International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

Design of a Novel Deep Learning Methodology for IOT Botnet based Attack Detection

Anil Kumar Jakkani[1], Premkumar Reddy[2], Jayesh Jhurani[3]
[1]Assistant Professor, E&TC Dept. ISB&M College of Engineering, Pune
[2]Sr Softwarer engineer, 15950 Paramount way, Frisco Texas, 75189
[3]IT Manager, Cumming, GA
anilkumar.svnit@gmail.com[1], Jakkidiprem@gmail.com[2], Jayesh.jhurani@gmail.com[3]

ABSTRACT:

The hackers take advantage of the rapid expansion of the Internet of Things (IoT) to launch attacks on connected devices. There must be a reliable way to identify hostile attacks in order to lessen difficulties about the security of IoT devices. IoT devices are susceptible to botnet attacks, which are common and very hazardous. Static Internet of Things devices are susceptible to security breaches due to a lack of memory and computation results for a platform. Furthermore, there are a number of ways to find new trends in IoT networks in order to provide security. A Recurrent Neural Network (RNN) based on Bidirectional Long Short-Term Memory (BLSTM) is used to build a detection model using as an innovative Deep Learning application. As soon as it detects text, word embedding turns attack packets into integers via tokenization. We compare the BLSTM-RNN detection model to an LSTM-RNN in terms of accuracy and loss for four different routes used by mirai botnet attacks. While the bidirectional approach reduces the processing time and costs every epoch, the study claims that it eventually becomes the better progressive model.

Index Terms: Deep Learning, Attack, Botnet, RNN, IoT, LSTM.

1. INTRODUCTION

Many sectors, including those dealing with energy, manufacturing, retail, healthcare, and finance, have benefited from the IoT's [1] fast expansion in recent years. There are already twenty billion IoT devices in use around the world. According to BI Intelligence, there will be 55 billion IoT devices and 25 trillion USD invested by 2025 [2]. Security problems have grown as a result of the IoT fast development. Polls carried out by the Eclipse Foundation have shown that developers' main difficulty over the last three years has been the security of the IoT. The distributed denial of service attack ever perpetrated against Dyn occurred on October 21, 2016. Tens of millions of IP addresses, most of which came from Internet of Things devices, were the target of attacks by the Mirai botnet. The publication of the Mirai source code sped up the creation of botnets for the internet of things. There are a plethora of Mirai-based versions, each with an ever-improving set of attack techniques. Satori and IoT Reaper are two of the more well-known examples. Specialists look on IoT botnet detection, monitoring, measurement, prediction, and combat in an effort to avoid future growth and devastation. Current research is focused on detection, which is both the cornerstone and the most crucial part of follow-up studies. The application of machine learning for botnet traffic identification was pioneered by Livadas et al. [3]. The J48 decision tree, Bayesian network, and naive Bayes algorithm were used to distinguish between IRC traffic and non-IRC traffic. Then, regular IRC activity and traffic from botnet controllers were detected. Having said that, these three classifiers did a poor job. False positive rates (FPR) of 10% to 20% and FNRs of 30% to 40% were the best that the Bayesian network could do, despite its top performance. They found that botnet features must be carefully studied for botnet identification to work, and that machine learning alone does not work. Attacks [4], infection, communication with command and control, and dissemination are typical botnet operations. Using the following line of reasoning, we are able to detect Internet of Things botnets in their final stages of operation: a malevolent botnet will launch an attack regardless of its ability to quickly generate new types and display more intricate patterns of behaviour. When the security solution detects botnet attack traffic, it can swiftly deactivate compromised IoT devices from the network to stop the botnet from propagating.

2. LITERATURE REVIEW

In order to protect cyberspace and identify botnet attacks, several researchers have developed certain frameworks.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

Attacks using botnets constitute the bulk of distributed denial of service attacks against IoT devices. One of the most effective ways to prevent unauthorised users from gaining access to your network is via an intrusion detection system. New attack batches could be found by comparing signature attacks using the proposed method. Using anomaly-based and signature-based intrusion detection, unexpected patterns can be extracted from network statistics to identify attacks.

Applications for image identification, geolocation, and extra security were created by Al-Garadi et al. [2] using deep learning. An intrusion detection system for smart cities was developed by Xie et al. [3] using multilayer perceptron (MLP) and short-term memory neural network (LSTMNN) models. Although LSTM-G-NB is able to get the maximum level of accuracy. The SVM, KNN, and NB algorithms were introduced by Alam et al. [4] for the purpose of Internet of Things device classification. Quicker findings are produced via linear discriminant analysis, or LDA. With the use of deep learning and machine learning, we created a system for spotting outliers in this study [5]. In their analysis, the writers considered the pros and cons of popular methods. The security system is about to undergo a paradigm shift thanks to a newly proposed improved technique. One of the ways the engineers intend to enhance the system is by making it better at detecting network attacks. In order to identify malicious attacks on wireless networks, the authors proposed a CNN model [6]. With the fewest false positives and maximum accuracy, these CNN model results are the best available.

Malware on the internet of things Distributed denial of service attacks target Internet of Things devices. These attacks propagate malware since most Internet of Things devices do not have automated updates. Protecting against malware requires an intrusion detection system (IDS). Haddad Pajouh and colleagues [7] used the LSTM classifier to detect malware attacks on IoT infrastructure. One hundred distinct strains of malware were used for practice by the authors. The system's accuracy can go as high as 97%. Deep learning can be able to identify botnet attacks, according to research by McDermott et al. [8]. The Mirai botnet was deemed classified based on the study conducted. To counter botnet attacks, recurrent neural network (RNN) models for bidirectional long short-term memory (BLSTM) were used. The accuracy of BLSTM is 99.98%, whereas that of LSTM is 99.51%. In order to detect attacks, Brun et al. [9] used dense RNN. Attacks like barrage, broadcast, sleep-deprivation, UDP, and TCP SYN flooding can all be detected by this approach. The packets that were recorded are used to obtain the sequence statistics. Several IoT devices were part of a 3G SIM card network that was used for this investigation. Internet of Things devices include things like smoke detectors, security cameras, plugs, thermostats, televisions, and watches. The information gleaned from these packets was used by Meidan et al. [10]. Following its recommendation, the proposed technique has achieved a 94% accuracy rate in detecting unauthorised Internet of Things devices using the random forest tree methodology. Doshi et al. [11] proposed KNN, a Lagrangian support vector machine (LSVM), decision tree (DT), random forest (RF), and neural network (NN), to predict DoS attacks on IoT traffic. Packet size and protocol features are examples of stateless network characteristics, while bandwidth and packet headers—which contain source and destination addresses—are examples of stateful network qualities. In order to detect DDoS and DoS attacks, Hodo et al. [12] used ANN algorithms. Intrusion detection systems that operate on hosts and those that operate on networks formed the basis of these algorithms. An accuracy of 99.4 percent was achieved using the proposed method.

For the goal of anomaly detection, Miedan et al. [13] proposed a deep autoencoder. Considering the N-BaIoT dataset was done. Protecting the configuration of the Internet of Things, the technology averts botnet attacks. The system's skills to detect botnet attacks are remarkable, especially when contrasted with SVM and decision tree algorithms. According to what Haddad Pajouh et al. [14] said, they used an LSTM classifier in IoT applications that were based on ARM. The authors tested the LSTM classifier using 100 samples of malware data that weren't used for training. On average, the proposed model has a 97% accuracy rate.

3. METHODOLOGY

IoT systems are a prime target for attacks such network packets and malware tailored to infiltrate particular IoT devices because of their growing computing and processing power. The proliferation of IoT systems in so many different domains is largely to blame. Low latency, resource specialisation, scattered nature, and mobility are some of the service needs that set Internet of Things attack detection apart from previous systems [15]. For IoT security, this means traditional network attack detection methods will have a harder time keeping up. Most IoT devices were vulnerable to the Mirai and Hajime malware due to default passwords or unpatched vulnerabilities, as found by Kaspersky Lab in 2016 [16].Internet of Things protocols are leading to the development of many zero-day attacks. Since most of these attacks are really smaller versions of larger cyberattacks that have happened before, it is still difficult to detect them, even with advanced computational intelligence like plain old

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

machine learning systems. Despite machine learning's promise to improve security threat hunting, incorporating it into static and dynamic cyber security analysis is currently not feasible due to the widespread use of Internet of Things devices, especially low-cost ones with limited processing power [17]. In contrast, cybersecurity experts are curious about the impact of deep learning (DL) on big data. Computer architecture advancements (like NVIDIA DGX platforms) and new neural network frameworks (like Theano and Tensorflow) have made deep learning more practical. There are now access to massive and diverse training datasets, which has also helped deep learning algorithms. Artificial intelligence (AI) domains that could gain from deep learning (DL) include computer vision, pattern recognition, and image processing. Classification and prediction accuracy could be greatly improved by deep neural networks in challenging problems. Because deep learning compresses information, doesn't need supervised pre-training, and doesn't require human feature engineering, it is viable to utilise it in networks with few resources. In order to identify novel distributed attacks in IoT structures, DL is a great contender because to its self-learning capability, which increases its accuracy and processing speed [18]. Importance of this for IoT security cannot be overstated because these systems are vulnerable to eavesdropping, jamming, spoofing, and resource constraints like out-of-memory accesses and unsafe programming languages.

Using deep learning, this technique detects botnet attacks in the cybersecurity area. Some people have tried to reduce botnet attacks by using machine learning and evolutionary computing. Autonomization of bot roles in operations and the elimination of master-slave interactions are both within the realm of possibility according to swarm intelligence [19]. The ever-changing nature of botnets makes them infamously hard to detect. In order to keep up with botnets' constant evolution, behavioural detection methods have proved useful in uncovering patterns in their life cycle. No bot can receive new orders until it connects to the command and control server. Over time, this link can be recorded to provide data for detection approaches.

Managing massive data sequences is necessary for long-term network traffic observation. The Long Short Term Memory (LSTM) network is one example of a recurrent neural network (RNN) that can identify changing state sequences throughout time. They are able to span long periods of time between important input and the necessary result because of this [19]. A number of fields, including as image recognition, machine translation, and natural language processing, have shown that this structure offers an effective paradigm for tagging tasks [19]. In addition, BLSTMs use two separate layers to store future and previous data contextually [20]. In order to identify botnet attacks, this research adds a new layer to deep learning by using several types of LSTM networks in network traffic analysis.

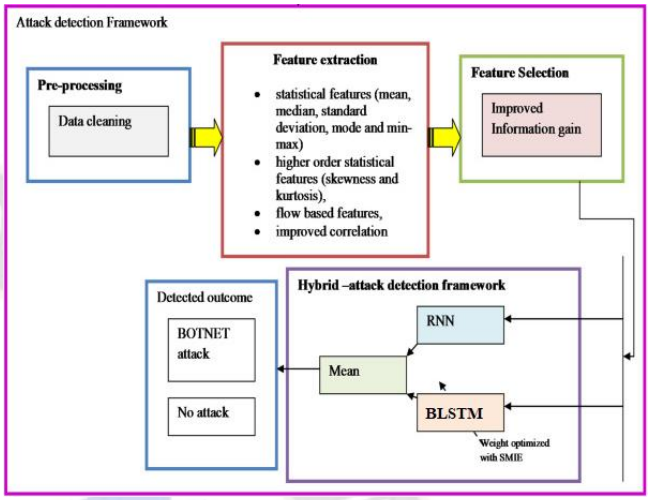

Fig. 1. The Architecture of the Deep Learning Model for Botnet Detection

A description of the botnet's environment and the techniques used to make it reproducible can be found on this page.

A secure sandbox is shown in Figure 1. It was made up of three servers: one for controlling and scanning, one for loading, and one for DNS queries and reporting tools. To facilitate monitoring, it was determined to establish a soft tap (Tap0) SPAN port that would relay all pertinent traffic to a packet sniffer. Two Sricam AP009 IP Cameras running busybox conducted an attack against a Raspberry Pi as its target. The Mirai source code can be obtained from the GitHub repository. To accurately portray a Mirai infection and attack, we made minimal modifications to the source code. However, we had to make a few adjustments to the settings to meet ethical and legal requirements. Figure 2 shows the botnet detection mechanism in action.

TABLE 1. Deep Lerning Model Specifications

Variables	Values
Activation	Sigmoid
Loss	Mean Absolute Error (mae)
Optimiser	Adam
BLSTM layer total units	20
Dense layer total unit	6
Epochs	100

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

Only numerical data can be processed by Artificial Neural Networks (ANNs) and more advanced Recurrent Neural Networks (RNNs), including Long Short-Term Memory (LSTMs). In [20], it was shown that a BLSTM-RNN, which stands for Deep Bidirectional Long Short Term Memory, could improve text recognition. Combining a BLSTM-RNN with Word Embedding allowed the authors of [20] to model and predict sequential text. This made it possible to convert expressions and words into vectors or numerical values.

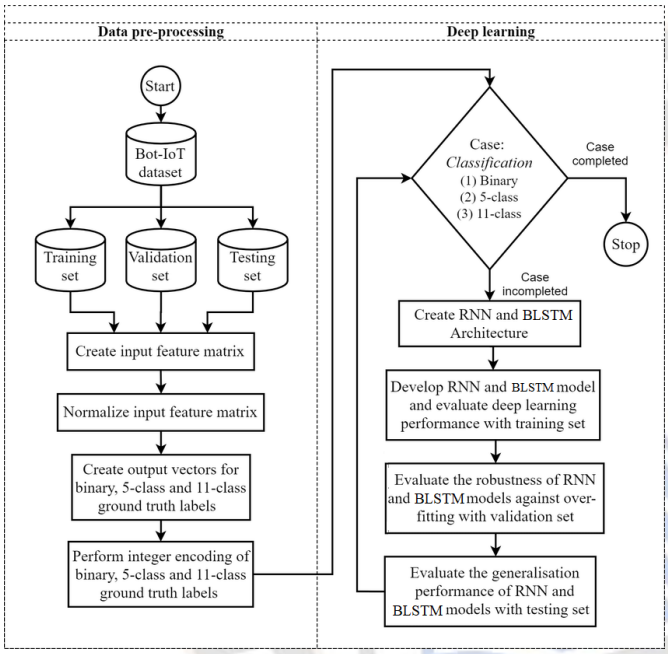

Fig. 2. A Flowchart Showing the Botnet Detection Solution.

TABLE 2. Attack Samples Capture

	Attack	Normal	Mirai	Cleaned
Mirai	0	598676	5102	595478
UDP	9380	587524	2576	601542
ACK	67444	588560	6372	632889
DNS	8706	588410	4408	602496

3.1 LSTM-RNN Modelling

The most significant contribution of this study is the use of deep learning for botnet detection in the Internet of Things. Word embedding was used to convert text to tokenized integers that could be used by deep neural networks. This detection model is tested using LSTM-RNN and BLSTM-RNN against attacks from the Mirai botnet to see how successful it is. Method 1 calls for the use of sigmoid-activated unit and output layers in the construction of detection models. Table 1 shows that the model is created 100 times using the Adam optimiser and the MAE loss function. Figure 1 depicts the proposed detection system that processes botnet data via three stages. To make the data representation more algorithm-friendly, properties are adjusted during preprocessing. Word Embedding is used to tokenize data before normalisation and missing packet removal. The LSTMN-RNN and BLSTMRNN methods are used in the modelling step to construct, train, and assess the detection model. Finally, the Anomaly Detection step assesses the model's accuracy and the impact it has on the constructed dataset.

4. RESULTS

When comparing the various deep learning detection models, we conducted four trials for each of them. We compared it to a bidirectional LSTM-RNN, which can collect contextual information from both the past and the future, in order to see whether or not it could enhance the accuracy or loss metrics of our dataset. This is because unidirectional LSTM-RNN only saves information from the past. In Experiment 1, each sort of attack was split into two categories: train and validate. It was then given to each model, and it was trained via a total of twenty iterations. Table 3 displays the average accuracy and loss metrics for each attack during the course of the attack.

TABLE 3. Detection Accuracy and Loss

	Train	Validate	BLSTM Accuracy	LSTM Accuracy	BLSTM Loss	LSTM Loss
Mirai	387060	208418	99.998992	99.571605	0.000809	0.027775
UDP	391002	210540	98.582144	98.521440	0.125630	0.125667
ACK	411384	221515	93.765198	93.765198	0.858700	0.858773
DNS	391622	210874	98.488289	98.488289	0.116453	0.116453
Mulit-Vector (with ACK)	419887	226094	91.951002	91.951002	0.841303	0.841381
Mulit-Vector (without ACK)	395564	212996	97.521033	97.521033	0.115293	0.115293
Mulit-Vector (with three ACK)	468534	252289	92.243513	92.243513	0.161890	0.242358

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

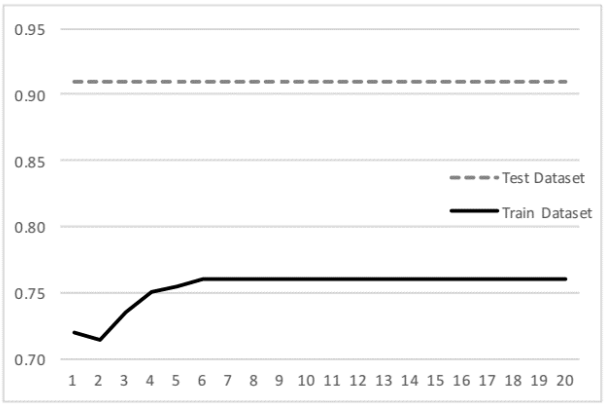

Fig. 3. LSTM Accuracy

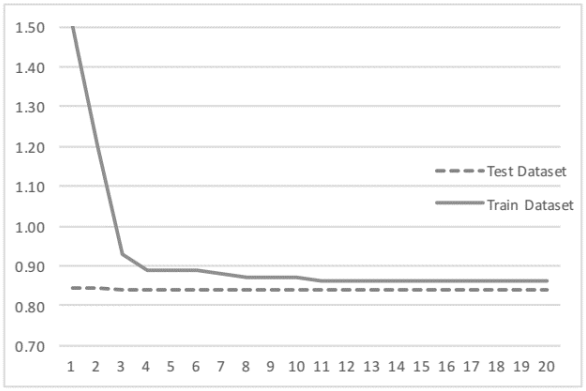

Fig. 4. LSTM Loss

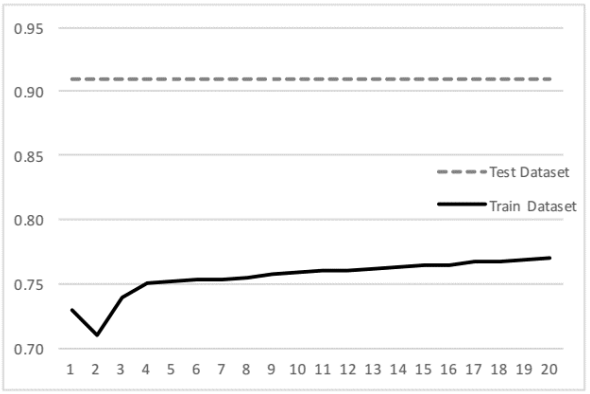

Fig. 5. BLSTM Accuracy

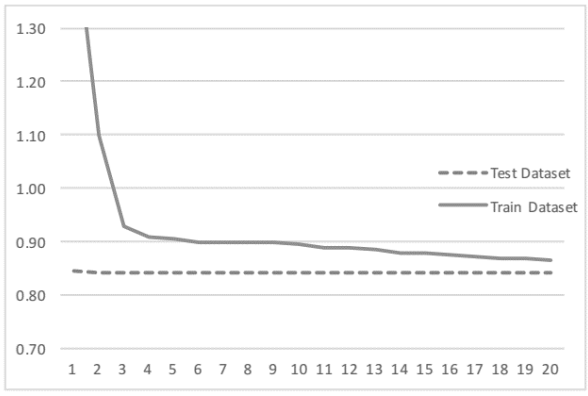

Fig. 6. BLSTM Loss

Experiment was designed to generate a multi-vector attack scenario by combining norm, mirai, udp, dns, and ack captures. This was done in response to the growing prevalence of multi-vector distributed denial of service attacks. Table 3's row 5 illustrates how the ack attack influences the accuracy of detection and the metrics used to measure loss. Experiment created a multi-vector attack scenario without the ack attack by combining norm, mirai, udp, and dns captures. This was done in order to corroborate the findings of the previous experiment. According to the data shown in Row 6 of Table 3, the detection and prediction accuracy of the model are relatively high even when the ack attack is not present. In the fourth experiment, this finding was validated by carrying out three ack attacks simultaneously, so expanding the sample size, with the purpose of evaluating accuracy and forecasting variance. According to Row 7 of Table 3, an increase in the sample size brings the validation accuracy up to 92%, and BLSTMRNN yields the superior loss metric, demonstrating that this model is able to more accurately estimate attack traffic.

The accuracy of the detection model and the loss metrics are shown in Figures 3–(6). Despite the fact that the metric results are comparable and the bidirectional approach adds overhead to each epoch and processing time, the trajectory reveals a more robust progressive model over the course of time. It is possible that the utility of BLSTM-RNN could be shown by a larger dataset that contains more samples.

5. CONCLUSION

Using a Bidirectional Long Short Term Memory Recurrent Neural Network (BLSTM-RNN) and Word Embedding, this study employs deep learning for botnet detection. We tested the BLSTM-RNN against a unidirectional LSTM-RNN to find out whether it improves accuracy or loss metrics for our dataset by using past and future contextual information. With regard to the four attack channels used by the mirai botnet malware, both models exhibit high levels of accuracy with low loss. The validation accuracy of mirai, udp, and dns is 99%, 98%, and 98%, respectively, with validation losses of 0.000809, 0.125630, and 0.116453. Despite the article's

demonstration that a larger sample size could improve accuracy and decrease loss, the ack attack vector metrics were subpar. Our groundbreaking deep learning botnet detection approach for the Internet of Things has been validated by the results. By directing detection to the packet level and using text recognition on often ignored data, we were able to circumvent limitations imposed by flow-based or specification-based detection. The bidirectional approach can increase processing time and costs with each iteration, but it seems to be the better progressive model in the long run.

There have been several avenues of investigation. We will begin by creating a second dataset that includes all 10 attack channels used by the Mirai botnet malware. By modifying the mirai source code, we will create a third dataset and compare our model against signature and flow-based anomaly detection methods. This will demonstrate that our model is capable of identifying new botnet variations. Next, we'll look at ways to improve the situational awareness of IoT botnets once we've solved the detection difficulty. We want people to be more aware of the dangers of contaminated gadgets so they can make better choices when buying and using them.

REFERENCES

[1]. Alshamkhany, Mustafa, et al. "Botnet attack detection using machine learning." 2020 14th International Conference on Innovations in Information Technology (IIT). IEEE, 2020.
[2]. Ullah, Imtiaz, Ayaz Ullah, and Mazhar Sajjad. "Towards a hybrid deep learning model for anomalous activities detection in internet of things networks." IoT 2.3 (2021): 428-448.
[3]. Popoola, Segun I., et al. "Federated deep learning for zero-day botnet attack detection in IoT-edge devices." IEEE Internet of Things Journal 9.5 (2021): 3930-3944.
[4]. Wazzan, Majda, et al. "Internet of Things botnet detection approaches: Analysis and recommendations for future research." Applied Sciences 11.12 (2021): 5713.
[5]. Wei, Chongbo, Gaogang Xie, and Zulong Diao. "A lightweight deep learning framework for botnet detecting at the IoT edge." Computers & Security (2023): 103195.
[6]. Qureshi, Sirajuddin, et al. "A hybrid DL-based detection mechanism for cyber threats in secure networks." IEEE Access 9 (2021): 73938-73947.
[7]. Alkhudaydi, Omar Azib, Moez Krichen, and Ans D. Alghamdi. "A deep learning methodology for predicting cybersecurity attacks on the internet of things." Information 14.10 (2023): 550.
[8]. Alharbi, Abdullah, et al. "Botnet attack detection using local global best bat algorithm for industrial internet of things." Electronics 10.11 (2021): 1341.
[9]. Shafiq, Muhammad, et al. "Selection of effective machine learning algorithm and Bot-IoT attacks traffic identification for internet of things in smart city." Future Generation Computer Systems 107 (2020): 433-442.
[10]. Dong, Xudong, et al. "BotDetector: An extreme learning machine-based Internet of Things botnet detection model." Transactions on Emerging Telecommunications Technologies 32.5 (2021): e3999.
[11]. Li, Yuxi, et al. "Deep learning in security of internet of things." IEEE Internet of Things Journal 9.22 (2021): 22133-22146.
[12]. Samy, Ahmed, Haining Yu, and Hongli Zhang. "Fog-based attack detection framework for internet of things using deep learning." IEEE Access 8 (2020): 74571-74585.
[13]. Jayalaxmi, P. L. S., et al. "DeBot: A deep learning-based model for bot detection in industrial internet-of-things." Computers and Electrical Engineering 102 (2022): 108214.
[14]. Shafiq, Muhammad, et al. "CorrAUC: A malicious bot-IoT traffic detection method in IoT network using machine-learning techniques." IEEE Internet of Things Journal 8.5 (2020): 3242-3254.
[15]. Popoola, Segun I., et al. "Memory-efficient deep learning for botnet attack detection in IoT networks." Electronics 10.9 (2021): 1104.
[16]. Alothman, Zainab, Mouhammd Alkasassbeh, and Sherenaz Al-Haj Baddar. "An efficient approach to detect IoT botnet attacks using machine learning." Journal of High Speed Networks 26.3 (2020): 241-254.
[17]. Popoola, Segun I., et al. "Hybrid deep learning for botnet attack detection in the internet-of-things networks." IEEE Internet of Things Journal 8.6 (2020): 4944-4956.
[18]. Soe, Yan Naung, et al. "Machine learning-based IoT-botnet attack detection with sequential architecture." Sensors 20.16 (2020): 4372.
[19]. Hasan, Tooba, et al. "Securing industrial internet of things against botnet attacks using hybrid deep learning approach." IEEE Transactions on Network Science and Engineering (2022).
[20]. Alzahrani, Mohammed Y., and Alwi M. Bamhdi. "Hybrid deep-learning model to detect botnet attacks over internet of things environments." Soft Computing 26.16 (2022): 7721-7735.