intrusion Detection IoT Devices Network in Smart Home, in: 7th IEEE World Forum on Internet of Things, WF-IoT 2021, 2021, pp. 836–841.

[16]. J. Liu, D. Yang, M. Lian and M. Li, "Research on Intrusion Detection Based on Particle Swarm Optimization in IoT," in IEEE Access, vol. 9, pp. 38254-38268, 2021

[17]. Xiu Kan, Yixuan Fan, Zhijun Fang, Le Cao, Neal N. Xiong, Dan Yang, Xuan Li. "A novel IoT network intrusion detection approach based on Adaptive Particle Swarm Optimization Convolutional Neural Network". Information Sciences, Volume 568,2021.

[18]. M. Zeeshan et al., "Protocol-Based Deep Intrusion Detection for DoS and DDoS Attacks Using UNSW-NB15 and Bot-IoT Data-Sets," in IEEE Access, vol. 10, pp. 2269-2283, 2022.

[19]. C. Yao, Y. Yang, K. Yin and J. Yang, "Traffic Anomaly Detection in Wireless Sensor Networks Based on Principal Component Analysis and Deep Convolution Neural Network," in IEEE Access, vol. 10, pp. 103136-103149, 2022.

[20]. M. Mohy-Eddine, A. Guezzaz, S. Benkirane, M. Azrour and Y. Farhaoui, "An Ensemble Learning Based Intrusion Detection Model for Industrial IoT Security," in Big Data Mining and Analytics, vol. 6, no. 3, pp. 273-287, September 2023.

[21]. I. A. Kandhro et al., "Detection of Real-Time Malicious Intrusions and Attacks in IoT Empowered Cybersecurity Infrastructures," in IEEE Access, vol. 11, pp. 9136-9148, 2023.

[22]. Govinda.K1, Kevin Thomas. "Survey on Feature Selection and Dimensionality Reduction Techniques". International Research Journal of Engineering and Technology Volume: 03 Issue: 07, 2016.