Lightweight Intrusion Detection System(L-IDS) for the Internet of Things

D Divya Priya[1]
Department of Computer Science and Engineering
MLR Institute of Technology
Hyderabad, India
divya.degala@gmail.com

Ajmeera Kiran[2]
Department of Computer Science and Engineering
MLR Institute of Technology
Hyderabad, India
kiranphd.jntuh@gmail.com

P Purushotham[3]
Department of Computer Science and Engineering
MLR Institute of Technology
Hyderabad, India
purushotham541@gmail.com

2022 International Conference on Advancements in Smart, Secure and Intelligent Computing (ASSIC) | 978-1-6654-6109-2/22/$31.00 ©2022 IEEE | DOI: 10.1109/ASSIC55218.2022.10088328

***Abstract* - Internet of Things devices collect and share data (IoT). Internet connections and emerging technologies like IoT offer privacy and security challenges, and this trend is anticipated to develop quickly. Internet of Things intrusions are everywhere. Businesses are investing more to detect these threats. Institutes choose accurate testing and verification procedures. In recent years, IoT utilisation has increasingly risen in healthcare. Where IoT applications gained popular among technologists. IoT devices' energy limits and scalability raise privacy and security problems. Experts struggle to make IoT devices more safe and private. This paper provides a machine-learning-based IDS for IoT network threats (ML-IDS). This study aims to implement ML-supervised IDS for IoT. We're going with a centralised, lightweight IDS. Here, we compare seven popular categorization techniques on three data sets. The decision tree algorithm shows the best intrusion detection results.**

Keywords—*IDS,,Decision Tree algorithm*

I. INTRODUCTION

There are two primary causes of security and privacy breaches. First, there is the issue that most IoT devices aren't very powerful or efficient. Using common Internet security methods like AES and RSA in the IoT environment could be challenging [1]. End-to-end encryption through TLS or IPsec is possible in high-resource gadgets like smartphones, tablets, and personal computers (IPsec). There is no way to apply these methods directly to limited resource objects, resulting in monitoring, side-channel attacks, and listening in on conversations. For IoT security, machine-learning-based intrusion detection must be deployed. Devices are linked to online services via the Internet of Things (IoT). IoT drives automation in the home, in industry, in the healthcare system, and in the infrastructure of smart cities. The latest technological advancements are linking the nation's economy, communities, and government institutions and Critical National Infrastructure (CNI). Internet of Things (IoT) and smart technologies fuel connected dwellings, vehicles, hospitals, cities, and power systems. CNI principles make regular tasks easier, yet IoT and ICT gadgets raise safety concerns. The availability of systems and energy supplies can be harmed in several ways, such as by spoofing, data escape, denial of service, energy bleed, insecure gateways, and so on. Service can be hampered by security concerns. In the event of an attack on mass transportation systems or power grids, energy waste and outages can occur. A central cloud can't provide the service needs of IoT attack detection. [2] The Internet of Things (IoT) refers to a network of computers and other gadgets that may exchange data and have wireless conversations without any human intervention. As the number of connected devices grows, so do the number of hacking attempts. When an intruder gains access to a system, they do so without authorization. The end outcome is anything from data modification to data absence to data misuse and beyond. We must secure IoT devices from threats or intrusions. These breaches are uncovered by the intrusion detection system. Our post builds an IoT intrusion detection system. Having an IDS on every IoT node isn't cost-effective. We plan to implement a centralised IDS using a network of Internet of Things gadgets. Our article uses feature selection and classification. In feature selection, we take only those data set features that are most important for attack detection. We chose the seven most well-known classification algorithms—Logistic-Regression,

978-1-6654-8695-8/22/$31.00 ©2022 IEEE

Decision-Tree, K-Nearest-Neighbor Multi-Layer Perceptron, Naive-Bayes Random-Forest, and Support-Vector-Machine—and compared how well they performed in a classification task.

II. LITERATURE SURVEY

There has been a lot of study done on protecting IoT devices. IoT intrusion detection was first presented by Shahid Raza [3]. The Intrusion Detection System of the Contiki Operating System. Content spoofing, slurp, and selective transfer attacks are the only ones picked out by this system. A deep-packet anomaly detection method was presented for Internet-of-Things devices by Douglas et al. [4]. This technique models payloads based on n-gram bit-patterns and accommodates n-gram sizes of varying lengths.

Using KNN, Li et al. [5] proposed an intrusion detection method for a wireless sensor network. Only an oversaturation of a wireless sensor network will be detected by this gadget.

Non-symmetric deep auto-encoders (NDAEs) were developed by Shone et al. [6] to acquire features without human oversight. NDAEs are stacked for learning and categorization.

Oh et al. [7 identified dangerous patterns to secure IoT networks. They were able to lessen their reliance on pattern-matching memory by employing techniques like auxiliary shifting and early choosing. They claimed effectiveness in detecting a dangerous pattern early, but they couldn't identify and classify DoS, bogus data injection, and other assaults. An attacker can try a different pattern each time, making it harder for a node to detect an assault.

In order to get the parameters of their classifiers to converge quickly, Ali et al. [8] built a fast learning network (FLN) using PSO. While the findings may be satisfactory, the intricacy of the system makes it challenging to implement using sensor nodes because to their limited computing and energy-storage capabilities. Particle swarm optimization (PSO) was combined with a genetic algorithm (GA) and a support vector machine (SVM) by Moukhafi et al. [9]. The algorithm has almost perfect accuracy in differentiating DoS attacks from other forms of attacks, but not typical class signals. To improve the performance of a support vector machine (SVM) classifier, Vajayanand et al. [10] proposed a hybrid feature-selection approach. A GA and MI were utilised in this method (MI). In addition, they demonstrated that an SVM-based classifier can achieve better results than an artificial neural network [11,12]. They found that training the classifier with 400 samples resulted in 96% accuracy in their experiment. The advanced mode of intrusion detection with the machine learning, big data and SDN methods are discussed in [13,14, 15].

III. PROPOSED SYSTEM

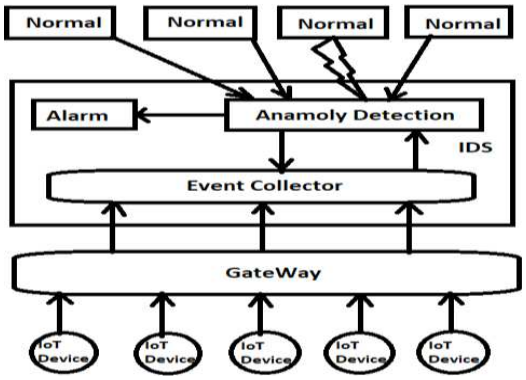

Fig 1: LIDS Architecture

Due to assaults on IoT devices, we need an IDS. We provide a lightweight IoT intrusion detection system. Lightweight because we have a centralised intrusion detection system instead of one at each node, which is more cost-effective for small IoT devices. [10] Figure 1 displays our lightweight IDS architecture.

We follow these procedures to implement our IDS:

Dataset upload: We used UNSW-NB15, KDD Cup 99, and NSL-KDD in our article.

A. Preprocessing

In preprocessing, we alter our dataset and create a new one for our machine learning model. The dataset is transformed, binarized, standardised, and normalised during preprocessing.

B. Features Collection:

Here, we chose only the dataset features most important to the outcome. Wrapper, embedding, and filter are feature selection models.

We chose filter approach since it's efficient and cost-effective. This filter method assigns a correlation value to each feature based on its impact on output. We'll establish a threshold value and only select features with a higher association.

C. Classification Techniques:

Training and examination of models are both part of the classification process. In the process of data preparation, the dataset is partitioned into a training and testing component [10,11]. During training, we make use of a dataset that has been labelled. In order to validate our model, we will want a testing dataset. In this article, we will be discussing Logistic-Regression, Decision-Tree, K-Nearest-Neighbor Multi-Layer Perceptron[12,13], Naive-Bayes Random-Forest, and Support-Vector-Machine—and compared how well they performed in a classification task [14].

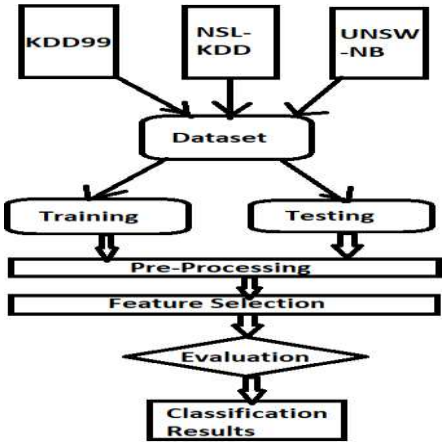

Fig 2: Classification Process

D. Performance evaluation

We analyse each algorithm's performance to identify the best classifier for our situation. The decision tree approach performs best for all three data sets, as seen in the graph below.

IV. EVALUATION AND RESULTS

The results of our experiments are as shown in the below graph:

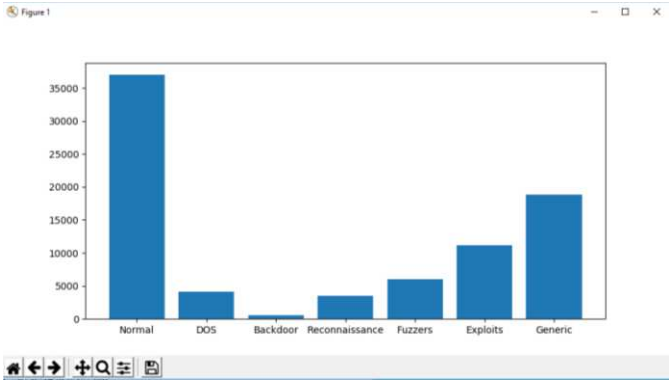

Fig 3: Analysis of Attacks of different types

In above graph x-axis we have attack type name and on y-axis we have count of each attack.

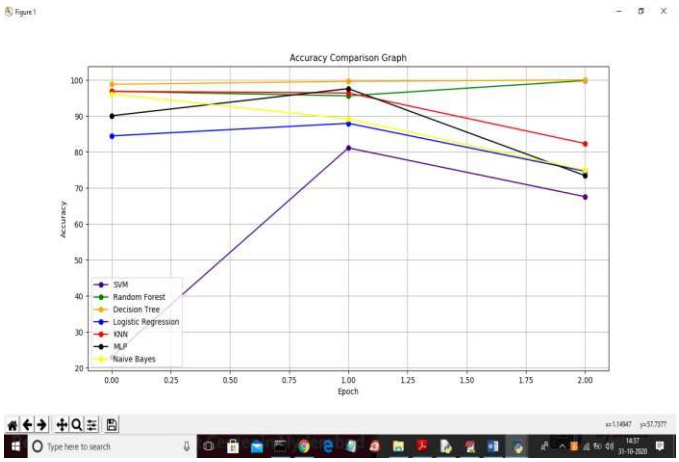

Fig 4: Accuracy graph

In this step, we analyse the performance of each and every algorithm in order to select the most effective classifier for our particular challenge. The decision tree algorithm is demonstrating the best performance across all three data sets, as can be seen in the graph that has just been presented to us.

V. CONCLUSION & FUTURE WORK

The purpose of this essay is to determine which classifier model is the most effective at locating intrusions more quickly and accurately. Following the execution of a number of different classification algorithms on our data sets, we found that the DT and KNN algorithms provided the highest levels of accuracy when compared to the other techniques. However, due to the longer amount of time required to carry out the KNN method, we have decided to go with DT as the best algorithm that is suitable for intrusion detection rather than KNN. Because of this, in our article, we came to the conclusion that the DT algorithm is superior when it comes to the detection of intrusions in IoT devices.

In this post, we will discuss the top seven algorithms that are the most well-known. In the future, we will be able to investigate additional algorithms and determine which ones are most suited for the intrusion detection needs of real-time IoT devices.

REFERENCES

[1]. Atzori, L., Iera, A., Morabito, G. (2010). The Internet of Things: A survey. Computer Network, 54(15): 2787- 2805. https://doi.org/10.1016/j.comnet.2010.05.010

[2]. Weiser, M. (1991). The computer for the 21st century. Scientific American, 265(3): 94-105.

[3]. Leo, M., Battisti, F., Carli, M., Neri, A. (2014). A federated architecture approach for internet of things security. in Euro Med Telco Conference (EMTC), pp. 1- 5. https://doi.org/10.1109/ EMTC. 2014. 6996632

[4]. Sherasiya, T., Upadhyay, H., Patel, H.B. (2016). A survey: Intrusion detection system for Internet of Things. International Journal of Computer Science and Engineering (IJCSE), 5(2): 91-98.

[5]. KDD cup 99 Intrusion detection dataset. http://kdd.ics.uci.edu/databases /kddcup99/ kddcup.data_10_percent.gz, accessed on March 1, 2019.

[6]. [6] Paliwal, S., Gupta, R. (2012). Denial of-service, probing & remote to user (R2L) attack detection using genetic algorithm. International Journal of Computer Applications, 60(19): 57- 62. https://doi.org/10.5120/9813-4306

[7]. [7] N. Chandra Sekhar Reddy, Vemuri P,Govardhan A"An emperical study on support vector machines for intrusion detection"-International Journal of Emerging Trends in Engineering Research (2019)

[8]. Ajmeera Kiran and D. Vasumathi, "A Comprehensive Survey on Privacy Preservation Algorithms in Data Mining", Proceedings of the 2017 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC-2017), 978-1-5090-6621-6/17/$31.00 ©2017 IEEE.

[9]. J. Rajendra Prasad, Avantika Tiwari, O. Venkata Siva† And J. Nageswara Rao, Ajmeera Kiran,"A Comprehensive Study On Normalization Techniquesf Or Privacy Preservation In Data Mining", Journal Of Interconnection Networks ,2141040, World Scientific Publishing Company , Doi: 10.1142/S0219265921410401,2022.

[10]. D Shanthi, N Swapna, Ajmeera Kiran, A Anoosha",Ensemble Approach Of GP,ACOT,PSO,And SNN For Predicting Software Reliability", International Journal Of Engineering Systems Modelling And Simulation , 2022. [11] Raza, S., Wallgren, L., Voigt, T. (2013). SVELTE: Realtime intrusion detection in the Internet of Things. Ad Hoc Networks, 11(8): 2661-2674.

[11]. Summerville, D.H., Zach, K.M., Chen, Y. Ultra-lightweight deep packet anomaly detection for Internet of Things devices. 2015 IEEE 34th International Performance Computing and Communications Conference (IPCCC). https://doi.org/10.1109/PCCC.2015.7410342

[12]. Li, W.C., Yi, P., Wu, Y., Pan, L., Li, J.H. (2014). A new intrusion detection system based on KNN classification algorithm in wireless sensor network. Journal of Electrical and Computer Engineering, 2014: 8 pages, http://dx.doi.org/10.1155/2014/240217

[13]. K. M. Sudar, M. Beulah, P. Deepalakshmi, P. Nagaraj and P. Chinnasamy, "Detection of Distributed Denial of Service Attacks in SDN using Machine learning techniques," *2021 International Conference on Computer Communication and Informatics (ICCCI)*, 2021, pp. 1-5, doi: 10.1109/ICCCI50826.2021.9402517.

[14]. K. M. Sudar, P. Nagaraj, P. Deepalakshmi and P. Chinnasamy, "Analysis of Intruder Detection in Big Data Analytics," *2021 International Conference on Computer Communication and Informatics (ICCCI)*, 2021, pp. 1-5, doi: 10.1109/ICCCI50826.2021.9402402.

[15]. V. Praveena, A. Vijayaraj, P. Chinnasamy, I. Ali, R. Alroobaea et al., "Optimal deep reinforcement learning for intrusion detection in uavs," Computers, Materials & Continua, vol. 70, no.2, pp. 2639–2653, 2022.