

Detect botnet attacks traffic using long shorts term memory technique

Muna Mohammad Taher Jawhar, Maha Abd Alalla Mohammad

Department of Software, College of Computer and Mathematical Science, University of Mosul, Mosul, Iraq

Article Info

Article history:

Received Dec 14, 2022

Revised Mar 4, 2023

Accepted Mar 12, 2023

Keywords:

Botnet

Cybersecurity

Internet of things

Long shorts term memory

Network attacks

ABSTRACT

The spread of the internet of things (IoT) greatly are to its targeting by other parties that are considered suspicious or malicious, such as the attacks that are exposed to various networks to endanger their security. For this reason, it was necessary to take strict measures to protect the security and stability of networks in general and the internet of things in particular. It is worth noting that the current study presented a model and chose a long shorts term memory (LSTM) for attack detection through the use of deep learning technology via the internet of things as well as the detection of bots in IoT systems.

This is an open access article under the [CC BY-SA](#) license.



Corresponding Author:

Muna Mohammad Taher Jawhar

Department of Software, College of Computer and Mathematical Science, University of Mosul

Mosul, Iraq

Email: dr.muna_taher@uomosul.edu.iq

1. INTRODUCTION

The usage of the internet of things (IoT) has expanded substantially in recent years, as with the increasing of cybersecurity concerns. Cybersecurity has become a serious concern for institutions and businesses of all kinds, with the quantity and sophistication of attacks increasing at an alarming rate [1]. Internet of things prototypes may be used for a variety of reasons and installed in a variety of locations depending on the used cases. On deployment, the size of these devices can range from microscopic to massive, carrying the most critical and sensitive information across all sensory modes of everyday living activities [2]. The main worry with IoT systems is dealing with device security and data protection from assaults. Cyber-attacks are the cyberattacks express the intentional exploitation or unlawful access to the information of a specific person or the private infrastructure of another person or organization. It is not easy to protect IoT devices because of the hardware and protocols from attacks because they are directly exposed to devices over the internet; and resource limits on devices [3].

The term "bots" refers to a network of robots. Typically, a botmaster or attacker takes control of a computer by infecting it with a virus or malicious malware. The botmaster gains an access to the victim system in this manner. As a result, the infected machine will thereafter be controlled by the bot management and will carry out its directives. As a result, the bot manager can make use of this capability. The majority of the time, users of these devices are unaware that their systems are being remotely managed and abused [4]. When the target is directly attacked by a large number of infected systems, a bot attack occurs, causing the target systems to fail to service. Such attacks are planned and organized through the use of botnets to infect systems [5]. Since bot assaults are a severe and difficult problem, several solutions have been offered to combat them. In general,

there is no mechanism that can ensure that such assaults will not occur. Instead, there are simple ways of preventing repeated assaults and lessening the impact of other attacks [6].

Long-term memory, a recurrent neural network (RNN) development, was introduced by Hochreiter and Schmidhuber [7] to address the problems of defects in RNN by adding additional reactions per a unit (or cell). LSTMs are a special type of RNN that is capable of learning long term dependencies and remembers information for long periods of time as a default. The LSTM model is structured as a chain structure [8], [9]. The problem security typical for the IoT, as well as the purpose of gaining unauthorized access to the IoT [10].

The main goal is to develop an effective and dynamic action plan capable of detecting IoT attacks. The current study proposes, within the framework of its work, a special model that contributes to the discovery of botnet attacks and breaches that occur on IoT devices. Using the LSTM model, two well-known, common, and dangerous IoT attacks (Bashlet and Mirai). The current proposed model reveals four types of security cameras in this study. It contains data about attacks on devices connected to the IoT in suspicious packages collected in real time. The results were reasonably satisfactory.

The current study has provided several concepts and strategies for protecting the IoT from the threats it faces. In this part, the present study has come over the works of earlier researchers on this topic. The author's study [11] intends to explore cyber security in the face of distribution denial of service (DDOS), binary intrusion detection system (B-IDS), and malware assaults. For botnet attack detection, he employed a variety of machine learning methods, including "support vector machine, naive Bayes, linear regression (LR), artificial neural network (ANN), decision tree, random forest, fuzzy classifier, K-nearest neighbor (K-NN), adaptive boosting, gradient boosting, and tree ensemble". These algorithms were evaluated for performance on nine sensor devices use network-based detection of IoT (N-BaIoT) datasets to evaluate the intrusion finding the system security and accuracy. The results illustrate the tree-based algorithm which obtained more than 99% higher accuracy on the same sensor compared to other tested methods used sensors. Mohamed and colleagues used a "Bayesian optimization Gaussian process classification (BO-GP)" and "decision tree (DT)" model to identify botnet attacks on IoT devices [12]. The suggested optimized DT-based architecture enhanced accuracy, precision, recall, and F-score in experiments. It achieved values of 99.99%, 0.99, 1.00, and 1.00 for these four measures, respectively. Sriram employed numerous traditional machine learning (ML) classifier methods in his study [13], and the results of his experiments are shown in his publication. Yan and colleagues used three different ML algorithms for botnet attack detection in [14], including an ANN, a J48 decision tree, and Naive Bayes, with an overall detection performance of around 99%.

Lee *et al.* [15] utilized four different machine learning algorithms on three different botnet attack datasets: Stratosphere lab at CTU-Prague (CTU-13), intrusion detection evaluation dataset (CIC-IDS2017), and IoT-23. Alkahtani and Aldhyani [16], Seungjin developed a strategy for botnet detection that combines honeypots and machine learning to characterize botnet assaults. The experimental findings indicated that the random forest method with the Weka machine learning application produced a high accuracy of more than 96% and a false positive rate of 0.24127. The study is divided into sections: the introduction and the relevant work in in this field, method in section 2 examines the botnet database on the IoT and goes over the LSTM that were employed in the present study and performance of network in identified IoT threats. Section 3 describes the outcome, whereas section 4 analyzes the study's findings.

2. METHOD

2.1. Botnet dataset

Most of the researchers in the field of cyber-attacks and the IoT worked on internationally accredited databases for the purpose of scientific research [17]-[20]. The dataset used in this research was created using real network traffic and commercial IoT devices, which obtained from packages coming from different types of surveillance cameras used in homes and shops connected to the internet. Table 1 shows the security camera commercial devices that were utilized extracting network traffic which includes botnet assaults. The dataset contains two primary assaults, Mirai and Bashlite, with subtype attacks for each, as indicated in Table 2.

Table 1. Devices which were used to develop dataset'

Device type	Devices used in model
Security camera	Provision PT-737E
Security camera	Provision PT-838
Security camera	Simple Home XCS7-1002-WHT
Security camera	Simple Home XCS7-1003-WHT
Security camera	Samsung SNH1011N

Table 2. The type of botnet attacks

Attacks name	Sub attacks	Description
Bashlite	Junk	Sending spam data
	TCP flood	Sending flood of request
	UDP	Sending flood of request
	Scan	Scans network for victim device
	COMBO	Open connection IP address and network port
Miai	ACK	Send flood of acknowledgment
	SYN	Send synchronize packet flood
	Plain UDP	UDP flood by optimizing sending packet per second
	UDP flood scan	Scan the network for victim device

2.2. Long-shorts term memory (LSTM)

Memory of long-term in an artificial neural network which is used in many areas such as deep learning and artificial intelligence. In contrasting to the standard feed forward ANN, LSTM possesses feedback of connections. Such a model of a RNN to a process that is not only the dependent points of a single data but also is to the entire sequence of the data used [21].

LSTM states the analogy in a standard RNN which meant to contain both "long-term memory" and "short-term memory". Therefore, the network connectivity weights and biases change once per loop during train, similar to the physiological changes which occur in synaptic strengths which is called the "store long-term memories". Activation patterns in the network is changed once for each time step [22], which is an analogous to the way in which a momentary change in electrical unlocking patterns. That occurs in the brain stores" short-term memories".

The LSTM architecture aims to provide a "short-term memory" for an RNN which can use and last for thousands of time steps, consequently "long short-term memory" [23]. A common of LSTM module consists of cells, "an output gate, an input gate, and a forget gate". The cell remembers the values at random time for intervals while the three gates control the process of information flow which happens in and out of the cell [24].

The LSTM networks are suitable in many areas which includes "classifying, processing and making predictions" which based on time series data, where there can be multiple unknown delays that are between important events in a given time series. In fact, LSTMs were developed in order to deal with several problems including the problem of gradient fading that can be encountered in the case to train the traditional RNNs. Relative gap length sensitivity is one of the features of "LSTM over RNNs" and other sequential learning methods used in many fields and applications [25].

The small variables represent vectors in the next equations. Matrices WE_q and IN_q contain, correspondingly, the values of input weights and values of the frequent connections, where there is a low q which can be either the input gate ig , output gate og , the forget gate fo or the memory cell c , according to the current account activation. The study uses in this section, 'vector of notation' [26]. In order to calculate the aggregate numbers, that found in the equations of the forward-passing LSTM cell with the forget gate used, according formulas have been used [24], [27]:

$$fo_t = \sigma_g (WE_{fo} xin_t + IN_{fo} hi_{t-1} + b_{fo}) \quad (1)$$

$$ig_t = \sigma_g (WE_{ig} xin_t + IN_{ig} hi_{t-1} + b_{ig}) \quad (2)$$

$$og_t = \sigma_g (WE_{og} xin_t + IN_{og} hi_{t-1} + b_{og}) \quad (3)$$

$$ci_t = \sigma_c (WE_c xin_t + IN_c hi_{t-1} + b_c) \quad (4)$$

$$c_t = fo_t \odot c_{t-1} + ig_t \odot ci_t \quad (5)$$

$$hi_t = og_t \odot \sigma_{hi}(c_t) \quad (6)$$

where the initial values are used $c_0 = 0$ and $hi_0 = 0$. It shows the operator \odot used to the Hadamard product (element-wise product). The time step is indexed by the subscript t . The following Table 3 shows the symbols used in the above equations.

Symbol	Meaning of symbol
x_{in}	Input vector
f_o	Forget gate
i_g	Input / update gate
o_g	Output gate
h_i	Hidden state
c_i	Cell input
c	Cell state
b	Bias value
σ_g	The sigmoid function
σ_c	The hyperbolic tangent function
σ_{hi}	The hyperbolic tangent function

3. EXPERIMENTAL RESULTS

In this part of the paper, the steps of the model that was built and the analysis and presentation of the results were explained. After performing the initial processing on the data, it is sent to the LSTM network whose details are described in the previous part. The results obtained can determine whether it is a type of botnet attack or is it just an ordinary packet. As shown in Figure 1 illustrates the work of the proposed model.

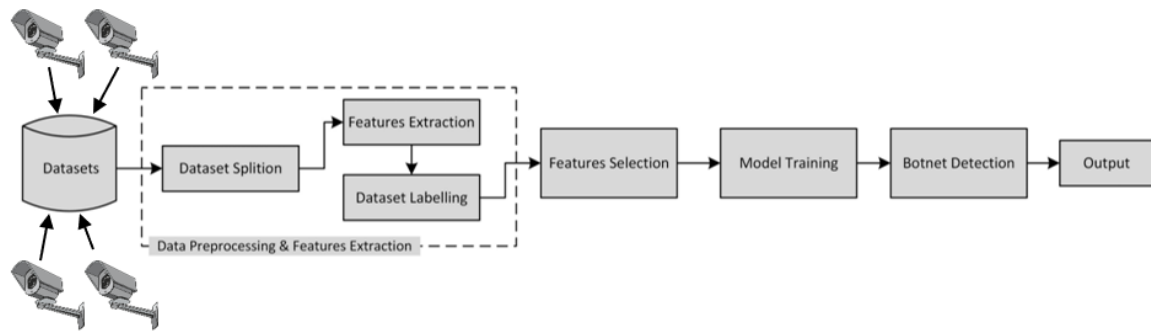


Figure 1. Methodology for botnet attacks detection

The evaluation metrics to evaluate the system for detection of botnet assaults, accuracy, recall, precision, and F1-score metrics were used. The following are:

$$Accuracy = \frac{(TP+TN)}{(FP+FN+TP+TN)} \times 100\% \tag{7}$$

$$precision = \frac{TP}{(FP+TP)} \times 100\% \tag{8}$$

$$sensitivity = \frac{TP}{(TP+FN)} \times 100\% \tag{9}$$

$$recall = \frac{TP}{(TP+FN)} \times 100\% \tag{10}$$

$$f1 - score = 2 \times \frac{(precision \times sensitivity)}{(precision + sensitivity)} \times 100\% \tag{11}$$

wherever true positif (TP) states true positive that false positif (FP) is false positive, true negative (TN) stands for true negative, and false negative (FN) refers to false negative. In this research, work on four types of special security cameras, which are considered as types of internet of things devices, and verifying the possibility of being exposed to attacks called botnets, and examining the effectiveness of the firefly algorithm in detecting botnet attacks against internet of things devices. The types of cameras used are: provision PT-737E, Provision PT-838, simple home XCS7-1002-W and simple home XCS7-1003-WHT. The results of the experiment showed that the presented system was good and acceptable based on the evaluation metrics as shown in the Table 4.

Table 4. The model performances detect botnet attacks from for types of camera as IoT devices

Camera types	Accuracy	Precision	Recall	F1-score
Provision PT-737E	94.27	96.57	96.21	96.38
Provision PT-838	92.46	99.60	94.73	97.10
Simple Home XCS7-1002-W	94.57	97.33	95.88	96.59
Simple Home XCS7-1003-WHT	94.57	99.68	96.22	97.91

4. CONCLUSION

In this study, LSTM has considered a deep learning architecture that depends on an artificial recurrent neural network. LSTMs have a viable solution for problems including sequences and time series. In addition, LSTM is useful in time series prediction because of its feature to remember the previous inputs used to detect botnet attacks that affect devices used in internet of things systems, and through the results the algorithm proved that it is efficient and flexible in dealing with data in addition to its efficiency in the detection. The proposed model in this paper works to detect attacks on four types of security cameras. It contains data about attacks on devices connected to the internet of things in suspicious packages collected in real time. According to assessment metrics, the experiment results demonstrated that the suggested system performed well. The suggested system for identifying the botnet which is used on the provision PT-737E camera revealed the following results: accuracy: 94.27%, recall: 96.57%, and F1 score: 96.38%. Thus, the system results in classifying the botnet attacks the Provision PT-838 camera were 92.46% for accuracy, 94.73% for recall and 97.10% for f1 score. The results for simple home XCS7-1002-W were 94.57% accuracy, 95.88% for recall and 96.59% for f1 score. The results for simple home XCS7-1003-WHT were 94.57% accuracy, 96.22% for recall and 97.91% for f1 score.




REFERENCES

- [1] M. Y. Alzahrani and A. M. Bamhdi, "Hybrid deep-learning model to detect botnet attacks over internet of things environments," *Soft Computing*, vol. 26, no. 16, pp. 7721–7735, Aug. 2022, doi: 10.1007/s00500-022-06750-4.
- [2] K. Mandal, M. Rajkumar, P. Ezhumalai, D. Jayakumar, and R. Yuvarani, "WITHDRAWN: Improved security using machine learning for IoT intrusion detection system," *Materials Today: Proceedings*, Dec. 2020, doi: 10.1016/j.matpr.2020.10.187.
- [3] K. V. V. N. L. S. Kiran, R. N. K. Devisetty, N. P. Kalyan, K. Mukundini, and R. Karthi, "Building an intrusion detection system for IoT environment using machine learning techniques," *Procedia Computer Science*, vol. 171, pp. 2372–2379, 2020, doi: 10.1016/j.procs.2020.04.257.
- [4] A. H. Lashkari, G. D. Gil, J. E. Keenan, K. F. Mbah, and A. A. Ghorbani, "A survey leading to a new evaluation framework for networkbased botnet detection," in *ACM International Conference Proceeding Series*, Nov. 2017, pp. 59–66, doi: 10.1145/3163058.3163059.
- [5] W. Kuochen, H. Chun-Ying, T. Li-Yang, and L. Ying-Dar, "Behavior-based botnet detection in parallel," *Security and Communication Networks*, vol. 2, pp. 1849–1859, 2014, doi: 10.1002/sec.898/abstract.
- [6] M. Asadi, M. A. J. Jamali, S. Parsa, and V. Majidnezhad, "Detecting botnet by using particle swarm optimization algorithm based on voting system," *Future Generation Computer Systems*, vol. 107, pp. 95–111, Jun. 2020, doi: 10.1016/j.future.2020.01.055.
- [7] J. Chung, C. Gulcehre, K. Cho, and Y. Bengio, "Gated feedback recurrent neural networks," in *32nd International Conference on Machine Learning, ICML 2015*, Feb. 2015, vol. 3, pp. 2067–2075.
- [8] C. Dyer, M. Ballesteros, W. Ling, A. Matthews, and N. A. Smith, "Transition-based dependency parsing with stack long short-term memory," in *ACL-IJCNLP 2015 - 53rd Annual Meeting of the Association for Computational Linguistics and the 7th International Joint Conference on Natural Language Processing of the Asian Federation of Natural Language Processing, Proceedings of the Conference*, 2015, vol. 1, pp. 334–343, doi: 10.3115/v1/p15-1033.
- [9] D. Bahdanau, K. H. Cho, and Y. Bengio, "Neural machine translation by jointly learning to align and translate," Sep. 2015, *arxiv: 1409.0473v7*.
- [10] M. Waqas *et al.*, "Botnet attack detection in internet of things devices over cloud environment via machine learning," *Concurrency and Computation: Practice and Experience*, vol. 34, no. 4, 2022, doi: 10.1002/cpe.6662.
- [11] M. N. Injadat, A. Moubayed, and A. Shami, "Detecting botnet attacks in IoT environments: An Optimized Machine Learning Approach," in *Proceedings of the International Conference on Microelectronics, ICM*, Dec. 2020, vol. 2020-December, pp. 1–4, doi: 10.1109/ICM50269.2020.9331794.
- [12] S. Sriram, R. Vinayakumar, M. Alazab, and K. P. Soman, "Network flow based IoT botnet attack detection using deep learning," in *IEEE INFOCOM 2020 - IEEE Conference on Computer Communications Workshops, INFOCOM WKSHPs 2020*, Jul. 2020, pp. 189–194, doi: 10.1109/INFOCOMWKSHPs50562.2020.9162668.
- [13] Y. N. Soe, Y. Feng, P. I. Santosa, R. Hartanto, and K. Sakurai, "Machine learning-based IoT-botnet attack detection with sequential architecture," *Sensors (Switzerland)*, vol. 20, no. 16, pp. 1–15, Aug. 2020, doi: 10.3390/s20164372.
- [14] F. Hussain, S. G. Abbas, U. U. Fayyaz, G. A. Shah, A. Toqeer, and A. Ali, "Towards a universal features set for IoT botnet attacks detection," in *Proceedings - 2020 23rd IEEE International Multi-Topic Conference, INMIC 2020*, Nov. 2020, pp. 1–6, doi: 10.1109/INMIC50486.2020.9318106.
- [15] S. Lee, A. Abdullah, N. Jhanjhi, and S. Kok, "Classification of botnet attacks in IoT smart factory using honeypot combined with machine learning," *PeerJ Computer Science*, vol. 7, pp. 1–23, Jan. 2021, doi: 10.7717/PEERJ-CS.350.
- [16] H. Alkahtani and T. H. H. Aldhyani, "Botnet attack detection by using CNN-LSTM model for internet of things applications," *Security and Communication Networks*, vol. 2021, pp. 1–23, Sep. 2021, doi: 10.1155/2021/3806459.
- [17] Irfan, I. M. Wildani, and I. N. Yulita, "Classifying botnet attack on internet of things device using random forest," *IOP Conference Series: Earth and Environmental Science*, vol. 248, no. 1, p. 012002, Apr. 2019, doi: 10.1088/1755-1315/248/1/012002.
- [18] J. Rose, "913 malicious network traffic PCAPs and binary visualisation images dataset," *IEEE Dataport*, 2021, doi: 10.21227/pda3-zy88.




- [19] M. Yair *et al.*, “detection_of_IoT_botnet_attacks_N_BaIoT Data Set,” 2018. [Online]. Available: https://archive.ics.uci.edu/ml/datasets/detection_of_IoT_botnet_attacks_N_BaIoT#.
- [20] H. Il Suk, “An introduction to neural networks and deep learning,” in *Deep Learning for Medical Image Analysis*, 2017, pp. 3–24.
- [21] I. Sutskever, J. Martens, and G. Hinton, “Generating text with recurrent neural networks,” in *Proceedings of the 28th International Conference on Machine Learning, ICML 2011*, 2011, pp. 1017–1024.
- [22] H. Sak, A. Senior, and F. Beaufays, “Long short-term memory recurrent neural network architectures for large scale acoustic modeling,” in *Proceedings of the Annual Conference of the International Speech Communication Association, INTERSPEECH*, Sep. 2014, pp. 338–342, doi: 10.21437/interspeech.2014-80.
- [23] Q. Lyu and J. Zhu, “Revisit long short-term memory: an optimization perspective,” in *NIPS 2014 Deep Learning and Representation Learning Workshop*, 2014, pp. 1–9.
- [24] N. Kalchbrenner, I. Danihelka, and A. Graves, “Grid long short-term memory,” Jul. 2015, *arxiv: 1507.01526*.
- [25] D. Eck and J. Schmidhuber, “Finding temporal structure in music: Blues improvisation with LSTM recurrent networks,” in *Neural Networks for Signal Processing - Proceedings of the IEEE Workshop*, 2002, vol. 2002-January, pp. 747–756, doi: 10.1109/NNSP.2002.1030094.
- [26] H. Hewamalage, C. Bergmeir, and K. Bandara, “Recurrent neural networks for time series forecasting: current status and future directions,” *International Journal of Forecasting*, vol. 37, no. 1, pp. 388–427, Jan. 2021, doi: 10.1016/j.ijforecast.2020.06.008.
- [27] I. Kang, S. Pang, Q. Zhang, N. Fang, and G. Barbastathis, “Recurrent neural network reveals transparent objects through scattering media,” *Optics Express*, vol. 29, no. 4, p. 5316, Feb. 2021, doi: 10.1364/OE.412890.

BIOGRAPHIES OF AUTHORS



Muna Mohammad Taher Jawhar    received the D.Sc. degree (doctor) in computer science from the Jamia Milia Islamia, Academy of Sciences, New Delhi, India. with the dissertation “Design of intrusion detection model using neural network”. She is a teacher of computer science in college of computer science and mathematics, software department. She has published over 18 journal papers and conference proceedings. She researches interests are in network security, artificial intelligence. She can be contacted at email: dr.muna_taher@uomosul.edu.iq.



Maha Abd Alalla Mohammad    received the B.Sc. (1999) in Mosul University, college of computer science and mathematics, MSc. (2004) in Mosul University, College of Computer Science and Mathematics, (2009) obtain the title of lecturer in artificial intelligence techniques. She is teacher of computer science in college of computer science and mathematics, software department the following subjects in undergraduate studies: discrete structure, theory of compatibility, databases, compilers and artificial intelligence. She has published over 12 journal papers and conference proceedings. She researches interests are in artificial intelligence and pattern recognition. She can be contacted at email: mahaabd77@uomosul.edu.iq.