Survey of Botnet Detection Techniques using Deep Learning in the IoT Environment

Laila Al-Qaisi
InterNetWorks Research Lab
Universiti Utara Malaysia
06010 UUM Sintok, Kedah, Malaysia
layla_mohammad@ahsgs.uum.my

Suhaidi Hassan
InterNetWorks Research Lab
Universiti Utara Malaysia
06010 UUM Sintok, Kedah, Malaysia
suhaidi@uum.edu.my

Abstract— **The steady growth in the adoption of IoT devices in various aspects of life poses serious challenges to network security. Many previous works indicate that botnets form threats. This is because they can be used to detect and exploit IoT devices' vulnerabilities to attack them. Those works also, outline the use of various techniques for detecting botnets. This paper surveys the use of Deep Learning (DL) techniques for detecting botnets in the IoT environment. An extensive literature search was conducted on various online databases, then findings were filtered by reviewing abstracts, introduction, and conclusion. A summary for a sample of recent research papers is presented to simplify future work. This work is important to assist network security researchers to have an initial insight on various DL-based detection techniques for botnets in the IoT environment.**

Keywords— Network security, Botmaster, Intrusion detection, Systematic literature review, Data mining

I. INTRODUCTION

Internet of Things IoT is defined by [1] as a network which connects devices to facilitate information exchange, improve computational abilities and communication as well as enhancing sense. It is used to conduct human-to-things and things-to-things communication.

Security is considered the main challenge for an IoT environment and it has been a hot topic for around a decade now. IoT network includes various heterogeneous types of devices, it may include low-cost ones with no security measures to protect them. Moreover, most of them save passwords and credentials by default. Yet, these reasons and more make IoT devices vulnerable to an attack.

Botnets are an example of the major threats that may be faced in IoT environment and most security attacks were botnet-based attacks.

Anomaly detection is one of the popular solutions to catch security attacks. They are defined as software that is used to monitor the data flow within a network and capture whether it includes any unfamiliar or malicious pattern. Basically, it has been used and studied through the literature on various kinds of networks and using different algorithms.

This paper will present a survey of botnet detection techniques using deep learning in an IoT environment. Starting with botnets definition including stages and structure. Followed by a discussion on detection techniques along with a suitable taxonomy for botnet detection in an IoT environment. Afterward, deep learning techniques are defined and explained. Finally, a summary of the most recent studies about 'botnet detection techniques using deep learning in the IoT environment" is presented. The remainder of this paper is organized as follows: Section 2 defines and explains Botnets in an IoT. Then, Section 3 defines and discusses techniques used in anomaly detection in IoT environment. Afterward, Section 4 summarizes researches that used Deep Learning as a Botnet detection technique.

II. BOTNETS

A. Definition

The botnet is a term that consists of two words, which are: Robot and Network. Being a top researched topic, various definitions were presented through the literature. The following table summarizes some of these definitions:

TABLE I. BOTNET DEFINITIONS FROM PREVIOUS STUDIES

Ref	Definition
[1]	A connected group of computers and devices and work cooperatively to run malicious activities to corrupt the victim
[2]	Number of infected hosts called bots, which is controlled by a human operator called Botmaster
[3]	System of customized computers controlled remotely by a botmaster. A botnet can execute various noxious activities, for example, phishing, spam messages, Distributed Denial of Service DDoS, and spreading malicious programming.
[4]	A network of infected end-hosts called bots are controlled by a human who is called botmaster and used to exploit other hosts vulnerabilities.

B. Botnet Stages

A botnet goes through three main stages as explained by [2] which can be summarized as follows:

1) Infection: use malware to attack new hosts and recruit them as new members of the bot. this may be performed through several methods such as; unreliable downloads, exploit the vulnerability, untrusted mail… etc after being infected, the host becomes part of BOTNET.

2) Command and Control: once infected the botmaster communicates with the host via commands.

3) Malicious Activities: Execution of attacks such as DDOS, spam, and information theft.

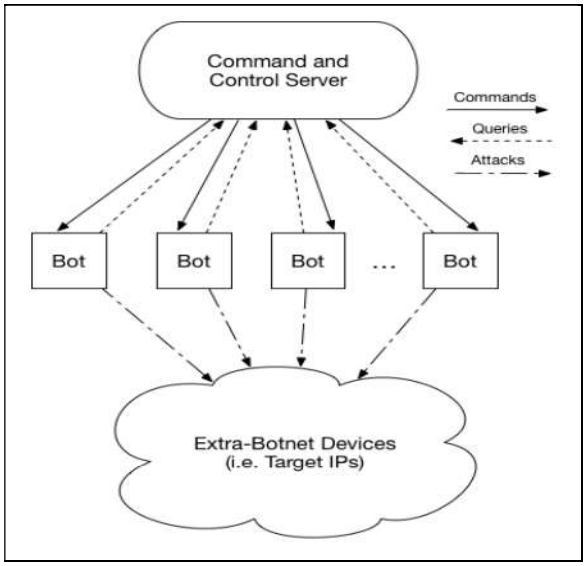

Fig. 12. Botnet Structure

Fig. 1 shows what exactly happens in botnet stages. For building a botnet, infected devices are highly needed or as they are called "bots". The more bots you add, the bigger the botnet becomes, and the higher the impact you get. So, the size really matters for committing the cyber-crime which is mainly targeting financial benefit. [6]

C. Botnet As A Threat

Like worms and viruses, bots are programs that are used to exploit vulnerable hosts and expand their reach. Afterward, recruit as much as possible of connected devices. In the current stage of the IoT environment around us and living in a world that is described as "computers everywhere" and these computers are all day connected. This increases the chance of being attacked. Statistics showed that in 2008, spam emails were generated by 6 botnets [7]. 16-25% of computers connected to the internet in 2013 were part of the botnet [8]. According to Spamhaus Malware Labs, 10,263 botnets hosted on 1,121 different networks in 2018 were identified and blocked. That is an 8% increase from the number of botnet C&C in 2017 [9].

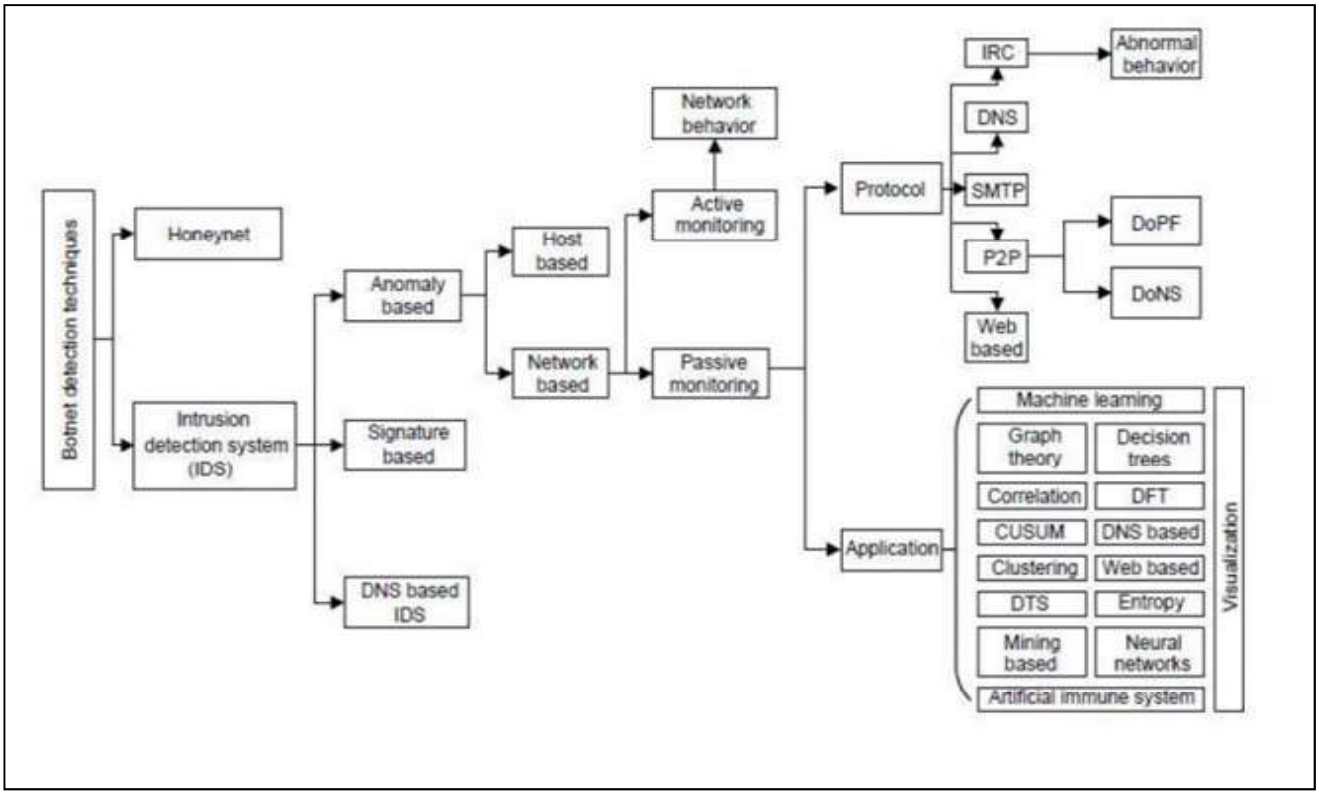

Fig. 13. Botnet Detection Technique Taxonomy, [10].

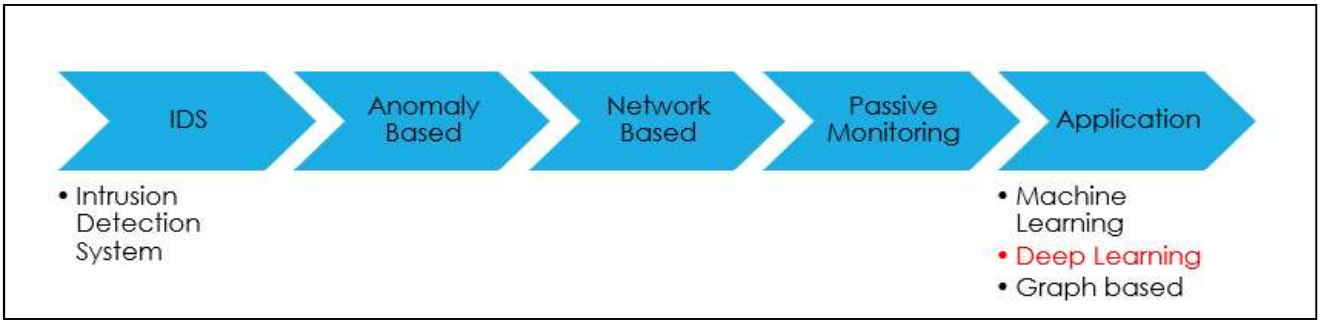

Fig. 14. Derived Botnet Detection Techniques Taxonomy

III. Detection Techniques

Many researchers had taken botnet detection and monitoring as a problem that needs extensive investigation. Especially when IoT environments were introduced and become real-life situations, increased security and privacy made it even more important. The field of "Botnet detection" has been studied thoroughly for the last decade in literature. Researchers have used different approaches and studied the topic in various aspects.

Following is the taxonomy of botnet detection techniques proposed by [10], which shows major specifications used by researchers to study Botnets.

Based on Fig. 2, a derived criterion to survey botnet detection techniques is illustrated as shown in Fig. 3.

A. Intrusion Detection Systems (IDS)

IDS have been widely studied and within different types of applications such as networks, clouds, and IoT environments. Basically, their main goal is to catch any abnormal data flow and report the managing website. IDS are categorized into signature-based, anomaly-based, and DNS-based IDSs [11]. The benefits of using IDS may be summarized to a feature that is included in these systems to have the ability to save signatures of recognized botnets. However, the disadvantages are; first, the low refresh rate of a signature update may result in not detecting anomalies as required. Second, frequent refresh for the signature repository is highly needed to be able to detect freshly launched botnets. [12]

B. Anomaly Based Detection

IDS work here based on guidelines already saved within the system. These guidelines help in classifying data into "normal" or "abnormal" and require further investigation. IDS is usually used to maintain IoT environment security. This environment consists of a network of connected devices and IDS is responsible for analyzing network traffic to catch attacks and malicious activities. Afterward, in case of a truly identified attack, a message is sent to the decision-making system as a warning for action-taking purposes. These IDSs were categorized in terms of detection technique used into several groups, such as statistical-based, machine learning, and data mining-based, rule-based…etc. [13]

C. Data Mining and Machine Learning

In IoT IDS, there is an orientation towards using data mining and machine learning techniques as [1] stated. Data mining is well known as the process of extracting knowledge from enormous data stored in data warehouses and information repositories. Also, this process is not aiming only to classify currently stored data efficiently, but also to generalize rules to classify new data. [14] Nevertheless, IoT data described as high-dimensional data, and the process of analyzing it, to detect anomalies, is complex and will require a massive amount of training data. This was solved by introducing the Feature selection (FS) process to reduce the number of features that represent this data, which may be hundreds to thousands of features. Such numbers may also affect the classification negatively as they may include noise, redundant, or unimportant features. This curse of dimensionality along with other reasons such as the increased complexity of cyber-attacks helped in changing the tendency to use deep learning (DL) [15]

D. Deep Learning (DL)

DL is defined as a branch of Machine Learning (ML) that has three types of techniques, namely, supervised, semi-supervised and unsupervised learning. DL Uses Multi-Layers of Artificial Neural Networks (ANN) check Fig. 4, and each layer has activation functions included which give non-linear output out of raw input. Usually, the more layers added, the deeper the model and the higher the performance. The whole concept is said to be inspired by human brain functionality. [16, 17]

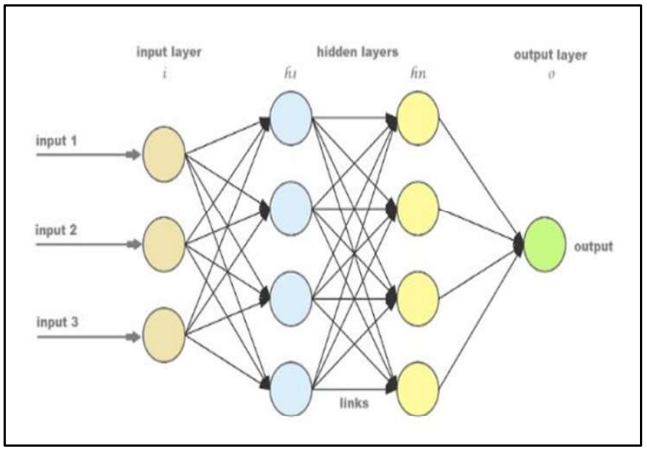

Fig. 15. ANN Architecture

Recently DL has gained attention more than traditional ML approaches. This is due to being able to learn more features, reduce the complexity of training models, higher accuracy, and capability of dealing with huge datasets as explained in the previous section about the curse of dimensionality. [18-21]

ANN is considered a useful and applicable approach after the enhancement of Convolutional Neural Network (CNN) and Recurrent Neural Network (RNN). CNN is usually used with multi-dimensional arrays of data as an input to manipulate their hidden properties and they include three layers: convolution, pooling, and fully connected layers. While RNN is used to deal with sequential information and they get the name recurrent from the fact that they execute the same function for each element in the sequence and output is generated depending on the previous computations. [22,23]

DL approaches are being applied in a wide range of fields and topics currently such as e-commerce, image processing, cybersecurity, speech recognition, language translation, and sentiment analysis. Nevertheless, cybersecurity and more specifically anomaly detection will be studied in detail in the following section.

IV. Methodology

This study employed the systematic literature review guidelines and standards proposed by [24]. This consists of a set of well-defined stages conducted in line with a predefined protocol. SLR consists of three phases: planning, conducting, and reporting the reviews according to [24]. These phases consist of the following processes: (1) identifying RQs; (2) developing a review protocol; (3) determining both exclusion

and inclusion criteria; (4) selecting search strategy and study process; (5) quality assessment (QA); and (6) extracting and synthesizing data.

A. Identifying Research Questions (RQs)

To achieve the main objectives of this study, we propose three key research questions:

- RQ1: What is the designed taxonomy and framework for Botnet detection techniques in IoT?
- RQ2: What are Botnet detection techniques that have been used in IoT?
- RQ3: What are the results of applying DL for Botnet detection in IoT?

B. Developing a Review Protocol

The review protocol considered a vital step in SLR, because it decreases study bias and differentiates SLR from traditional methods of reviewing the literature. Our protocol categorizes the review background, search strategy, development of RQs, extraction of data, criteria for study selection, and data synthesis.

C. Search Strategy

An extensive search was conducted through E-digital resources and online databases such as Scopus and science direct and only high-impact-factor publications were selected.

The main keywords included for the search were "botnet detection techniques, botnet detection using deep learning, deep learning for IoT botnet detection".

D. Criteria for Inclusion and Exclusion Articles

After getting results only publications of the years 2018, 2019 and 2020 were selected for the review process and the rest were excluded. For instance, results registered 49 research papers published in Scopus for 2020 only and 214 in Science Direct for the same year and topic. Afterward, a filtration process is applied by reviewing the title, abstract, and conclusion to get the most relevant of these found papers and table 2 summarizes some of the findings sorted by year of publication. While the next section summarizes a sample of selected studies published in 2020.

V. Summary of Botnet Detection Techniques Using Deep Learning in the IoT Environment

Major studies that were conducted in 2020 were, [1] Presented two-levels DL botnet detection system using DNS queries. The system can handle big data in real-time. The first level used Siamese Networks to get the similarity score and dissimilar s are passed to the second level which used DL for detection and classification.

While [25] proposed Particle Deep Framework (PDF) for botnet detection which included three main functions. First, extract network flow then verify integrity especially for encrypted networks. Second, optimize DL parameters using the PSO algorithm. Third, (MLP) neural network is used to detect and trace abnormal events.

Another study [30] developed a multiclassification NN based model that focused on aiming at fast training, real-time detection, and higher accuracy. FastGRNN is the proposed model that used RNN as a DL algorithm it outperformed other models that applied the same benchmarked datasets.

Another DL botnet detection model was introduced to achieve zero-day botnet attacks by [34]. The proposed DNN and feed-forward backpropagation ANN techniques were found to have the best performance with 99.6% accuracy when compared with SVM, NB, or backpropagation algorithms for the same benchmark dataset.

Furthermore, a study by [36] used a hybrid PSO algorithm along with a voting system called (BD-PSO-V) first to select outstanding features of detecting botnets. Then, a deep neural network algorithm, support vector machine (SVM), and decision tree C4.5 were included in the voting system to identify and detect botnets effectively. BD-PSO-V simulation results were promising and registered a performance improvement in terms of accuracy for both used benchmarked datasets.

Moreover, a study conducted by [40] discussed the experiment of using DL RNN and LSTM in botnet detection then compared the results with ML algorithms, namely; SVM (Support Vector Machine), LR (Linear Regression), and KNN (K-Nearest Neighbors) in terms of accuracy for the same benchmarked dataset. The proposed model results were 99% accuracy and 100% precision with an effective recall and f1-score value of 99.8%. This was proved to be outperforming SVM, LR, and KNN.

Finally, [41] proposed an ML botnet detection system with sequential architecture, along with a feature selection approach to achieve high performance, ML algorithms were (ANN), J48 decision tree, and Naïve Bayes and detection performance was 99% as experiments showed.

VI. Conclusion

This paper introduced botnets and detection techniques taxonomies studied in the literature. Also, derived a taxonomy that is followed for this survey to focus on detection techniques used for botnets in the IoT environment. Furthermore, introduced Deep Learning and reasons for orienting research recently to it. Moreover, SLR is applied to specify current stage of Deep Learning techniques exploited in detecting botnets in IoT. Papers published between 2018 and 2020 were selected for intensive study as discussed in methodology. As a result, a list of most relevant research papers proposing DL and applying it in detecting botnets is summarized in Table 2 including the major information required about each one. Finally, it was found that various types of DL algorithms have been applied, improved, and then studied thoroughly in the literature to solve the problem of detecting botnets. These DL algorithms were found to record high accuracy when compared with traditional ML algorithms.

Ref	Paper Information					
	Year	*Type*	*Methodology*	*Taxonomy*	*Dataset*	*Performance Measure*
[23]	2018	Journal	combination of convolutional and recurrent neural network	Classification	CTU-13 and ISOT	Accuracy: 99.3% F-measure: 99.1%
[26]	2018	Journal	LSTM Recurrent Network	Classification	CTU	Precision:81.26%,Recall: 99.34% F1-score: 89.40%
[27]	2018	Journal	Deep Learning Neural Network	Classification	CTU-13 and ISOT	Accuracy: 99%
[33]	2018	Conference	Multi-layer Perceptron (MLP) neural network	Classification	HogZilla	Accuracy: 96%
[24]	2019	Conference	Long Short-Term Memory (LSTM)	Classification	CICIDS 2017	Precision:99.95% Recall: 99.97 % F1-score: 99.91 %
[38]	2019	Journal	Convolutional Neural Network (CNN)	Classification	USTC-TFC 2016	Accuracy: 100%
[1]	2020	Journal	Siamese neural network (sometimes called Twin NN)	Classification	DMD-2018	Accuracy: 89.9% F1-score: 91.9%
[41]	2020	Journal	Artificial Neural Network (ANN)	Classification	N-BaIoT	Accuracy: 99%
[25]	2020	Journal	Particle Swarm Optimizer based Multi-layer Perceptron (MLP) neural network	Classification	Bot-IoT and UNSW_NB15	Accuracy: 99%
[28]	2020	Conference	Self-Organizing Map (SOM)	Classification	Kaggle	Highest accuracy
[30]	2020	Journal	Fast, accurate, stable, and tiny gated recurrent neural network (FastGRNN)	Classification	MedBIoT and Mirai-RGU	F1-score:99.99%, 99.04%
[31]	2020	Journal	Vector Convolutional Neural Network (VCDL)	Classification	UNSW's Bot-IoT	Accuracy:99.74% Precision:99.99% Recall: 99.75 %
[32]	2020	Journal	Extreme learning machine (ELM) which has been developed for Single Hidden Layer Feedforward Neural Networks (SLFNs)	Classification	ISCX-Bot-2014	Accuracy:98.67%
[34]	2020	Journal	DNN and feed-forward backpropagation ANN	Classification	CTU-13	Accuracy:99.2%
[35]	2020	Journal	hybrid of LSTM and RNN	Classification	MCFP	Accuracy:99.36% Precision:97.97% Recall: 98.86 %
[36]	2020	Journal	BD-PSO-V system, which is a combination of PSO and X-means algorithms and machine learning methods, i.e. **Deep Neural Network,** SVMLib, and C4.5 decision tree	Classification	ISOT and Bot-IoT	Accuracy:99.88%, 99.64%
[37]	2020	Journal	Distributed Convolutional Neural Network (DCNN) and Long-Short Term Memory (LSTM) network	Classification	N_BaIoT	Accuracy:94.80%
[39]	2020	Journal	Recurrent Neural Network (RNN) and Long Short-Term Memory (LSTM)	Feature Analysis	N_BaIoT	Accuracy:96%, 100%
[40]	2020	Journal	Recurrent Neural Network (RNN) and Long Short-Term Memory (LSTM)	Classification	UNSW-NB15	Accuracy: 99%

REFERENCES

[23] Vinayakumar, R., Alazab, M., Srinivasan, S., Pham, Q.V., Padannayil, S.K. and Simran, K., 2020. A visualized botnet detection system based deep learning for the Internet of Things networks of smart cities. IEEE Transactions on Industry Applications.

[24] Beltrán-García, P., Aguirre-Anaya, E., Escamilla-Ambrosio, P.J. and Acosta-Bermejo, R., 2019, November. IoT Botnets. In International Congress of Telematics and Computing (pp. 247-257). Springer, Cham.

[25] Khan, R.U., Zhang, X., Kumar, R., Sharif, A., Golilarz, N.A. and Alazab, M., 2019. An adaptive multi-layer botnet detection technique using machine learning classifiers. Applied Sciences, 9(11), p.2375.

[26] Alieyan, K., Almomani, A., Abdullah, R., Almutairi, B. and Alauthman, M., 2020. Botnet and Internet of Things (IoTs): A Definition, Taxonomy, Challenges, and Future Directions. In Security, Privacy, and Forensics Issues in Big Data (pp. 304-316). IGI Global.

[27] Habib, M., Aljarah, I., Faris, H. and Mirjalili, S., 2020. Multi-objective Particle Swarm Optimization for Botnet Detection in Internet of Things. In Evolutionary Machine Learning Techniques (pp. 203-229). Springer, Singapore.

[28] Habib, M., Aljarah, I. and Faris, H., 2020. A Modified Multi-objective Particle Swarm Optimizer-Based Lévy Flight: An Approach Toward Intrusion Detection in Internet of Things. ARABIAN JOURNAL FOR SCIENCE AND ENGINEERING.

[29] AsSadhan, B., Moura, J.M., Lapsley, D., Jones, C. and Strayer, W.T., 2009, July. Detecting botnets using command and control traffic. In 2009 Eighth IEEE International Symposium on Network Computing and Applications (pp. 156-162). IEEE.

[30] Silva, S.S., Silva, R.M., Pinto, R.C. and Salles, R.M., 2013. Botnets: A survey. Computer Networks, 57(2), pp.378-403.

[31] Spamhaus Malware Labs: Spamhaus Botnet Threat Report 2019, pp. 1–15 (2018)

[32] Karim, A., Salleh, R.B., Shiraz, M., Shah, S.A.A., Awan, I. and Anuar, N.B., 2014. Botnet detection techniques: review, future trends, and issues. Journal of Zhejiang University SCIENCE C, 15(11), pp.943-983.

[33] Stalmans, E. and Irwin, B., 2011, August. A framework for DNS based detection and mitigation of malware infections on a network. In 2011 Information Security for South Africa (pp. 1-8). IEEE.

[34] Kugisaki, Y., Kasahara, Y., Hori, Y. and Sakurai, K., 2007, October. Bot detection based on traffic analysis. In The 2007 International Conference on Intelligent Pervasive Computing (IPC 2007) (pp. 303-306). IEEE.

[35] Elrawy, M.F., Awad, A.I. and Hamed, H.F., 2018. Intrusion detection systems for IoT-based smart environments: a survey. Journal of Cloud Computing, 7(1), p.21.

[36] Tan, P.N., Steinbach, M. and Kumar, V., 2005. Introduction to data mining. 1st.

[37] Qiao, W., Tian, W., Tian, Y., Yang, Q., Wang, Y. and Zhang, J., 2019. The forecasting of PM2. 5 using a hybrid model based on wavelet transform and an improved deep learning algorithm. IEEE Access, 7, pp.142814-142825.

[38] Zhou, Y., Han, M., Liu, L., He, J.S. and Wang, Y., 2018, April. Deep learning approach for cyberattack detection. In IEEE INFOCOM 2018-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS) (pp. 262-267). IEEE.

[39] Wang, C., Dong, S., Zhao, X., Papanastasiou, G., Zhang, H. and Yang, G., 2019. Saliencygan: Deep learning semisupervised salient object detection in the fog of iot. IEEE Transactions on Industrial Informatics, 16(4), pp.2667-2676.

[40] Guo, Y., Liu, Y., Oerlemans, A., Lao, S., Wu, S. and Lew, M.S., 2016. Deep learning for visual understanding: A review. Neurocomputing, 187, pp.27-48.

[41] Papernot, N., McDaniel, P., Jha, S., Fredrikson, M., Celik, Z.B. and Swami, A., 2016, March. The limitations of deep learning in adversarial settings. In 2016 IEEE European symposium on security and privacy (EuroS&P) (pp. 372-387). IEEE.

[42] Shokri, R. and Shmatikov, V., 2015, October. Privacy-preserving deep learning. In Proceedings of the 22nd ACM SIGSAC conference on computer and communications security (pp. 1310-1321).

[43] Wang, J., Chen, Y., Hao, S., Peng, X. and Hu, L., 2019. Deep learning for sensor-based activity recognition: A survey. Pattern Recognition Letters, 119, pp.3-11.

[44] Amanullah, M.A., Habeeb, R.A.A., Nasaruddin, F.H., Gani, A., Ahmed, E., Nainar, A.S.M., Akim, N.M. and Imran, M., 2020. Deep learning and big data technologies for IoT security. Computer Communications, 151, pp.495-517.

[45] Pektaş, A. and Acarman, T., 2019. Deep learning to detect botnet via network flow summaries. Neural Computing and Applications, 31(11), pp.8021-8033.

[46] Liang, X. and Znati, T., 2019, December. A Long Short-Term Memory Enabled Framework for DDoS Detection. In 2019 IEEE Global Communications Conference (GLOBECOM) (pp. 1-6). IEEE

[47] Koroniotis, N., Moustafa, N. and Sitnikova, E., 2020. A new network forensic framework based on deep learning for Internet of Things networks: A particle deep framework. Future Generation Computer Systems.

[48] Maimó, L.F., Gómez, Á.L.P., Clemente, F.J.G., Pérez, M.G. and Pérez, G.M., 2018. A self-adaptive deep learning-based system for anomaly detection in 5G networks. IEEE Access, 6, pp.7700-7712.

[49] Pektaş, A. and Acarman, T., 2018. Botnet detection based on network flow summary and deep learning. International Journal of Network Management, 28(6), p.e2039.

[50] Naveed, K. and Wu, H., 2020, June. Poster: A Semi-Supervised Framework to Detect Botnets in IoT Devices. In 2020 IFIP Networking Conference (Networking) (pp. 649-651). IEEE.

[51] Vinayakumar, R., Alazab, M., Srinivasan, S., Pham, Q.V., Padannayil, S.K. and Simran, K., 2020. A visualized botnet detection system based deep learning for the Internet of Things networks of smart cities. IEEE Transactions on Industry Applications.

[52] Alzahrani H., Abulkhair M. and Alkayal, E., 2020. A Multi-Class Neural Network Model for Rapid Detection of IoT Botnet Attacks. International Journal of Advanced Computer Science and Applications(IJACSA), 11(7), 2020.

[53] Bhuvaneswari Amma N.G. and Selvakumar S., 2020. Anomaly detection framework for Internet of things traffic using vector convolutional deep learning approach in fog environment. Future Generation Computer Systems

[54] Dong, X., Dong, C., Chen, Z., Cheng, Y. and Chen, B., 2020. BotDetector: An extreme learning machine-based Internet of Things botnet detection model. Transactions on Emerging Telecommunications Technologies, p.e3999.

[55] Letteri, I., Della Penna, G. and De Gasperis, G., 2018, October. Botnet detection in software defined networks by deep learning techniques. In International Symposium on Cyberspace Safety and Security (pp. 49-62). Springer, Cham.

[56] Ahmed, A.A., Jabbar, W.A., Sadiq, A.S. and Patel, H., 2020. Deep learning-based classification model for botnet attack detection. Journal of Ambient Intelligence and Humanized Computing, pp.1-10.

[57] Shi, W.C. and Sun, H.M., 2020. DeepBot: a time-based botnet detection with deep learning. SOFT COMPUTING.

[58] Asadi, M., Jamali, M.A.J., Parsa, S. and Majidnezhad, V., 2020. Detecting botnet by using particle swarm optimization algorithm based on voting system. Future Generation Computer Systems, 107, pp.95-111.

[59] Parra, G.D.L.T., Rad, P., Choo, K.K.R. and Beebe, N., 2020. Detecting Internet of Things attacks using distributed deep learning. Journal of Network and Computer Applications, p.102662.

[60] Hwang, R.H., Peng, M.C. and Huang, C.W., 2019. Detecting IoT Malicious Traffic based on Autoencoder and Convolutional Neural Network. In 2019 IEEE Globecom Workshops (GC Wkshps) (pp. 1-6). IEEE.

[61] Kim,J., Won, H., Shim,M., Hong, S., Choi, E., 2020. Feature Analysis of IoT Botnet Attacks based on RNN and LSTM. International Journal of Engineering Trends and Technology

[62] Costa, J., Dessai, N.F., Gaonkar, S., Aswale, S. and Shetgaonkar, P., 2020. IoT-Botnet Detection using Long Short-Term Memory Recurrent Neural Network. International Journal of Engineering Research & Technology (IJERT)

[63] Soe, Y.N., Feng, Y., Santosa, P.I., Hartanto, R. and Sakurai, K., 2020. Machine Learning-Based IoT-Botnet Attack Detection with Sequential Architecture. Sensors, 20(16), p.4372.