ISSN 2278-3091

Volume 12, No.5, September - October 2023

International Journal of Advanced Trends in Computer Science and Engineering

Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse011252023.pdf

https://doi.org/10.30534/ijatcse/2023/011252023

Botnet Threat Intelligence in IoT-Edge Devices

Ahsan Ali[1], Nabeel Aslam[2], Arfan Shahzad[3], Muhammad Junaid Arshad[4]

[1] Department of Computer Science, University of Engineering and Technology, Pakistan, ahsanmsuet@gmail.com

[2] Department of Computer Science, University of Engineering and Technology, Pakistan, nabeelaslam2000@gmail.com

[3] Department of Computer Science, University of Engineering and Technology, Pakistan, arfanskp@gmail.com

[4] Faculty of Computer Science, University of Engineering and Technology, Pakistan, mjunaiduet@gmail.com

Received Date : August 27, 2023 Accepted Date: September 23, 2023 Published Date: October 06, 2023

ABSTRACT

Recently, deep learning has gotten progressively popular in the domain of security. However, Traditional machine learning models are not capable to discover zero-day botnet attacks with extraordinary privacy. For this purpose, researchers have utilized deep learning based computational framework for Botnet which can detect zero-day attacks, achieve data privacy and improve training time using machine learning techniques for the IoT-edge devices. However, it combines and integrates various models and contexts. As a result, the objective of this research was to incorporate the deep learning model which controls different operation of IoT devices and reduce the training time. In deep learning, there are numerous components that aspect the false positive rate of every detected attack type. These elements are F1 score, false-positive rate, and training time; reduce the time of detection, and Accuracy. Bashlite and Mirai are two examples of zero-day botnet attacks that pose a threat to IoT edge devices. The majority of cyber-attacks are executed by malware-infected devices that are remotely controlled by attackers. This malware is often referred to as a bot or botnet, and it enables attackers to control the device and perform malicious actions, such as spamming, stealing sensitive information, and launching DDoS attacks. The model was formulated in Python libraries and subsequently tested on real life data to assess whether the integrated model performs better than its counterparts. The outcomes show that the proposed model performs in a way that is better than existing models i.e. DDL, CDL and LDL as Botnet Attacks Intelligence (BAI) the purposed deep learning model.

Key words: Botnet detection, Deep learning (DL), Deep neural network (DNN), Federated learning

1. INTRODUCTION

IoT-Edge devices, which include a different connected devices such as sensors, cameras, and smart devices, are becoming increasingly ubiquitous in our daily lives. While these devices offer a wide range of benefits, such as increased convenience and efficiency, they also pose a significant are botnets [1]. Botnets are collections of compromised devices that can be remotely managed by an attacker, frequently without the owner's knowledge or agreement [3]. Once a device has been compromised, a variety of criminal actions, including DDoS attacks, spamming, phishing, and crypto currency mining, can be performed on it.

Many of these devices are designed to be low-cost and energy-efficient, which means that they often lack the necessary security features to protect against botnet attacks [2]. To mitigate the risks of botnet attacks on IoT-Edge devices, threat intelligence can play a critical role. This information can then be used to develop proactive strategies and solutions for identifying and mitigating botnet attacks.

For example, threat intelligence can help organizations identify patterns of botnet activity and develop targeted responses to prevent or mitigate attacks [1]. It can also help identify vulnerabilities in IoT-Edge devices and inform the development of more secure devices in the future. In summary, botnets pose a significant threat to IoT-Edge devices, but threat intelligence can play a critical role in mitigating these risks. By providing timely and accurate information about potential threats and vulnerabilities, threat intelligence can help organizations develop proactive strategies and solutions to protect against botnet attacks [17].

It changed the way we communicate with technology in our daily routine. IoT-Edge devices, such as sensors, cameras, and smart home devices, are now an integral part of our homes, workplaces, and public spaces [1]. However, as the number of devices upsurges, so does the risk of cyber threats, particularly botnets. Botnets are collections of compromised devices that a cybercriminal can remotely operate without the owner's knowledge or permission [4]. Botnets can be used to carry out a range of malicious activities, including Distributed Denial of Service attacks, spamming, phishing, and crypto currency mining. IoT-Edge devices are particularly vulnerable to botnet attacks due to their limited processing power, memory, and security mechanisms [3]. To mitigate the risks of botnet attacks on IoT-Edge devices, threat intelligence plays a critical role. Threat intelligence involves collecting, analyzing, and sharing information about potential threats and vulnerabilities [2]. This information can then be used to develop proactive strategies and solutions for identifying and mitigating botnet attacks. In this thesis, we will discuss the importance of botnet threat intelligence in IoT-Edge devices, the challenges and risks associated with botnet attacks, and the strategies and solutions that can be implemented to mitigate these risks [3]. We will also explore the role of technology and innovation in addressing the challenges of botnet attacks on IoT-Edge devices

As continues to expand, the amount of data generated by IoT networks is increasing rapidly. It is projected to reach 70 zettabytes (ZB) by 2025. This data is typically transmitted to server for pre-processing and analysis [1]. To address the issue of botnet attacks in large network data, the method has been widely suggested. This method has demonstrated good classification performance in detecting botnet attacks [5]. Other approaches, such as Deep Reinforcement Learning and Lightweight Dynamic Auto-encoder Network have been projected for detecting network interruption in Wireless Sensor Networks with limited resources [3].

Different Deep Learning (DL) techniques have been suggested in earlier studies as a means of defending communication networks from cyber-attacks. It might be difficult to offload enormous distributed IoT network traffic data to a remote central cloud server for real-time data processing, nevertheless, as IoT networks continue to grow and become more scalable [4]. The CDL technique also needs more time for training, has a lot of communication overhead, and takes up a lot of RAM for data storage [1]. Additionally, because cloud data centers are frequently installed far from where IoT devices are deployed, processing IoT data in real-time has additional hurdles.

Ensuring data privacy protection is a critical concern in the modern world, and violating data privacy regulations can result in significant penalties [2]. Under GDPR, for example, fines for a data privacy breach can be very high. To overcome the difficulties brought on by the challenges of data privacy, high communication costs, big memory space needs, quick training times, and high latency, edge computing and Deep Learning (DL) techniques can be combined [1]. By moving intelligence closer to where data is generated, edge computing can help address these issues.

Localized DL and Distributed DL methods have been proposed as means of achieving edge intelligence without having to aggregate data [3]. However, these methods have shown limited performance in detecting zero-day botnet attacks, There are previously unidentified flaws in IoT systems that hackers use a network of infected computing devices to attack. Lack of prior knowledge regarding the frequency of such attacks is the primary cause of the difficulties in identifying zero-day attacks [1]. The capacity to identify zero-day botnet assaults with a high detection rate and a low false alarm rate is thus necessary for creating an intrusion detection system for IoT edge networks [4].

The BAI approach is what we recommend for identifying zero-day botnet assaults in IoT edge devices. By utilizing the Botnet Attacks Intelligence technique, which enables collaborative deep learning without disclosing private network traffic data to a central cloud server, we hope to allay worries about data privacy. To classify network traffic data, we use DNN architecture, and we apply an algorithm for aggregating updating a local DNN model [2]. Using the Bot-IoT dataset, we assess the BAI method's performance in terms of classification accuracy, precision, recall, and F1 score. To evaluate the BAI method's effectiveness, we compare it to three state-of-the-art DL methods, which are the CDL, LDL, and Distributed DL [3].

To enhance the security of IoT devices, Intrusion Detection Systems (IDS) can be used to detect and respond to potential cyber threats. IDS continuously monitor data streams from various sources and analyze them to detect suspicious activities. Two common approaches to threat detection are signature-based and anomaly-based. A signature-based IDS, also known as a rule-based IDS, matches patterns or signatures against observed events to identify known attacks and report threats [18]. Large data sets are the foundation for artificial intelligence (AI) and machine learning (ML), which poses questions about data privacy and security during collection and storage. However, there is a need to reduce the quantity of data provided in light of the advent of new privacy legislation, such as the ePrivacy Directive and General Data Protection Regulation (GDPR). As a result, efforts have been made to bring AI closer to users, which can also have advantages like lower latency and bandwidth utilization. Tasks like security monitoring can also be completed using AI at the edge of IoT deployments [8], which may not have been appropriate in a shared cloud environment.

The remaining parts of this paper are organized as follows: In Section II, we present the review of related others works, in Section III, we describe the proposed method for zero-day botnet attack detection in IoT-edge devices; in Section IV, we develop models, analyze and compare the effectiveness of the BAI DL models; and in Section V we summaries our results and improvements.

2. LITERATURE REVIEW

Various datasets are available for network, but many of them present challenges such as unreliable labels, limited attack diversity, and outdated scenarios. For example, popular datasets are outdated and do not reflect current attack scenarios. The DEFCON-8 dataset is limited by a small number of benign samples, while the UNIBS dataset focuses only on DoS attacks and lacks labeled features. Meanwhile, the CAIDA and LBNL datasets lack ground truth information about attacks or labeled features [1]. The ISCX and CICIDS2017 datasets were generated using profiling and are complex, and their ground truth information is not available. Botnet scenarios and network data are also underrepresented in existing.

The Bot-IoT dataset was created to give a publically available dataset for network-based botnet attack detection in IoT networks in order to address this issue. This dataset includes both benign and malicious traffic generated by a variety of IoT devices using various communication protocols, including UDP, TCP, ARP, ICMP, IPv6-ICMP, IGMP, and RARP [10]. Millions of IoT botnet attack traffic samples are included in the dataset, which may be divided into four different scenarios: reconnaissance, and information theft [3].

According to your statement, it appears that the authors of a specific study failed to consider the possibility of zero-day vulnerabilities in edge IoT devices, which can be a concern in real-life scenarios due to the unique statistical distribution of training data on each device. Previous research made the assumption that local training data were evenly, independently, and uniformly dispersed among different types of network traffic, but IoT network traffic may not conform to this assumption [2].

The Bot-IoT dataset was created and made available to the public for cyber security research in order to solve this issue [8]. This dataset was produced by creating traffic from gadgets like weather stations, smart fridges, motion-activated lighting, remote-controlled garage doors, and smart thermostats. It includes benign IoT network traffic as well as four botnet attack scenarios, including data theft. The authors suggested a procedure for gathering network packets and removing features from the dataset. [9].

The unsupervised deep learning method that creates a low-dimensional latent-space representation while looking at the dynamic interactions between high-dimensional data components. To represent the long-term linked changes in network traffic properties, the LAE model uses LSTM units, which sets it apart from standard auto encoders [1]. This subsection describes the creation of the LAE approach, which attempts to acquire a low-dimensional latent space feature representation with the least amount of reconstruction error feasible while reducing the feature dimensionality of enormous IoT network traffic data [4].

For spotting assaults from IoT botnets, a deep auto encoder strategy has been adopted. Utilising snapshots of typical IoT device traffic behaviour, statistical features are extracted using this method [2]. Then, for each IoT device, these attributes are used to train deep learning-based auto encoders. For traffic observations, reconstruction error is calculated and compared to a threshold to determine whether it is normal or unusual [6]. A lightweight ensemble of auto encoders deployed on network gateways and routers to detect local network attacks is another method that has been suggested [1].

EDIMA is an architecture designed to detect IoT botnets, and it has a modular structure that comprises several components [6]. One of the crucial modules is the Feature Extractor, which extracts features from the combined gateway traffic. The Traffic Parser/Sub-sampler module organizes the gateway traffic into traffic sessions and can also sub-sample the packet traffic from IoT devices across the devices [4]. The Feature Extractor is then sent this sub-sampled traffic. However, there is a trade-off in terms of detection delay despite the fact that the sub-sampling method reduces storage overhead [8]. The proposed approach involves designing a secure IoT edge computing device based on CPU and FPGA to analyze and summarize traffic in real time. A fast threat situation detection method that uses flow entropy algorithm is deployed on the CPU of this device to generate situation information [16]. The study also develops a machine learning-based strategy for analyzing threat situations that enhances the ad boost algorithm's ability to assess traffic threat levels based on uploaded situational data. The technique then issues the SIE for situation projection, closes the loop on danger situation awareness, and acquires the defensive measure in accordance with threat information. The results of the experiments demonstrate that the suggested approach effectively addresses the recognition recall rate, cleaning success rate, and other indicators while preserving the regular operation of IoT equipment and the capability for second-level early warning..

Malicious and benign gateway traffic are separated into two types. Bot scanning packets are included in malicious traffic, whereas benign traffic does not, and vice versa. The set of ingress/egress packets over a predetermined amount of time at a network interface is referred to as a traffic session and is where the traffic is recorded [19]. The classification algorithm is used to traffic sessions rather than individual packets. This is so because per-packet classification costs more to compute and offers few advantages over per-session classification. Because some payloads could be encrypted, the feature extraction process only extracts features from TCP packet headers. The aggregate traffic classification approach handles encrypted traffic by avoiding the need of payload data [5].

In order to process the results of the feature selection techniques, Bayesian networks (BN) and C4.5 algorithms were used [3]. The authors used the KDD CUP 99 network dataset to analyse the suggested system [9].

Convolutional Neural Network and Long Short-Term Memory (CNN-LSTM), a hybrid deep learning technique, was proposed in this study to detect botnet attacks like BASHLITE and Mirai on nine commercial IoT devices [1]. A genuine N-BaIoT dataset with both benign and malicious patterns was used to assess the suggested system [8]. With accuracies of 90.88% and 88.61% in recognizing botnet attacks from doorbells and an accuracy of 88.53% in doing so for thermostat devices, the trial findings showed the CNN-LSTM model's superiority [7]. With accuracies ranging from 87.19% to 89.64%, the suggested method also demonstrated good accuracy in identifying botnet attacks using security cameras. Overall, the CNN-LSTM model was successful in accurately identifying botnet attacks in Figure 1 from a variety of IoT devices

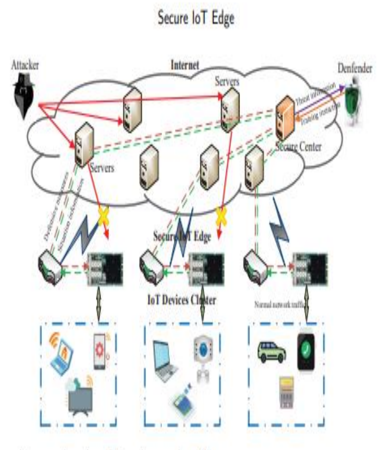


Figure 1: IoT Defense Architecture

Threat situation awareness is an emerging technology that aims to prevent network attacks and maintain equipment security. With the increasing complexity of end equipment services and huge traffic in IoT networks, real-time threat situation awareness based on network traffic can effectively warn and eliminate threat traffic [3]. However, the existing deployment of threat situation awareness is limited to a single location and relies on central nodes for data collection, detection, and cleaning, which can be bandwidth-intensive and not suitable for high-speed scenes. Moreover, the transmission of traffic or log data may compromise privacy and security [10]. This paper proposes architecture for threat situation awareness based on IoT edge and network traffic. The design involves a secure IoT edge computing device based on CPU and FPGA that uses the FPGA pipeline to analyze traffic and generate real-time summaries. The paper also introduces a fast threat situation detection method that uses the flow entropy algorithm to generate situation information [8].

The suggested solution enhances the ad boost algorithm's ability to identify and categories dangers in the traffic by including a machine learning-based threat situation comprehension mechanism. The threat situation awareness closed loop is then completed by the approach by obtaining defensive measures in accordance with threat intelligence and issuing the SIE for situation projection [9]. The suggested method may achieve good performance under various indications while ensuring the normal operation of IoT equipment and offering second-level early warning capability, according to experimental results on KDD and unsw-nb15 public data sets. [10]. additionally, you aim to develop a framework that ensures data privacy and reduces training time while improving classification performance as mentioned in below Figure 2. This plan encompasses important steps towards achieving the goal of detecting botnet attacks using machine learning methods.

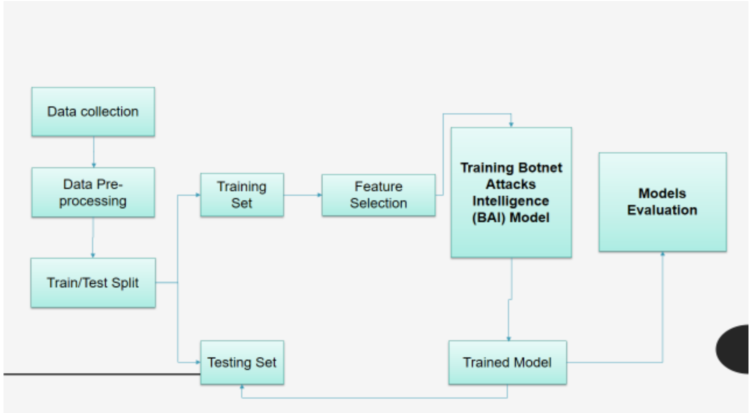


Figure 2: Overview of Research Methodology

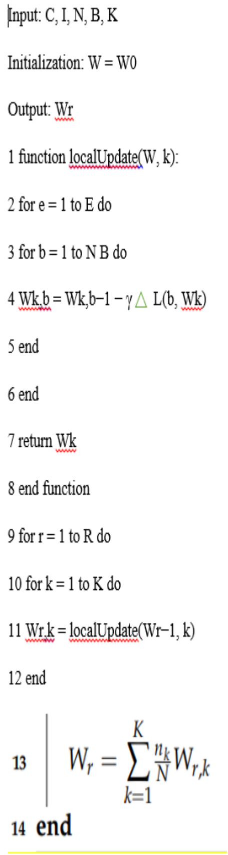
3. PROPOSED METHODOLGY

In our study performing an extensive analysis of the Bot-IoT dataset, applying pre-processing techniques, and utilizing various machine learning algorithms to detect botnet attacks

3.1 Botnet Attacks Intelligence

The BAI strategy makes use of algorithms to detect zero-day botnet assaults on IoT edge devices [14]. It comprises of an edge IoT device and a model parameter server, with the server in charge of organising the training of DNN models on the device. It chooses crucial training parameters like the quantity of epochs, the size of the batch, and the number of communication rounds. On each edge IoT device, a distinct DNN model is trained using local training data. The device transmits its changes to the model parameter server at the conclusion of each epoch for aggregation using the Fed method, which is carried out over several communication rounds. This method has potential for identifying botnet attacks on IoT edge devices [15].

BAI method is proposed to detect zero-day botnet attacks in IoT-enabled critical infrastructure based on Algorithm. The BAI framework comprised of a model parameter server and K IoT edge nodes. Also, it determines the number of training iterations/epochs (I), the batch size of training data (B), and the number of communication rounds (C). In this method, K LAE-BLSTM models are trained separately with local training data that are privately held in K IoT edge nodes. After each training of I epochs, all the edge IoT devices send their local model updates to the model parameter server for aggregation using FedAvg algorithm. Model aggregation is performed by model parameter server in C communication rounds as shown in Figure 3.



```
Input: C, I, N, B, K
Initialization: W = W0
Output: Wr
function localUpdate(W, k):
    for e = 1 to E do
        for b = 1 to N B do
            $Wk,b = Wk,b−1 − γ △ L(b, Wk)$
        end
    end
    return Wk
end function
for r = 1 to R do
    for k = 1 to K do
        $Wr,k = localUpdate(Wr−1, k)$
    end
    $W_r = \sum_{k=1}^{K} \frac{n_k}{N} W_{r,k}$
end
```

Figure 3: BAI Algorithm

3.2 Bot-IoT Dataset

The The Bot-IoT dataset is a useful tool for the community of cyber security researchers. It includes four different botnet attacks, including DoS, DDoS, and data theft, together with harmless IoT network traffic. Several IoT gadgets, including a smart fridge, a weather station, motion-activated lights, a remote-controlled garage door, and a smart thermostat, were responsible for the benign traffic. Tshark4 and Argus5 were employed to collect network packets and extract characteristics. A prior study demonstrated the efficacy of the feature extraction method for classifying multi-class network data. The dataset consists of 2,786,124 samples of botnet attack traffic and 477 samples of benign IoT network traffic. To characterize each network packet's behavior, 43 features were retrieved from the dataset.

In this research, we examine zero-day botnet attack scenarios using the Bot-IoT datasets across four IoT edge devices. These devices have limited computational resources and storage capacity for private network traffic data, which is why such data is stored on a device for simple processing. The study makes use of four distinct IoT edge devices, which are denoted as IoTD1, IoTD2, IoTD3, and IoTD4. The study focused on newer datasets that were recently made available to the scholarly community as defined in Table 1. These updated datasets not only include modern-day attacks, but they're also produced using industry-accepted standards for reliable bot-net detection datasets.

Table 1: Edge Devices Instances

Class	IoTD1	IoTD2	IoTD3	IoTD4
DDoS	25752	1673	0	1673
Dos	15782	89	15782	34683
Normal	12954	12954	54	12954
Reconn	2356	2356	0	93

The Bot-IoT dataset's distribution of training and testing data among IoT edge devices is shown. To test the BAI model's capacity to identify zero-day botnet assaults without jeopardizing data privacy, one class of network traffic was blocked from each IoT edge device. DDoS and reconnaissance attacks were specifically excluded from all of the devices. The training data was purposefully dispersed unevenly among the four IoT edge devices and the four classes to mimic a real-world scenario [20]. For each IoT edge device, a different set of testing data was used to assess the generalization performance of the BAI model.

3.3 Deep Neural Network

Input, hidden, and output are the three layers that make up the DNN model's architecture, and each layer is made up of neurons. The quantity of characteristics in the network traffic training data determines the number of neurons in the input layer. In this work, the input layer had 32 and 103 neurons, respectively, depending on whether the Bot-IoT dataset or the N-BaIoT dataset was used [11]. In most cases, experiments are used to calculate the number of hidden layers and neurons in each layer. While the number of neurons in each layer varied between 15 and 100 at an interval of 15, the number of hidden layers varied from 1 to 5. The BAI method involved sending the training data from each of the IoT edge devices to a central server for aggregation, and then training the BAI model using the combined data in the cloud. Then, using the appropriate testing data, the trained BAI model was delivered back to all of the IoT edge devices for network traffic classification. On the other hand, the LDL method required each IoT edge device to train a different model using local training data [13]. Similar to the DDL technique, local models were trained on IoT edge devices using model parameters, however these parameters were communicated to a model parameter server for aggregation.

.

4. RESULTS AND DISCUSSION

This chapter discusses the outcomes of the deep learning based system and delves into the discussion whether the data manipulations accommodating deep learning models allowed us to improve the precision, accuracy and reduce false rate in edge devices in the security domain by selecting the optimal features. In Particular, this section discusses the evaluation criteria used, the results of the enhanced Botnet attacks intelligence model and discussion of the outcomes. As discussed previously, this study has utilized the Botnet attacks intelligence learning-based system. A deep learning-based model is commonly used for intrusion detection [26]. Specifically, this study focused on the enhancement of this model so that its precision and accuracy can be improved. This enhancement was facilitated through the use of adaptive system, which has been increasingly used by previous researchers for the improvement of IDS. It is a system that enables us to deal with rapid changes in the behavior of attacks and unforeseen circumstances and thus arrive at a better prediction of attacks [12].

4.1 Experiment Setup

Dataset normalization, instance segmentation will be done in python. Deep learning model will also be developed using python along TensorFlow6 and Keras7 frameworks were used for BAI method. The models were trained using the Spyder9 integrated development environment (IDE) with following specifications: random access memory (32 GB), processor (Intel Core i7-9700K CPU @ 3.60 GHz × 8), and 64-bit operating system (OS).

Writing the experimental results of a deep learning model involves presenting the outcomes and performance metrics obtained during the evaluation of the model. Begin by providing a brief overview of the deep learning model you implemented and the purpose of your experiment. Mention the research question or objective your model aimed to address. In second step Dataset Description: Describe the dataset used for training, validation, and testing. Include details such as the size of the dataset, the number of classes (if applicable), and any preprocessing steps applied. In the third phase experimental Setup: Explain the configuration and parameters of your deep learning model. Specify the architecture, including the type and number of layers, activation functions used optimizer, learning rate, batch size, and any other relevant details. Evaluation Metrics: Clearly state the metrics you used to evaluate the performance of your model. Limitations: Acknowledge any limitations or potential sources of bias in your experimental setup. This could include issues like class imbalance in the dataset, lack of certain features, or computational constraints.

When reporting the evaluation results of a deep learning model, it's important to use appropriate metrics that accurately reflect the performance of the model

.

4.2 Classification Metrics

Dataset Accuracy: The proportion of correctly classified instances.

- **Precision**: The ratio of true positives to the sum of true positives and false positives. It measures the model's ability to correctly identify positive instances.

- **Recall** (Sensitivity or True Positive Rate): The ratio of true positives to the sum of true positives and false negatives. It measures the model's ability to identify all positive instances.

- **F1 Score**: The harmonic mean of precision and recall. It provides a balanced measure of precision and recall.

Area under the Receiver Operating Characteristic curve (**AUC-ROC**): It measures the performance across different classification thresholds and provides an aggregated measure of the model's ability to distinguish between classes.

5. CONCLUSION

This thesis reports the development of a deep learning-based system using BAI for network attacks detection on the Bot-Iot dataset. Additionally, the development of a newly created model to solve the classification of attacks is also reported.

In this part, we will conclude our work and provide suggestions for further work. The aim of this study was to integrate the deep learning model with the Botnet Attacks Intelligence to identify the large amount of real-time network intrusions in edge devices and to solve multi-class classification problem. Taking into account a larger number of factors allowed us to increase the level of information considered in the process. Because of the extensive usage of connected devices, security and privacy concerns have becoming increasingly serious.

This increased level ultimately allowed us to improve the accuracy rate and reduce false positive rate of the intrusion system in the context of network based security. The half of the attacks on network-based systems is detected only after they have already affected the system. Therefore, improving the accuracy of the intrusion detection system and reducing false positives is crucial to enhancing the security of these systems. The proposed a Botnet Attacks Intelligence (BAI) method which can detect zero-day botnet attacks, achieve data privacy in IoT-edge devices and improve training time of the model. The performance of the BAI model is compared with three deep learning models CDL, DDL and LDL using the Bot-IoT dataset. The effectiveness of our proposed model (BAI) outperformed all three compared models, the BAI model preserves the privacy and security of network traffic data, involves data aggregation, and it achieved high classification performance. Interestingly, CDL, LDL, and DDL models took a long training time but BAI took only 510 seconds to train the model.

ACKNOWLEDGEMENT

Special thanks to our author Muhammad Junaid Arshad for contributing to this work by performing experiments to validate the accuracy of the system.

REFERENCES

1. S. Popoola, Segun I., Ruth Ande, Bamidele Adebisi, Guan Gui, Mohammad Hammoudeh, and Olamide Jogunola. **Federated deep learning for zero-day botnet attack detection in IoT-edge devices**. *IEEE Internet of Things Journal*, Vol. 9(5), pp. 3930-39445, July 2021
2. Eskandari, Mojtaba, Zaffar Haider Janjua, Massimo Vecchio, and Fabio Antonelli. **Passban IDS: An intelligent anomaly-based intrusion detection system for IoT edge devices,** IEEE *Internet of Things Journal* , vol 7(8), pp. 6882-6897, Jan 2020
3. Sudharsan, Bharath, Dineshkumar Sundaram, Pankesh Patel, John G. Breslin, and Muhammad Intizar Ali. **Edge2guard: Botnet attacks detecting offline models for resource-constrained iot devices**, *IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops),* pp. 680-685, Mar 2021.
4. Zhao, Yuyu, Guang Cheng, Yu Duan, Zhouchao Gu, Yuyang Zhou, and Lu Tang. **Secure IoT edge: Threat situation awareness based on network traffic**, *Computer Networks, vol.* 201, pp. 108525, Dec 2021

5. Wang, Han, Luis Barriga, Arash Vahidi, and Shahid Raza. **Machine learning for security at the iot edge-a feasibility study**. *In 2019 IEEE 16th International Conference on Mobile Ad Hoc and Sensor Systems Workshops (MASSW)*, pp. 7-12, Nov 2019.
6. Kumari, Kimmi, and M. Mrunalini. **Detecting Denial of Service attacks using machine learning algorithms.** *Journal of Big Data, vol* 9(1), pp. 1-17, Dec 2022.
7. Kumar, Ayush, Mrinalini Shridhar, Sahithya Swaminathan, and Teng Joon Lim. **Machine learning-based early detection of IoT botnets using network-edge traffic.** *Computers & Security, vol* 117, pp.102693. Jun 2022
8. Alkahtani, Hasan, and Theyazn HH Aldhyani. **Botnet attack detection by using CNN-LSTM model for Internet of Things applications**. *Security and Communication Networks*: pp. 1-23, Sep 2021
9. Popoola, Segun I., Bamidele Adebisi, Mohammad Hammoudeh, Guan Gui, and Haris Gacanin. **Hybrid deep learning for botnet attack detection in the internet-of-things networks**. *IEEE Internet of Things Journal*, vol 8(6), pp. 4944-4956,Oct 2020.
10. Hosseini, Soodeh, Ali Emamali Nezhad, and Hossein Seilani. **Botnet detection using negative selection algorithm, convolution neural network and classification methods**. *Evolving Systems*, vol 13(1) pp. 101-115, Oct 2022
11. Shareena, Jishma, Aiswarya Ramdas, and Haripriya AP. **Intrusion detection system for iot botnet attacks using deep learning**, *SN Computer Science*, vol. 2(3), pp. 205. May 2021
12. Sattari, Fraidoon, Ashfaq Hussain Farooqi, Zakria Qadir, Basit Raza, Hadi Nazari, and Muhannad Almutiry. **A Hybrid Deep Learning Approach for Bottleneck Detection in IoT**, *IEEE Access*, vol. 10 pp. 77039-77053, July 2022
13. Elsayed, Nelly, Zag ElSayed, and Magdy Bayoumi. **IoT Botnet Detection Using an Economic Deep Learning Model**, *arXiv preprint arXiv,* pp. 2302.02013, Feb 2023.
14. Saad, Sherif, William Briguglio, and Haytham Elmiligi. **The curious case of machine learning in malware detection**, *arXiv preprint arXiv* pp.1905.07573, May 2019.
15. Dietz, Christian, Raphael Labaca Castro, Jessica Steinberger, Cezary Wilczak, Marcel Antzek, Anna Sperotto, and Aiko Pras. **IoT-botnet detection and isolation by access routers**. *In 2018 9th International Conference on the Network of the Future (NOF)*, pp. 88-95. Nov 2018.
16. Anushiya, R., and V. S. Lavanya. **A new deep-learning with swarm based feature selection for intelligent intrusion detection for the Internet of things**. *Measurement: Sensors, vol.* 26, pp. 100700, April 2023
17. Cruz, Antonia Raiane S. Araujo, Rafael L. Gomes, and Marcial P. Fernandez. **An Intelligent Mechanism to Detect Cyberattacks of Mirai Botnet in IoT Networks**. *In 2021 17th International Conference on Distributed Computing in Sensor Systems (DCOSS)*, pp. 236-243, July 2021.
18. Auliar, Rufaida Bibi, and Girish Bekaroo. Security in IoT-based Smart Homes: **A Taxonomy Study of Detection Methods of Mirai Malware and Countermeasures**. *In 2021 International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME)*, pp. 1-6, Oct 2021.
19. Zhao, Binbin, Shouling Ji, Wei-Han Lee, Changting Lin, Haiqin Weng, Jingzheng Wu, Pan Zhou, Liming Fang, and Raheem Beyah. **A large-scale empirical study on the vulnerability of deployed iot devices**. *IEEE Transactions on Dependable and Secure Computing, vol* 19(3), pp. 1826-1840. Nov 2020
20. Hasan, Nasimul, Zhenxiang Chen, Chuan Zhao, Yuhui Zhu, and Cong Liu. **IoT Botnet Detection framework from Network Behavior based on Extreme Learning Machine**, *In IEEE INFOCOM 2022-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, pp. 1-6, May 2022.