Intelligent Botnet Detection Approach in Modern Applications

https://doi.org/10.3991/ijim.v15i16.24199

Khattab M. Ali Alheeti[1], Ibrahim Alsukayti[2(✉)], Mohammed Alreshoodi[2]
[1]University of Anbar, Ramadi, Iraq
[2]Qassim University, Buraydah, Saudi Arabia
co.khattab.alheeti@uoanbar.edu.iq

Abstract—Innovative applications are employed to enhance human-style life. The Internet of Things (IoT) is recently utilized in designing these environments. Therefore, security and privacy are considered essential parts to deploy and successful intelligent environments. In addition, most of the protection systems of IoT are vulnerable to various types of attacks. Hence, intrusion detection systems (IDS) have become crucial requirements for any modern design. In this paper, a new detection system is proposed to secure sensitive information of IoT devices. However, it is heavily based on deep learning networks. The protection system can provide a secure environment for IoT. To prove the efficiency of the proposed approach, the system was tested by using two datasets; normal and fuzzification datasets. The accuracy rate in the case of the normal testing dataset was 99.30%, while was 99.42% for the fuzzification testing dataset. The experimental results of the proposed system reflect its robustness, reliability, and efficiency.

Keywords—IDS, IoT, deep neural networks, DDoS, Bot-IoT

1 Introduction

Internet of Things (IoT) provides a technological movement towards effective physical-digital convergence. It enables the development of intelligent systems interconnecting physical things surrounding us over the Internet. Such technological advancements have resulted in a broad scope of IoT applications in varying domains. Examples of these applications include smart homes, e-healthcare, smart grid, and intelligent transportation systems. The IoT technology has also been applied in various industrial environments for effective monitoring, smart control, and intelligent automation. As a result, real deployments of IoT systems with an increasing number of IoT-enabled objects and devices have been growing during recent years. Accordingly, various IoT networks increasingly emerged along with a massive amount of IoT data communicated over the Internet. This poses serious challenges concerning IoT security and privacy, which can delay the effective deployment of IoT systems, particularly for data-sensitive applications.

In reality, IoT systems are vulnerable to a wide range of cyber-attacks which can lead to vital damage at different levels. This is more evident in the case of critical industrial and military applications with large IoT setups. Therefore, there is a need in current and future IoT deployments to address adequate practical IoT security support and establish effective resilience of any IoT attacks. IoT security solutions providing effective detection of malicious activities at early stages is critical to immune IoT systems. This gives rise to the need to develop Intrusion Detection Systems (IDSs) oriented for IoT systems.

IDSs enable monitoring network traffic and observing user activities to detect any abnormal actions or system abuse. The IDS functionality is based on detecting and responding to malicious traffic, which has made its way through the firewall system. IDSs can be implemented for the detection of misuses and anomalies. They can also be developed for host-based and network-based detection following either passive or reactive approaches. However, traditional IDS-based security solutions would require further improvement to be more effective in IoT environments. Most of the IoT systems are deployed with physical resources of limited computational and storage capabilities. Cybersecurity solutions need to be developed with lightweight yet efficient intrusion detection for adequate practical security support in IoT environments. Figure 1 shows the basic structure of a traditional detection system in IoT networks.

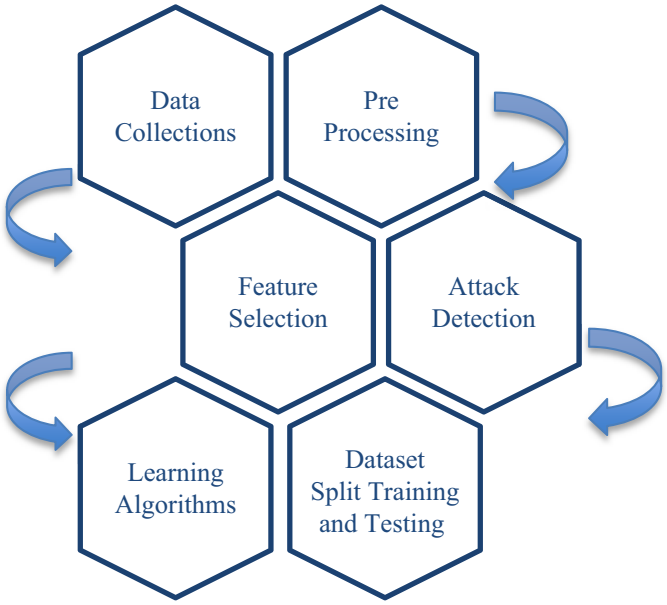

Fig. 1. Traditional detection system in IoT networks

In this paper, a new IDS is proposed to secure IoT resources against cyber-attacks. The proposed solution is heavily based on deep learning networks to increase the efficiency in providing resilient and secure environments for various IoT applications. The recent IoT dataset, Bot-IoT, was adopted for the development of the proposed IDS.

The experimental results reflect the robustness, reliability, and efficiency of the deep learning IDS.

2 Related works

Intrusion detection in IoT environments is crucial to provide adequate protection from separate various critical attacks that would compromise the security of IoT resources. Several IDSs have been introduced to secure IoT systems against different attacks. For example, effective detection of the Denial of Service (DoS) attack was addressed in [1–4] to prevent exhausting IoT resources. Another common IoT attack is Distributed DoS (DDoS), which was considered in [5–6]. Other Network IDSs were also proposed for mitigating routing attacks, including Wormhole [7–8], Sinkhole [9], and Sybil [10–11] attacks. In other research proposals, more effective IDSs were introduced to address the detection of multiple routing attacks such as Blackhole and Selective Forwarding attacks in addition to other attacks [12–14]. Moreover, the proposed IDS in [15] provided a solution to detect DoS, DDoS, surveillance, and information theft attacks. In [16–17], the focus was on developing IDSs to secure IoT networks against DoD, DDoS, Remote 2 Local (R2L), User 2 Root (U2R), and probe attacks.

Addressing effective detection of such IoT attacks was differently approached by the research community. Many IoT-oriented IDSs based on machine learning methods were proposed in the literature. These include the solutions proposed in [13, 18], which introduced Support Vector Machine (SVM) models for IoT intrusion detection. The Artificial Neural Network (ANN) method was also adopted in various IDSs proposals to secure IoT resources against different attacks [6, 19–21]. Other machine learning methods such as Naïve Bayesian [5, 22], random forest [23–24], optimum-path forest [25], and logistic regression [13] were also considered.

More effective IDS approaches such as those based on deep learning were also proposed for securing IoT Environments. In [26], the performance of two IoT intrusion detection based on deep learning models was compared and examined the effects of adversarial samples on such deep learning models. In [16], the need for optimal features selection to build an effective deep learning IDS was addressed using the spider monkey optimization (SMO) algorithm in addition to incorporating the stacked-deep polynomial network (SDPN) to enhance detection recognition. In [17], a deep learning IDS model incorporating a self-taught technique (STL) was introduced to support innovative home IoT applications. In [27], the focus was on helping IoT Fog security with fully automated deep learning IDS based on cascaded filtering that can be adaptively tuned to improve the detection of specific IoT attacks. In [28], a combination of a deep learning method and a shallow learning engine was considered to build IDS for IoT applications. In [29], a Deep Learning model was also combined with Dendritic Cell Algorithm (DCA) for a better feature selection process with less complexity. In [30], another combination was proposed to enhance the adaptive selection of the hyper-parameter values of a deep learning model using the Particle Swarm Optimization (PSO) method. In [31], the researchers proposed an IDS framework

based on combining network visualization and deep learning for large-scale IoT networks. In [32], the proposed IDS approach was based on implementing the Deep Belief Network, a type of deep learning algorithm. In [33], an IDS based on a deep migration learning model was proposed for IoT smart city applications.

On the other hand, such IDSs' effectiveness relies on the efficiency of the dataset adopted to develop the proposed model. In this regard, there are several publicly available datasets considered by the research community. Among the widely adopted ones are KDD99 [34], NSL-KDD [35], UNSW-NB15 [36]. For example, NSL-KKD was considered in [2, 17, 20–21, 24, 27, 37] to develop different machine learning and deep learning-based IDSs. UNSW-NB15 was also a common dataset among many IoT-oriented IDS solutions [19, 22, 28, 38–39]. Other examples also include CICID2017 [40] which contains traces for network flows and was utilized to build different machine learning IDSs in [41–42].

However, such datasets were not oriented towards IoT systems, and few IoT-based datasets are currently available to the research community. Thus, few IDS models developed using IoT-based datasets were proposed in the literature. One recent IoT dataset is the Bot-IoT dataset [43] which has drawn the attention of some researchers. For example, the dataset was utilized to develop the IDS solutions in [44–47]. The presented work in this paper provides an effective intrusion detection based on deep learning using the Bot-IoT dataset.

3 The methodology of proposed system

A new security system is proposed in this paper to provide a good production environment for IoT applications. However, it will play an essential vital role in deploying various innovative trends. The proposed system is heavily based on a dataset that collected IoT devices. In more detail, this dataset is reflected in the internal and external behaviours of various devices/nodes that are connected with local/ global networks directly [1]. The phases of the proposed system are explained below:

3.1 Dataset source

The Intrusion Detection system proposed in this paper is heavily based on dataset features [1]. In addition, these features described the events of devices in IoT. However, the IXIA PerfectStrom tool is employed to produce raw network packets of UNSW-NB.

This dataset is used to evaluate the performance of the security system proposed in this paper. Thus, it contains normal and malicious behaviours of the network packets. Table 1 shows the names of the features of the dataset used to evaluate the efficiency and effectiveness of the proposed system.

Table 1. Features of the dataset [1]

Features Names
id,dur,proto,service,state,spkts,dpkts,sbytes,dbytes,rate,sttl,dttl,sload,dload,sloss,dloss,sinpkt,dinpkt, sjit,djit,swin,stcpb,dtcpb,dwin,tcprtt,synack,ackdat,smean,dmean,trans_depth,response_body_len,ct_ srv_src,ct_state_ttl,ct_dst_ltm,ct_src_dport_ltm,ct_dst_sport_ltm,ct_dst_src_ltm,is_ftp_login,ct_ftp_ cmd,ct_flw_http_mthd,ct_src_ltm,ct_srv_dst,is_sm_ips_ports,attack_cat,label

Table 1 describes 46 features that are used to evaluate the performance of the proposed security system.

3.2 Intelligent detection system

The intelligent security system utilizes deep learning networks to distinguish between normal and abnormal connections via IoT. Therefore, it will be trained and tested with (more than 700000 connections) which describe the normal and abnormal behaviors of various IoT devices. On the one hand, the dataset is classified into three subsets which are training, testing, and validation. On the other hand, the first subset is testing (25%) and validation (25%), whereas training (50%).

The learning phase is stopped at a deep learning network when the square error is reached between actual output and desired. In more detail, this network has another stopping vector, epoch, namely 500. The basic structure of the deep network is shown in Figure 2.

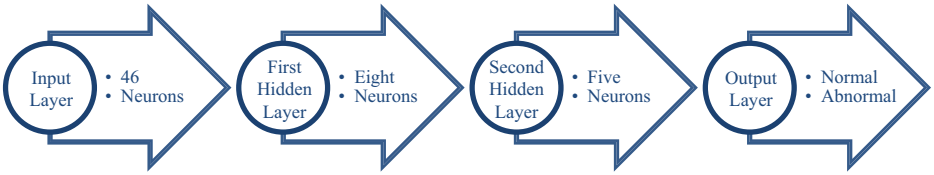

Fig. 2. The basic structure of a deep neural network

According to Figure 2, we can quickly notice that deep neural networks are composed of three layers. These layers are input, hidden, and output layers. However, the input layer is formed of 46 features, whereas the output layer has one output normal or abnormal connection. Therefore, the neural network is integrated from two hidden layers, and the first one has eight neurons while the second contains five neurons. The number of hidden layers or the number of neurons of each layer is considered a significant issue in a design detection system based on one of the artificial intelligence tools. Thus, in this paper, train-and-error is utilized to select the optimal number of hidden layers and the number of neurons at each layer.

The primary parameters of neural networks are considered an essential part of the design/build intelligent network for this Table 2 shows the initial parameters.

Table 2. Primary parameters of deep neural network

Training Parameter	Values
TrainParam. epochs	**24**
TrainParam. lr	**$1*10^{-11}$**
TrainParam. goal	**0**
TrainParam. min_grad	**$1*10^{-16}$**

The proposed system has been simulated on the system with the Intel Core i3 processor (2.53GHZ).

3.3 The model of intrusion detection system

In general, security systems are considered a very important point in an open wireless area [48–49]. The security system is composed of the main three-phase which are dataset collection and preprocessing phase, training phase, and testing phase. All of these phases are shown in Figure 3.

- Data source and preprocessing: in this phase, we are prepared for training and testing by dividing into three subsets that are mentioned above. In addition, the dataset needs some preprocessing operations, such as uniform distribution and normalization.
- Training phase: the initial structure of the deep neural network will be trained with features of the dataset. In this phase, condition stop is applied to get the best training rate that is heavily based on the threshold value, which is 99%.
- Testing phase: the proposed system will be tested with a dataset of IoT. In this case, we have two options: one testing with the same training subset and another testing with another subset to prove the efficiency of the proposed system.

At this step, the detection system must have the ability to detect various types of attacks.

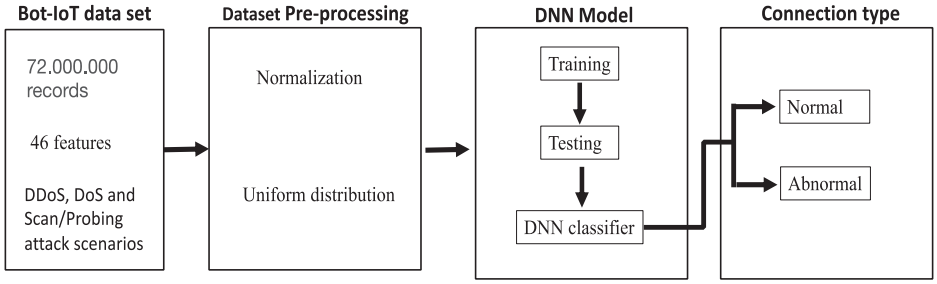

Fig. 3. Workflow of the proposed detection system

The hybrid detection system is based on a deep neural network that can learn from normal and abnormal behaviors. The low cost, real-time response encourages us to apply this type of tool to design security systems.

4 Experimental setup

In this stage, the Bot-IoT dataset was utilized to perform a further study on the performance of the proposed system. It has pcap files of 69.3 GB in size, which contains more than 72.000.000 records. The attacks considered in Bot-IoT include DDoS, DoS, OS and Service Scan, Keylogging, and Data exfiltration attacks. However, a subset of the original dataset comprised of 3 million records with a size of 1.07 GB was extracted via the use of select MySQL queries. The Bot-IoT dataset was classified into three subsets which are training (50%), testing (25%), and validation (25%).

To build an effective deep learning system, the three-hidden-layers deep neural network was developed with an input of 24 features. The system enables the classification of each information into one of five distinct classes. The system is based on three different hidden layers. The first one has six neurons, and the second contains eight neurons, while the last one includes five neurons. This setup was developed following a well-known artificial intelligence method, namely train-and-error, to optimally specify the optimal number of hidden layers and the number of neurons at each layer.

5 Results and discussion

In this work, the proposed system is tested with two datasets. Two options are dependent on one testing with the same training subset, and the second option is testing with another subset to measure and prove the efficiency of the proposed system. First, the performance metrics of training and testing the deep neural network with standard data are calculated to evaluate efficiency. The performance of the classification and the number of records utilized are shown in Table 3. The accuracy rate is calculated according to Equation 1.

$$Accuracy = \frac{\text{Number of correctly classified patterns}}{\text{Total number of patterns}} \tag{1}$$

Table 3. Accuracy of classification

Name	Actual Record	Deep Neural Network	Match Record	Miss Type	Accuracy Ratio
Normal	1865	1856	1855	1	99.46%
Abnormal	135	139	131	8	97.03%
Unknown	0	5	0	5	NaN

Moreover, the training/testing phases used the fuzzification dataset to calculate the accuracy rate of the proposed system. The accuracy rate of the training and testing= 99.20%, 99.42%, respectively. The performance of the classification and the number of records utilized are shown in Table 4.

Table 4. Accuracy of classification

Name	Actual Record	Deep Neural Network	Match Record	Miss Type	Accuracy Ratio
Normal	3724	3707	3707	0	99.54%
Abnormal	276	284	270	14	97.82%
Unknown	0	9	0	9	NaN

To measure and evaluate the proposed system performance, four types of alarms are measured: True Positive (TP), False Positive (FP), True Negative (TN), and False Negative (FN). Alarms rates are calculated to evaluate the efficiency of the proposed system. The equations in (2, 3, 4, and 5) show alarm rate calculation—the results of this calculation presented in Table 5 [50–51]:

$$\text{TP\_Rate} = \frac{\text{TP}}{\text{TP} + \text{FN}} \tag{2}$$

$$\text{TN}_{\text{Rate}} = \frac{\text{TN}}{\text{TN} + \text{FP}} \tag{3}$$

$$\text{FN}_{\text{Rate}} = \frac{\text{FN}}{\text{FN} + \text{TP}} \tag{4}$$

$$\text{FP}_{\text{Rate}} = \frac{\text{FP}}{\text{FP} + \text{TN}} \tag{5}$$

Table 5. Alarm rates

Alarm Type	With Normal Dataset (%)	With Fuzzification Dataset (%)
True Positive	99.94	100
True Negative	94.24	95.07
False Negative	0.0539	0
False Positive	5.75	4.92
Error Rate	0.70	0.57

Table 6 shows the results of alarm rate when training and testing the deep neural network with two datasets. First, the normal dataset was used, and the next fuzzification dataset was utilized. Secondly, the proposed system is tested with an IoT dataset, and some performance metrics are calculated. The results of four types of alarms are presented in Table 6.

Table 6. Alarm rates

Alarm Type with IoT dataset	Rate (%)
True Positive	100
True Negative	100
False Negative	0
False Positive	0

The result of training/testing the deep neural network with IoT data is presented in Figures 4 that shows the performance and the training status of the deep neural network.

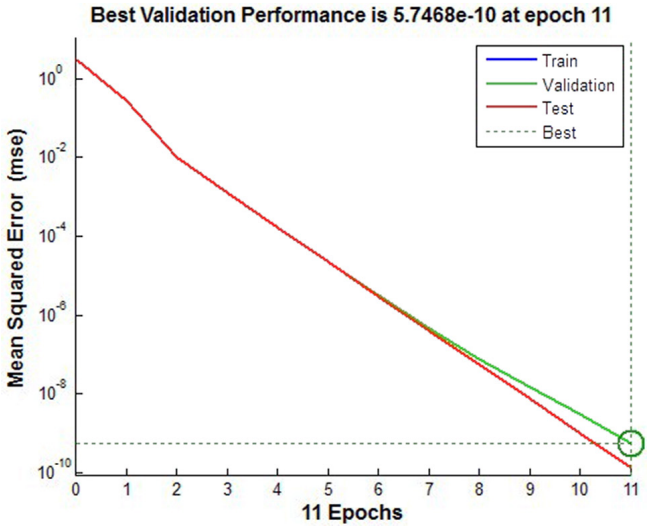

Fig. 4. Training performance

Therefore, we compare the accuracy rate of the proposed system with the latest works to distinguish our results from others explain in Table 7.

Table 7. Comparing the accuracy rate of the proposed system with the latest works

Security Systems	Accuracy Rate (%)
[52]	98.22
[53]	98.071
Our proposal with a normal dataset	99.46
Our proposal with fuzzification dataset	99.54

However, we can easily notice that our system is more efficient at detection rate than others. In more detail, the proposed security system can adopt to detect/ identify various attacks, such as sybil, wormhole attacks.

6 Conclusion

In the current human life, the use of the Internet is increased. Hence, the number of Internet of Things (IoT) devices connected to the Internet increased. For this reason, finding a robust security model for the IoT environment is a big challenge. This paper proposes a new intrusion detection system based on utilizing a deep neural network as a classifier. To measure and prove the efficiency of the proposed approach, the system is tested on two datasets. First, the performance metrics of training and testing the deep neural network with normal data are calculated to evaluate the efficiency. The total accuracy of training and testing absolute was 98.60%, 99.30%, respectively.

Moreover, the training and testing phases used the fuzzification dataset to calculate the accuracy rate of the proposed system. The training and testing accuracy were 99.20%, 99.42%, respectively. approach. The suggested system is tested with an IoT dataset and the performance metrics calculated in the second case. For future work, the DNN method can be compared with other machine learning methods including fuzzy logic system, genetic algorithm, and swarm algorithm. Moreover, the usage of the proposed DNN-based model can be applied to potential online applications for network/service providers.

7 References

[1] Verma, A., & Ranga, V. (2019). Machine Learning Based Intrusion Detection Systems for IoT Applications. Wireless Personal Communications, 1–24. https://doi.org/10.1007/s11277-019-06986-8

[2] Diro, A. A., & Chilamkurti, N. (2018). Distributed Attack Detection Scheme Using Deep Learning Approach for Internet of Things. Future Generation Computer Systems, 82, 761–768. https://doi.org/10.1016/j.future.2017.08.043

[3] Bamou, A., Khardioui, M., El Ouadghiri, M. D., & Aghoutane, B. (2019, July). Implementing and Evaluating an Intrusion Detection System for Denial of Service Attacks in IoT Environments. In International Conference on Artificial Intelligence and Symbolic Computation (pp. 167–178). Springer, Cham. https://doi.org/10.1007/978-3-030-33103-0_17

[4] Ioulianou, P. P., & Vassilakis, V. G. (2019). Denial-of-Service Attacks and Countermeasures in the RPL-Based Internet of Things. In Computer Security (pp. 374–390). Springer, Cham. https://doi.org/10.1007/978-3-030-42048-2_24

[5] Mehmood, A., Mukherjee, M., Ahmed, S. H., Song, H., & Malik, K. M. (2018). NBC-MAIDS: Naïve Bayesian Classification Technique in Multi-agent System-Enriched IDS for Securing IoT against DDoS Attacks. The Journal of Supercomputing, 74(10), 5156–5170. https://doi.org/10.1007/s11227-018-2413-7

[6] Hodo, E., Bellekens, X., Hamilton, A., Dubouilh, P. L., Iorkyase, E., Tachtatzis, C., & Atkinson, R. (2016, May). Threat Analysis of IoT Networks Using Artificial Neural Network Intrusion Detection System. In 2016 International Symposium on Networks, Computers and Communications (ISNCC) (pp. 1–6). IEEE. https://doi.org/10.1109/ISNCC.2016.7746067

[7] Pongle, P., & Chavan, G. (2015). Real Time Intrusion and Wormhole Attack Detection in the Internet of things. International Journal of Computer Applications, 121(9). https://doi.org/10.5120/21565-4589

[8] Deshmukh-Bhosale, S., & Sonavane, S. S. (2019). A Real-Time Intrusion Detection System for Wormhole Attack in the RPL based Internet of Things. Procedia Manufacturing, 32, 840–847. https://doi.org/10.1016/j.promfg.2019.02.292

[9] Khardioui, M., Bamou, A., El Ouadghiri, M. D., & Aghoutane, B. (2019, July). Implementation and Evaluation of an Intrusion Detection System for IoT: Against Routing Attacks. In International Conference on Artificial Intelligence and Symbolic Computation (pp. 155–166). Springer, Cham. https://doi.org/10.1007/978-3-030-33103-0_16

[10] Murali, S., & Jamalipour, A. (2019). A Lightweight Intrusion Detection for Sybil Attack under Mobile RPL in the Internet of Things. IEEE Internet of Things Journal. https://doi.org/10.1109/JIOT.2019.2948149

[11] Stephen, R., & Arockiam, L. (2017). Intrusion Detection System to Detect Sinkhole Attack on RPL Protocol in Internet of Things. International Journal of Electrical Electronics and Computer Science, 4(4), 16–20.

[12] Ioannou, C., & Vassiliou, V. (2019, May). Classifying Security Attacks in IoT Networks Using Supervised Learning. In 2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS) (pp. 652–658). IEEE. https://doi.org/10.1109/DCOSS.2019.00118

[13] Ioannou, C., & Vassiliou, V. (2018, October). An Intrusion Detection System for Constrained WSN and IoT Nodes Based on Binary Logistic Regression. In Proceedings of the 21st ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems (pp. 259–263). https://doi.org/10.1145/3242102.3242145

[14] Verma, A., & Ranga, V. (2019, April). ELNIDS: Ensemble Learning Based Network Intrusion Detection System for RPL Based Internet of Things. In 2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU) (pp. 1–6). IEEE. https://doi.org/10.1109/IoT-SIU.2019.8777504

[15] Ge, M., Fu, X., Syed, N., Baig, Z., Teo, G., & Robles-Kelly, A. (2019, December). Deep Learning-Based Intrusion Detection for IoT Networks. In 2019 IEEE 24th Pacific Rim International Symposium on Dependable Computing (PRDC) (pp. 256–25609). IEEE. https://doi.org/10.1109/PRDC47002.2019.00056

[16] Otoum, Y., Liu, D., & Nayak, A. (2019). DL-IDS: A Deep Learning–Based Intrusion Detection Framework for Securing IoT. Transactions on Emerging Telecommunications Technologies, e3803. https://doi.org/10.1002/ett.3803

[17] Akter, M., Dip, G. D., Mira, M. S., Hamid, M. A., & Mridha, M. F. (2020). Construing Attacks of Internet of Things (IoT) and A Prehensile Intrusion Detection System for Anomaly Detection Using Deep Learning Approach. In International Conference on Innovative Computing and Communications (pp. 427–438). Springer, Singapore. https://doi.org/10.1007/978-981-15-0324-5_37

[18] Jan, S. U., Ahmed, S., Shakhov, V., & Koo, I. (2019). Toward a Lightweight Intrusion Detection System for the Internet of things. IEEE Access, 7, 42450–42471. https://doi.org/10.1109/ACCESS.2019.2907965

[19] Hanif, S., Ilyas, T., & Zeeshan, M. (2019, October). Intrusion Detection In IoT Using Artificial Neural Networks On UNSW-15 Dataset. In 2019 IEEE 16th International Conference on Smart Cities: Improving Quality of Life Using ICT & IoT and AI (HONET-ICT) (pp. 152–156). IEEE. https://doi.org/10.1109/HONET.2019.8908122

[20] Pamukov, M. E., Poulkov, V. K., & Shterev, V. A. (2018, July). Negative Selection and Neural Network Based Algorithm for Intrusion Detection in IoT. In 2018 41st International Conference on Telecommunications and Signal Processing (TSP) (pp. 1–5). IEEE. https://doi.org/10.1109/TSP.2018.8441338

[21] Larijani, H., Ahmad, J., & Mtetwa, N. (2019, July). A Heuristic Intrusion Detection System for Internet-of-Things (IoT). In Intelligent Computing-Proceedings of the Computing Conference (pp. 86–98). Springer, Cham. https://doi.org/10.1007/978-3-030-22871-2_7

[22] Shi, Q., Kang, J., Wang, R., Yi, H., Lin, Y., & Wang, J. (2018). A Framework of Intrusion Detection System Based on Bayesian Network in IoT. International Journal of Performability Engineering, 14(10). https://doi.org/10.23940/ijpe.18.10.p4.22802288

[23] Mohamed, T., Otsuka, T., & Ito, T. (2018, June). Towards Machine Learning Based IoT Intrusion Detection Service. In International Conference on Industrial, Engineering and Other Applications of Applied Intelligent Systems (pp. 580–585). Springer, Cham. https://doi.org/10.1007/978-3-319-92058-0_56

[24] Ben Elhadj, H., Jmal, R., Chelligue, H., & Fourati, L. C. (2020). A2ISDIoT: Artificial Intelligent Intrusion Detection System for Software Defined IoT Networks. In Web, Artificial Intelligence and Network Applications: Proceedings of the Workshops of the 34th International Conference on Advanced Information Networking and Applications (WAINA-2020) (pp. 798–809). Springer International Publishing. https://doi.org/10.1007/978-3-030-44038-1_73

[25] Bostani, H., & Sheikhan, M. (2017). Hybrid of Anomaly-Based and Specification-Based IDS for Internet of Things Using Unsupervised OPF Based on MapReduce Approach. Computer Communications, 98, 52–71. https://doi.org/10.1016/j.comcom.2016.12.001

[26] Ibitoye, O., Shafiq, O., & Matrawy, A. (2019). Analyzing Adversarial Attacks Against Deep Learning for Intrusion Detection in IoT Networks. arXiv preprint arXiv:1905.05137. https://doi.org/10.1109/GLOBECOM38437.2019.9014337

[27] Almiani, M., AbuGhazleh, A., Al-Rahayfeh, A., Atiewi, S., & Razaque, A. (2019). Deep Recurrent Neural Network for IoT Intrusion Detection System. Simulation Modelling Practice and Theory, 102031. https://doi.org/10.1016/j.simpat.2019.102031

[28] Tian, Q., Li, J., & Liu, H. (2019). A Method for Guaranteeing Wireless Communication Based on a Combination of Deep and Shallow Learning. IEEE Access, 7, 38688–38695. https://doi.org/10.1109/ACCESS.2019.2905754

[29] Aldhaheri, S., Alghazzawi, D., Cheng, L., Alzahrani, B., & Al-Barakati, A. (2020). DeepDCA: Novel Network-Based Detection of IoT Attacks Using Artificial Immune System. Applied Sciences, 10(6), 1909. https://doi.org/10.3390/app10061909

[30] Koroniotis, N., Moustafa, N., & 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. https://doi.org/10.1016/j.future.2020.03.042

[31] Thamilarasu, G., & Chawla, S. (2019). Towards Deep-Learning-Driven Intrusion Detection for the Internet of Things. Sensors, 19(9), 1977. https://doi.org/10.3390/s19091977

[32] Balakrishnan, N., Rajendran, A., Pelusi, D., & Ponnusamy, V. (2019). Deep Belief Network Enhanced Intrusion Detection System to Prevent Security Breach in the Internet of Things. Internet of Things, 100112. https://doi.org/10.1016/j.iot.2019.100112

[33] Li, D., Deng, L., Lee, M., & Wang, H. (2019). IoT Data Feature Extraction and Intrusion Detection System for Smart Cities Based on Deep Migration Learning. International Journal of Information Management, 49, 533–545. https://doi.org/10.1016/j.ijinfomgt.2019.04.006

[34] S. Hettich and S. Bay, KDD Cup 1999 Data—The UCI KDD Archive, Dept. Inf. Comput. Sci., Univ. California at Irvine, Irvine, CA, USA, 1999. [Online]. Available: http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html

[35] NSL-KDD | Datasets | Research | Canadian Institute for Cybersecurity | UNB. [Online]. Available: http://www.unb. ca/cic/research/datasets/nsl.html

[36] Moustafa, N., & Slay, J. (2015, November). UNSW-NB15: A Comprehensive Data Set for Network Intrusion Detection Systems (UNSW-NB15 network data set). In Proc. Mil. Commun. Inf. Syst. Conf. (MilCIS), pp. 1–6. https://doi.org/10.1109/MilCIS.2015.7348942

[37] Li, Y., Xu, Y., Liu, Z., Hou, H., Zheng, Y., Xin, Y., ... & Cui, L. (2020). Robust Detection for Network Intrusion of Industrial IoT Based on Multi-CNN Fusion. Measurement, 154, 107450. https://doi.org/10.1016/j.measurement.2019.107450

[38] Kumar, V., Das, A. K., & Sinha, D. (2019). UIDS: A Unified Intrusion Detection System for IoT Environment. Evolutionary Intelligence, 1–13. https://doi.org/10.1007/s12065-019-00291-w

[39] Lawal, M. A., Shaikh, R. A., & Hassan, S. R. (2020). Security Analysis of Network Anomalies Mitigation Schemes in IoT Networks. IEEE Access, 8, 43355–43374. https://doi.org/10.1109/ACCESS.2020.2976624

[40] Canadian Institute for Cybersecurity. (2017). IDS 2017 | Datasets | Research | Canadian Institute for Cybersecurity | UNB. [Online]. Available: https://www.unb.ca/cic/datasets/ids-2017.html

[41] Ferrag, M. A., Maglaras, L., Ahmim, A., Derdour, M., & Janicke, H. (2020). RDTIDS: Rules and Decision Tree-Based Intrusion Detection System for Internet-of-Things Networks. Future Internet, 12(3), 44. https://doi.org/10.3390/fi12030044

[42] Roopak, M., Tian, G. Y., & Chambers, J. (2020, January). An Intrusion Detection System Against DDoS Attacks in IoT Networks. In 2020 10th Annual Computing and Communication Workshop and Conference (CCWC) (pp. 0562–0567). IEEE. https://doi.org/10.1109/CCWC47524.2020.9031206

[43] Koroniotis, N., Moustafa, N., Sitnikova, E., & Turnbull, B. (2019). Towards the Development of Realistic Botnet Dataset in the Internet of Things for Network Forensic Analytics: Bot-IoT Dataset. Future Generation Computer Systems, 100, 779–796. https://doi.org/10.1016/j.future.2019.05.041

[44] Ullah, I., & Mahmoud, Q. H. (2020). A Two-Level Flow-Based Anomalous Activity Detection System for IoT Networks. Electronics, 9(3), 530. https://doi.org/10.3390/electronics9030530

[45] Shafiq, M., Tian, Z., Sun, Y., Du, X., & Guizani, M. (2020). Selection of Effective Machine Learning Algorithm and Bot-IoT Attacks Traffic Identification for Internet of Things in Smart City. Future Generation Computer Systems, 107, 433–442. https://doi.org/10.1016/j.future.2020.02.017

[46] Asadi, M., Jamali, M. A. J., Parsa, S., & Majidnezhad, V. (2020). Detecting Botnet by Using Particle Swarm Optimization Algorithm Based on Voting System. Future Generation Computer Systems, 107, 95–111. https://doi.org/10.1016/j.future.2020.01.055

[47] Soe, Y. N., Feng, Y., Santosa, P. I., Hartanto, R., & Sakurai, K. (2020). Towards a Lightweight Detection System for Cyber Attacks in the IoT Environment Using Corresponding Features. Electronics, 9(1), 144. https://doi.org/10.3390/electronics9010144.

[48] Naman, H., Hussien, N., Al-dabag, M., & Alrikabi, H. (2021). Encryption System for Hiding Information Based on Internet of Things. International Journal of Interactive Mobile Technologies, 15(2). https://doi.org/10.3991/ijim.v15i02.19869

[49] Hussien, Naseer Ali, et al. (2021). Monitoring the Consumption of Electrical Energy Based on the Internet of Things Applications. International Journal of Interactive Mobile Technologies, 15(7). https://doi.org/10.3991/ijim.v15i07.20183

[50] Ali Alheeti, K. M., & McDonald-Maier, K. (2018). Intelligent Intrusion Detection in External Communication Systems for Autonomous Vehicles. Systems Science & Control Engineering Journal, 6(1), Taylor Francis Publication UK. https://doi.org/10.1080/21642583.2018.1440260

[51] Hussein, A. S., Khairy, R. S., Najeeb, S. M. M., & ALRikabi, H. T. (2021). Credit Card Fraud Detection Using Fuzzy Rough Nearest Neighbor and Sequential Minimal Optimization with Logistic Regression. International Journal of Interactive Mobile Technologies, 15(5). https://doi.org/10.3991/ijim.v15i05.17173

[52] Popoola, S. I., Adebisi, B., Ande, R., Hammoudeh, M., Anoh, K., & Atayero, A. A. (2021). SMOTE-DRNN: A Deep Learning Algorithm for Botnet Detection in the Internet-of-Things Networks. Sensors, 21(9), 2985. https://doi.org/10.3390/s21092985

[53] Ge, M., Fu, X., Syed, N., Baig, Z., Teo, G., & Robles-Kelly, A. (2019, December). Deep Learning-Based Intrusion Detection for IoT Networks. In 2019 IEEE 24th Pacific Rim International Symposium on Dependable Computing (PRDC) (pp. 256–25609). IEEE. https://doi.org/10.1109/PRDC47002.2019.00056

8 Authors

Khattab M. Ali Alheeti received the B.Sc. Computer Science degree in 2000 from Baghdad, Iraq, M.Sc. (Hons.) Computer Networking and Information in 2009 from the University of Al Al- Bayt, Jordan, and Ph.D. from Essex University in 2017, respectively. Currently, he is working at University of Anbar.

Ibrahim S. Alsukayti received the B.S. degree in Computer Science, from Qassim University, Buraydah, KSA, in 2006. He then received the M.S. degree in Computer and Information Networks from University of Essex, Colchester, UK, in 2010 and the Ph.D in Computer Networks from Lancaster University, Lancaster, UK, in 2014. Currently, he is an Associate Professor with the Computer Science Department, College of Computer, Qassim University, Buraydah, KSA. He is also a team member of two ongoing funded research projects and the director of a research group targeting Internet of Things technologies & applications. His research interests include network routing, Wireless Sensor Networks, networking protocols, network security, and IoT.

Mohammed Alreshoodi received the B.S. degree in computer science from Qassim University, Buraydah, KSA, in 2004 and the M.S degree in computer networks from University of Essex, Colchester, UK, in 2011. He also received the Ph.D. degree in in computer networks from University of Essex, Colchester, UK, in 2011. He is currently an Associate Professor in the department of applied science in Unizah community college at Qassim University, KSA. His research interest includes computer networking, wireless networks, WSN, IoT, networks security. He is a member of WSN research group and Cyber Security research group at Collage of Computer, Qassim University, KSA.

Article submitted 2021-05-17. Resubmitted 2021-06-22. Final acceptance 2021-06-24. Final version published as submitted by the authors.