Online-Journals.org

iJIM International Journal of Interactive Mobile Technologies

iJIM | eISSN: 1865-7923 | Vol. 17 No. 19 (2023) | OPEN ACCESS

https://doi.org/10.3991/ijim.v17i19.41379

PAPER

Performance Evaluation of Machine Learning Approaches in Detecting IoT-Botnet Attacks

Ashraf H. Aljammal[1](✉), Ahmad Qawasmeh[1], Ala Mughaid[2], Salah Taamneh[1], Fadi I. Wedyan[3], Mamoon Obiedat[2]

[1]Department of Computer Science and Applications, Prince Al Hussein bin Abdullah II Faculty of Information Technology, The Hashemite University, Zarqa, Jordan

[2]Department of Information Technology, Prince Al Hussein bin Abdullah II Faculty of Information Technology, The Hashemite University, Zarqa, Jordan

[3]Department of Engineering, Computing, and Mathematical Sciences, Lewis University, Romeoville, Illinois, USA

ashrafj@hu.edu.jo

ABSTRACT

Botnets are today recognized as one of the most advanced vulnerability threats. Botnets control a huge percentage of network traffic and PCs. They have the ability to remotely control PCs (zombie machines) by their creator (BotMaster) via Command and Control (C&C) framework. They are the keys to a variety of Internet attacks such as spams, DDOS, and spreading malwares. This study proposes a number of machine learning techniques for detecting botnet assaults via IoT networks to help researchers in choosing the suitable ML algorithm for their applications. Using the BoT-IoT dataset, six different machine learning methods were evaluated: REPTree, RandomTree, RandomForest, J48, metaBagging, and Naive Bayes. Several measures, including accuracy, TPR, FPR, and many more, have been used to evaluate the algorithms' performance. The six algorithms were evaluated using three different testing situations. Scenario-1 tested the algorithms utilizing all of the parameters presented in the BoT-IoT dataset, scenario-2 used the IG feature reduction approach, and scenario-3 used extracted features from the attacker's received packets. The results revealed that the assessed algorithms performed well in all three cases with slight differences.

KEYWORDS

Internet of Things, botnet detection, IoT botnet attack, machine learning, network security, cyber security

1 INTRODUCTION

The Internet of Things (IoT) are physical devices connected with each other over a network; these devices are able to collect and share data with other devices [1, 2]. The IoT devices are low power consumption devices, which makes them suitable for many applications in many sectors [3]. In addition, they have the ability to be used for remotely monitoring, controlling, and managing equipment and systems, which results in enhancing efficiency and reduce costs. Smart home systems are an example of IoT home utilization, which allows the home owners to remotely monitor and

Aljammal, A.H., Qawasmeh, A., Mughaid, A., Taamneh, S., Wedyan, F.I., Obiedat, M. (2023). Performance Evaluation of Machine Learning Approaches in Detecting IoT-Botnet Attacks. *International Journal of Interactive Mobile Technologies (iJIM)*, 17(19), pp. 136–146. https://doi.org/10.3991/ijim.v17i19.41379

Article submitted 2023-05-14. Revision uploaded 2023-08-02. Final acceptance 2023-08-08.

operate their home appliances [4]. Another example is the wearable devices that can collect health and fitness information to be used later in providing users with advice in terms of nutrition and exercise [5]. Furthermore, healthcare and transportation are growing applications of the IoT. In healthcare, the IoT devices are able to monitor patients' vital signs in real-time, providing the clinicians with the latest information about the patients for suitable care and treatment [6]. In transportation, IoT devices and sensors can be used to monitor and collect data about the traffic flow for better decision making in terms of, for example, reducing traffic jams [7]. However, as the field of IoT connected devices grows, concerns about privacy, security, and data management are emerging [8]. The way IoT devices collect and share data makes these devices vulnerable to many types of cyberattacks, especially in terms of preserving privacy [9, 10]. Therefore, there is need for systems to protect and defend the IoT networks. Despite these obstacles, the potential benefits of IoT are significant, and the technology is expected to expand and improve over the next few years. As more products connect to the internet, the possible applications of IoT become limitless, and it has the ability to change the way we live, work, and interact with the world around us [11].

One of the modern threats that the IoT faces nowadays is Bot-IoT attacks, also known as IoT botnet attacks. Bot-IoT attacks have become a serious threat in recent years as a result of the rise of internet-connected devices and the lack of effective security measures. Many types of bot-IoTIoT attacks include hackers acquiring control of a large number of connected devices (called zombies) and utilizing them to launch coordinated attacks, sometimes by exploiting software defects in the devices. One of the most common uses of bot-IoTIoT attacks is DDoS attacks, in which a large number of devices are used to flood a target server or network with traffic, causing it to become overloaded and unavailable for legitimate users. In rare cases, bot-IoTIoT attacks have been used to carry out ransomware attacks, in which data on the target device is encrypted and held for ransom. Bot-IoT attacks may be harmful for both individuals and businesses. In addition to the financial consequences of cyber-attacks, such as lost revenue and system and infrastructure damage, there may be severe reputational harm [12]. For example, if a bot-IoTIoT assault disrupts a company's operations, it may result in bad news and a loss of confidence from customers and partners. Therefore, it is vital to protect internet-connected devices in order to avoid bot-IoTIoT attacks. This includes updating devices with the most recent security patches as well as using strong passwords and two-factor authentication. It is also vital to regularly monitor network traffic and device behavior for signs of bot-IoTIoT activity, such as unusual spikes in traffic or unexpected changes in device behavior. A number of industry-wide efforts are also underway to fight the bot-IoTIoT threat. Several internet service providers, for example, are striving to restrict bot-IoT traffic, and industry-wide security rules for IoT devices are being created. The bot-IoT threat poses a significant hazard to the growing number of internet-connected devices. However, with proper security measures and proactive monitoring, these risks may be reduced, and the safety and security of these devices and the networks to which they connect can be assured [13].

Machine learning is one of the most recent methods for detecting and mitigating cyberattacks including bot-IoT threats [14]. Its algorithms are trained and tested using well-known benchmarks (datasets). Furthermore, it can identify new sorts of bot-IoT assaults in real-time scenarios [15]. Although machine learning is a potent tool for detecting bot-IoT threats, training and validation utilizing related and well-known datasets is critical to the effectiveness of its algorithms.

The structure of the paper is organized as follows. Section 2 illustrates the literature review. Section 3 presents an overview of the methodology. Section 4 discusses the experiments and results discussion. Section 5 concludes our work.

2 LITERATURE REVIEW

This section will explore some of the latest machine learning techniques used to detect bot-IoT and malwares in IoT environment.

The authors of [16] proposed a hybrid intelligent deep learning approach to secure industrial IoT infrastructure against different types of bit attacks. They have evaluated the proposed approach using N-BaIoT dataset. Authors of [17] proposed a machine learning based model to detect botnet based DDoS attacks in the IoT environment. Different machine learning algorithms were used to build the proposed model such as KNN, MLP ANN. The BoT-IoT dataset was used to train and test the proposed model. A packet based botnet detection system using machine learning is proposed by [18]. Seven features were extracted from network packet and used to train and test the dataset. The authors of [19] proposed a machine learning model combined with hybrid feature selection method to detect IoT botnets. The most informative features were selected to be used by machine learning models in the training and testing stages. A machine learning algorithm based on multilayer framework is proposed by [20] to detect botnet attacks. Filter module and classification module were used for the detection purpose of C&C botnet server. In addition, a behavior based analysis was used to analyze the captured packet's header. The behavioral features of the captured packets during a period of time were used by the proposed deep learning model by [21] to detect botnet attacks. The proposed model is able to classify the detected botnets into categories. Another deep learning algorithm is proposed by [22] to detect botnet attacks in the IoT environment. The proposed algorithm is able to handle imbalanced data using Synthetic Minority Oversampling Technique (SMOTE). The bot-IoT dataset is used by the authors to train and test the proposed algorithm. A two-level deep learning framework is proposed by [23] to detect botnet attacks in IoT networks of smart cities. The framework is able to distinguish the botnet behavior from the legitimate behavior at the application layer of the DNS services. A graph features-based machine learning model is proposed by [24] to detect botnet attacks over networks. CTU-13 and IoT-23 datasets were used to evaluate the proposed model. The model showed the ability to detect the families of the botnets in addition to the ability of facing the zero-day attacks. After testing different machine learning algorithms, authors decided to use ExtraTrees classifier with Pearson's correlation features subset in their proposed model. The authors of [25] put forward an adaptive online learning strategy to detect IoT botnet attacks in real-time. In addition, authors utilized online ensemble learning alongside the proposed adaptive strategy. A real IoT traffic dataset is used to train and test the proposed model.

2.1 The general approach of Bot-IoT detection

Figure 1 illustrates the general scheme of the bot-IoT detection process explaining the steps that will be followed in general to evaluate the machine learning algorithms. Hence, in the real environment, the first step is to capture the IoT network traffic. The next step is to extract the features (parameters) from the

captured packets to be used later (i.e., by the classifier) in the detection process. Therefore, it's vital to capture packets of the IoT network traffic as much as possible to increase the collected information ratio which, as a result, will affect final detection results.

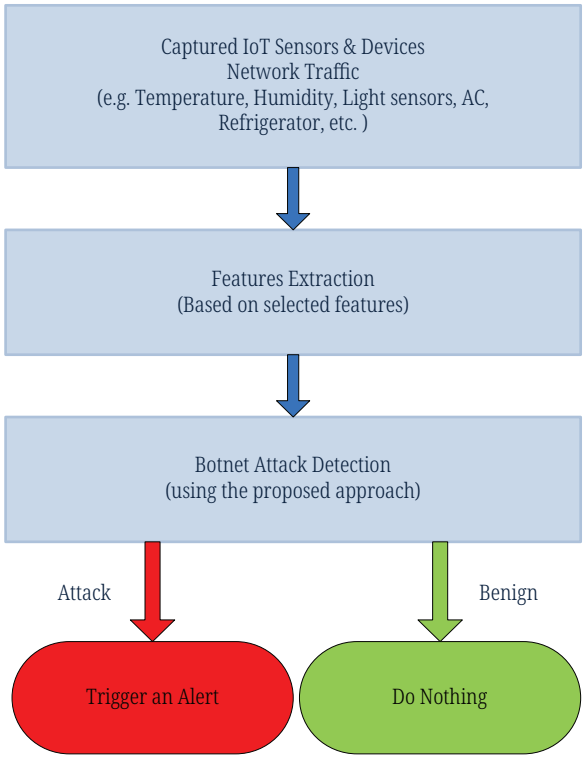

Fig. 1. General scheme of the IoT botnet detection approach

3 METHODOLOGY

3.1 Datasets

As it's difficult to setup a testbed to generate a realistic IoT traffic and simulate bot traffic, we chose to use a well-known benchmark dataset used by literature to evaluate different machine learning approaches [26]. Many researchers used the bot-IoT dataset to evaluate their proposed models. Therefore, we selected bot-IoT dataset for the evaluation purpose. The boT-IoT [27] dataset was developed in the Cyber Range Lab of the Australian Center for Cyber Security (ACCS) using the tshark tool. The collected traffic includes a mix of normal and abnormal (bot) traffic. Ostinato tool and Node-red were used to produce the simulated network traffic. The dataset contains four different types of attacks, namely DDoS, DoS, Scan (probe), and Information theft. The original dataset size is 17 GB. However 5% of the dataset is available for the evaluation of Machine Learning models [28], where reducing the number of used features in both training and testing ML models will reduce the amount of needed resources and, as a result, reduce the needed computing power [29]. Furthermore, to make it easier for the researchers and to achieve a good accuracy results of the training models, the dataset authors extracted a 5% of the original dataset with a total size of 1.07 GB and made it publicly available in CSV file format for academic research purposes [30].

Table 1. Features included in the bot-IoT dataset

Feature No.	Feature Name	Feature Description
1	pkSeqID	Row Identifier
2	proto	Protocol Name
3	saddr	Source IP address
4	sport	Source port number
5	daddr	Destination IP Address
6	dport	Destination port number
7	seq	sequence number
8	stddev	Standard deviation of aggregated records
9	N_IN_Conn_P_SrcIP	Number of inbound connections per source IP
10	min	Minimum duration of aggregated records
11	state_number	Numerical representation of feature state
12	mean	Average duration of aggregated records
13	N_IN_Conn_P_DstIP	Number of inbound connections per destination IP
14	drate	Destination-to-source packets per second
15	srate	Source-to-destination packets per second
16	max	Maximum duration of aggregated records

Table 1 shows the features (attributes) included in the bot-IoT dataset. The number of used features will differ based on the three scenarios, which will be discussed later in this paper.

3.2 Data preprocessing

To conduct the experiment, we analyzed and prepared the dataset to be suitable for the machine learning training and testing processes. Therefore, unnecessary features (i.e., attack subcategory) were taken out of the dataset and the nominal and string features have been converted to numerical values to suit the used classifiers (i.e. TCP-0, UDP-1, etc.) [31]. The 10-fold cross validation is used to evaluate the machine learning algorithms. Figure 2 illustrates the proposed framework to analyze the bot-IoT detection using different machine learning algorithms.

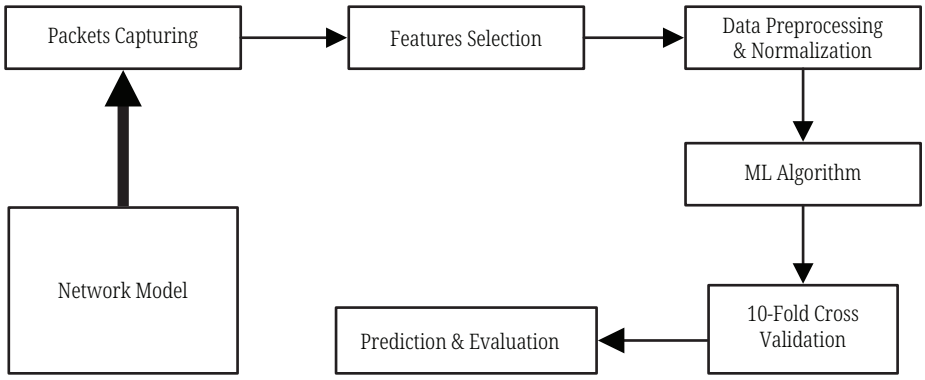

Fig. 2. The Proposed framework for bot-IoT attack detection analysis

4 EXPERIMENTS AND RESULTS DISCUSSION

Three scenarios have been used to evaluate six machine learning algorithms. The first scenario will be conducted using all dataset parameters, and in the second scenario, Information Gain algorithm is used to select the most significant parameters of the dataset. However, in the third scenario, the experiment will rely on source packet parameters. The six machine learning algorithms, namely REPTree, RandomTree, RandomForest, J48, metaBagging, and Naive Bayes, have been tested and evaluated using bot-IoT dataset. In addition, the confusion matrix is used to compare their performance.

4.1 Scenario #1: Experiment with all available parameters

In this section, the experiment will be conducted based on the extracted parameters (all parameters introduced by boT-IoT dataset) from the connection packets between attacker and the targets using six machine learning techniques. As shown in Figure 3, the results of the six classifiers are convergent with slight differences. For instance, Naive Bayes showed the least accuracy and TP rate ratios while the other five classifiers showed 100% of accuracy and TP rate. Whereas in terms of ROC Area, the RandomForest and Naive Bayes classifiers showed the best performance with ratio of 100%. Besides, with 0.2732%, Naive Bayes showed the poorest results in terms of correct instances classification.

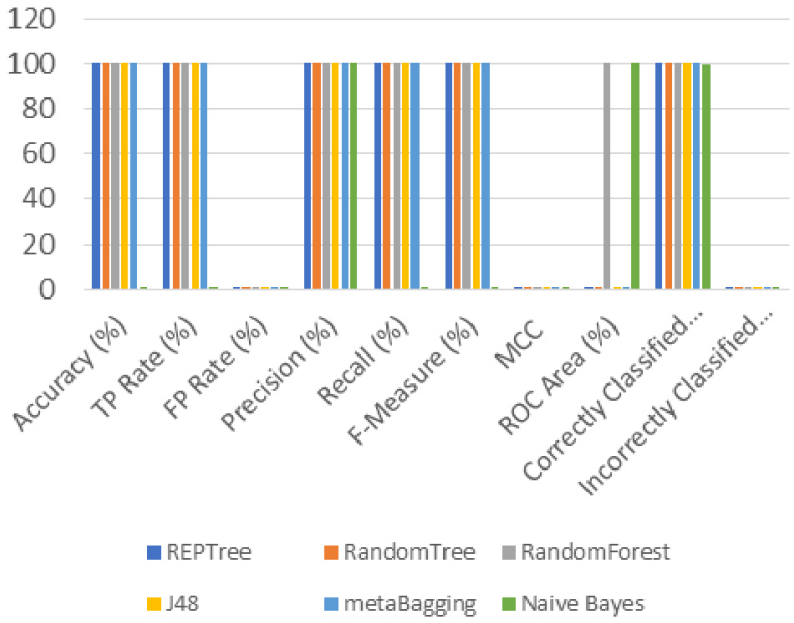

Fig. 3. Testing results using all dataset parameters

4.2 Scenario #2: Experiment with parameters reduction using information gain algorithm

Equation 1 describes the Information Gain algorithm, which is used to evaluate and reduce the number of used parameters. Table 2 illustrates the results of using

IG algorithm for the purpose of parameters reduction. Nine parameters with ranks greater than 0.0005 have been selected to be used in the classifiers testing phase.

$$\text{InfoGain(Class, Attribute)} = H(\text{Class}) - H(\text{Class} \mid \text{Attribute}) \quad (1)$$

Where:
H: represents the Entropy
Class: whether legitimate, suspicious or phishing websites
Attribute: denotes the features

Table 2. Selected features using IG algorithm

P#	P-Name
1	pkSeqID
5	daddr
6	dport
10	state_number
11	N_IN_Conn_P_DstIP
13	srate
8	N_IN_Conn_P_SrcIP
3	saddr
7	seq

Figure 4 shows the results of classifiers testing using the nine parameters selected using IG algorithm. On the first hand, the classifiers showed very good results on comparing with each other. On the other hand, Naive Bayes classifier showed the least performance compared to the other five classifiers in term of Accuracy, TP Rate, Recall, F-Measure, MCC, CCI, and ICI, with ratios 0.997%, 0.997%, 0.997%, 0.999%, 0.209%, 99.7261%, and 0.2739%, respectively. Here it showed a superior performance in terms of FP Rate, Precision, ROC area with ratios of 0.003%, 100%, 100%, respectively.

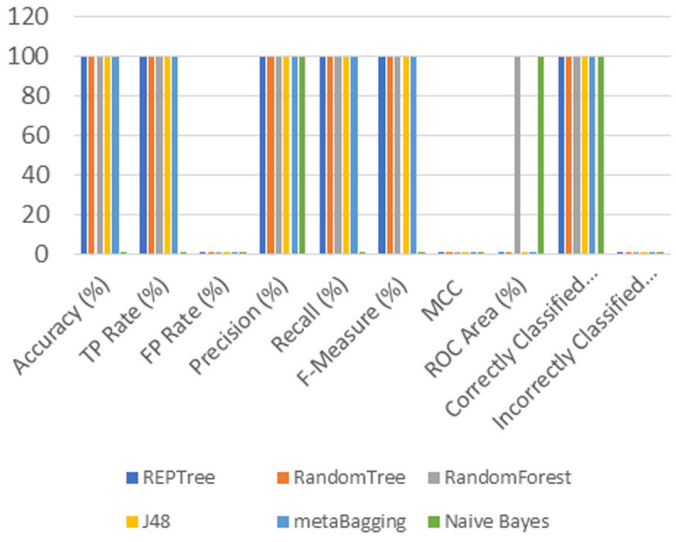

Fig. 4. Testing results using IG parameters reduction algorithm

4.3 Scenario #3: Experiment with source packets parameters

In this section, the experiment will be conducted based on the extracted parameters from the attacker source packets using six machine learning techniques. proto, saddr, sport, N_IN_Conn_P_SrcIP, srate are the five parameters that will be extracted from the attacker source packets to be used to detect the botnet attacks in the bot-IoT dataset. As illustrated in Figure 5, RandomTree classifier showed the best performance among the other five classifiers with following results; 100%, 100%, 0.23%, 100%, 100%, 100%, 0.791%, 0.838%, 99.9949%, 0.0051%, respectively. On the other hand, Naive Bayes classifier showed the least performance in terms of FP Rate, MCC, CCI, ICI with ratios of 0.776, 0.195, 99.9764, 0.0236, respectively.

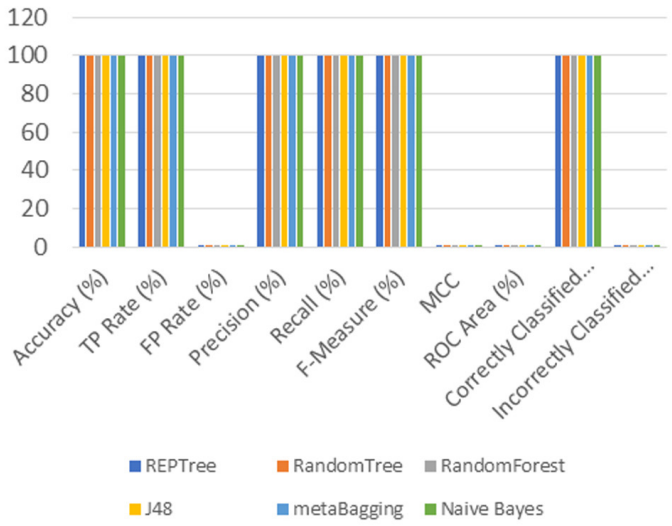

Fig. 5. Testing results using attacker source packets parameters

5 CONCLUSION

In this study, we investigated and examined six machine learning techniques for detecting Botnet attacks in the IoT context. The algorithms that have been tried include REPTree, RandomTree, RandomForest, J48, metaBagging, and Naive Bayes. The six machine learning methods are evaluated using the boT-IoT benchmark dataset, which is a well-known benchmark dataset. The results showed that the RandomForest Classifier outperformed the other examined classifiers in scenario number one. When compared to the other examined classifiers, the RandomTree classifier produced the best results in scenarios 2 and 3. Therefore, it's recommended to use the RandomTree classifier in the IoT environment to detect botnet activities. In the future, additional datasets will be explored to evaluate machine learning techniques. In addition, new machine learning classifiers will be tested in future research.

6 ACKNOWLEDGMENT

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

7 REFERENCES

[1] P. P. Ray, "A survey on internet of things architectures," *Journal of King Saud University-Computer and Information Sciences,* vol. 30, pp. 291–319, 2018. https://doi.org/10.1016/j.jksuci.2016.10.003

[2] J. H. Nord, A. Koohang, and J. Paliszkiewicz, "The internet of things: Review and theoretical framework," *Expert Systems with Applications,* vol. 133, pp. 97–108, 2019. https://doi.org/10.1016/j.eswa.2019.05.014

[3] M. K. Shambour and A. Gutub, "Progress of IoT research technologies and applications serving Hajj and Umrah," *Arabian Journal for Science and Engineering,* pp. 1–21, 2022.

[4] A. Reshan and M. Saleh, "IoT-based application of information security triad," *International Journal of Interactive Mobile Technologies,* vol. 15, pp. 61–76, 2021. https://doi.org/10.3991/ijim.v15i24.27333

[5] B. K. Sovacool and D. D. F. Del Rio, "Smart home technologies in Europe: A critical review of concepts, benefits, risks and policies," *Renewable and Sustainable Energy Reviews,* vol. 120, p. 109663, 2020. https://doi.org/10.1016/j.rser.2019.109663

[6] P. K. Malik, R. Sharma, R. Singh, A. Gehlot, S. C. Satapathy, W. S. Alnumay, *et al.*, "Industrial internet of things and its applications in industry 4.0: State of the art," *Computer Communications,* vol. 166, pp. 125–139, 2021. https://doi.org/10.1016/j.comcom.2020.11.016

[7] P. Ajay, B. Nagaraj, B. M. Pillai, J. Suthakorn, and M. Bradha, "Intelligent ecofriendly transport management system based on iot in urban areas," *Environment, Development and Sustainability,* pp. 1–8, 2022. https://doi.org/10.1007/s10668-021-02010-x

[8] A. H. Aljammal, H. Bani-Salameh, A. Qawasmeh, A. Alsarhan, and A. F. Otoom, "A new technique for data encryption based on third party encryption server to maintain the privacy preserving in the cloud environment," *International Journal of Business Information Systems,* vol. 28, pp. 393–403, 2018. https://doi.org/10.1504/IJBIS.2018.10014630

[9] O. Alfandi, S. Khanji, L. Ahmad, and A. Khattak, "A survey on boosting IoT security and privacy through blockchain: Exploration, requirements, and open issues," *Cluster Computing,* vol. 24, pp. 37–55, 2021. https://doi.org/10.1007/s10586-020-03137-8

[10] H. A. Abdul-Ghani and D. Konstantas, "A comprehensive study of security and privacy guidelines, threats, and countermeasures: An IoT perspective," *Journal of Sensor and Actuator Networks,* vol. 8, p. 22, 2019. https://doi.org/10.3390/jsan8020022

[11] S. N. Mohanty, K. Ramya, S. S. Rani, D. Gupta, K. Shankar, S. Lakshmanaprabu, *et al.*, "An efficient lightweight integrated blockchain (ELIB) model for IoT security and privacy," *Future Generation Computer Systems,* vol. 102, pp. 1027–1037, 2020. https://doi.org/10.1016/j.future.2019.09.050

[12] M. Shafiq, Z. Tian, A. K. Bashir, X. Du, and M. Guizani, "CorrAUC: A malicious bot-IoT traffic detection method in IoT network using machine-learning techniques," *IEEE Internet of Things Journal,* vol. 8, pp. 3242–3254, 2020. https://doi.org/10.1109/JIOT.2020.3002255

[13] J. L. Leevy, J. Hancock, T. M. Khoshgoftaar, and J. Peterson, "Detecting information theft attacks in the bot-IoT dataset," in *2021 20th IEEE International Conference on Machine Learning and Applications (ICMLA)*, 2021, pp. 807–812. https://doi.org/10.1109/ICMLA52953.2021.00133

[14] M. I. Alghamdi, "Survey on applications of deep learning and machine learning techniques for cyber security," *International Journal of Interactive Mobile Technologies,* vol. 14, pp. 210–224, 2020. https://doi.org/10.3991/ijim.v14i16.16953

[15] I. Ullah and Q. H. Mahmoud, "Design and development of a deep learning-based model for anomaly detection in IoT networks," *IEEE Access,* vol. 9, pp. 103906–103926, 2021. https://doi.org/10.1109/ACCESS.2021.3094024

[16] T. Hasan, J. Malik, I. Bibi, W. U. Khan, F. N. Al-Wesabi, K. Dev, *et al.*, "Securing industrial internet of things against botnet attacks using hybrid deep learning approach," *IEEE Transactions on Network Science and Engineering,* 2022. https://doi.org/10.36227/techrxiv.19313318

[17] S. Pokhrel, R. Abbas, and B. Aryal, "IoT security: Botnet detection in IoT using machine learning," *arXiv preprint arXiv:2104.02231,* 2021.

[18] M. M. Alani, "BotStop: Packet-based efficient and explainable IoT botnet detection using machine learning," *Computer Communications,* vol. 193, pp. 53–62, 2022. https://doi.org/10.1016/j.comcom.2022.06.039

[19] A. Guerra-Manzanares, H. Bahsi, and S. Nõmm, "Hybrid feature selection models for machine learning based botnet detection in IoT networks," in *2019 International Conference on Cyberworlds (CW)*, 2019, pp. 324–327. https://doi.org/10.1109/CW.2019.00059

[20] W. N. H. Ibrahim, S. Anuar, A. Selamat, O. Krejcar, R. G. Crespo, E. Herrera-Viedma, *et al.*, "Multilayer framework for botnet detection using machine learning algorithms," *IEEE Access,* vol. 9, pp. 48753–48768, 2021. https://doi.org/10.1109/ACCESS.2021.3060778

[21] W.-C. Shi and H.-M. Sun, "DeepBot: A time-based botnet detection with deep learning," *Soft Computing,* vol. 24, pp. 16605–16616, 2020. https://doi.org/10.1007/s00500-020-04963-z

[22] S. I. Popoola, B. Adebisi, R. Ande, M. Hammoudeh, K. Anoh, and A. A. Atayero, "smote-drnn: A deep learning algorithm for botnet detection in the internet-of-things networks," *Sensors,* vol. 21, p. 2985, 2021. https://doi.org/10.3390/s21092985

[23] R. Vinayakumar, M. Alazab, S. Srinivasan, Q.-V. Pham, S. K. Padannayil, and K. Simran, "A visualized botnet detection system based deep learning for the internet of things networks of smart cities," *IEEE Transactions on Industry Applications,* vol. 56, pp. 4436–4456, 2020. https://doi.org/10.1109/TIA.2020.2971952

[24] A. Alharbi and K. Alsubhi, "Botnet detection approach using graph-based machine learning," *IEEE Access,* vol. 9, pp. 99166–99180, 2021. https://doi.org/10.1109/ACCESS.2021.3094183

[25] Z. Shao, S. Yuan, and Y. Wang, "Adaptive online learning for IoT botnet detection," *Information Sciences,* vol. 574, pp. 84–95, 2021. https://doi.org/10.1016/j.ins.2021.05.076

[26] I. Apostol, M. Preda, C. Nila, and I. Bica, "IoT botnet anomaly detection using unsupervised deep learning," *Electronics,* vol. 10, p. 1876, 2021. https://doi.org/10.3390/electronics10161876

[27] N. M. Nickolaos Koroniotis. (2018, 30 Dec). *The Bot-IoT Dataset*. Available: https://research.unsw.edu.au/projects/bot-IoT-dataset

[28] N. Koroniotis, N. Moustafa, E. Sitnikova, and B. Turnbull, "Towards the development of realistic botnet dataset in the internet of things for network forensic analytics: Bot-iot dataset," *Future Generation Computer Systems,* vol. 100, pp. 779–796, 2019. https://doi.org/10.1016/j.future.2019.05.041

[29] S. Nõmm and H. Bahşi, "Unsupervised anomaly based botnet detection in IoT networks," in *2018 17th IEEE international conference on machine learning and applications (ICMLA)*, 2018, pp. 1048–1053. https://doi.org/10.1109/ICMLA.2018.00171

[30] N. M. Nickolaos Koroniotis. (2018, 30 Dec). *Bot-IoT Dataset Download Link*. Available: https://cloudstor.aarnet.edu.au/plus/s/umT99TnxvbpkkoE

[31] A. H. Aljammal, A. Qawasmeh, and H. B. Salameh, "Machine learning based phishing attacks detection using multiple datasets," *International Journal of Interactive Mobile Technologies,* vol. 17, 2023. https://doi.org/10.3991/ijim.v17i05.37575

8 AUTHORS

Ashraf H. Aljammal is currently an Associate Professor at the Department of Computer Science and Applications, The Hashemite University, Zarqa, Jordan. Dr. Aljammal received the B.S. degree in computer science from Albalqa' Applied University, Al-Salt, Jordan, in 2006, the master's degree from Universiti Sains Malaysia,

USM, Malaysia, in 2007, and the PhD degree from Universiti Sains Malaysia, USM, Malaysia, in 2011. His research interests include but are not limited to network security, cyber security, IoT security, network monitoring, cloud computing, Machine learning and Data mining (E-mail: ashrafj@hu.edu.jo).

Ahmad Qawasmeh is a native of Jordan where he studied Computer Engineering. He obtained his M.S. degree in Computer Science in 2010 and completed his PhD on performance analysis support for HPC applications in Computer Science from the University of Houston in 2015. His research interests include parallel programming languages, performance analysis, and machine learning. He joined the Hashemite University, Jordan, in 2016 as assistant professor in the Dept. of Computer Science (E-mail: ahmadr@hu.edu.jo).

Ala Mughaid was born in Irbid, Jordan, in 1984. He received the BSC degree in Computer Science from Jordan University of Science and Technology (JUST), Jordan, in 2006, and MSc in engineering degree in Computer Network from the Western Sydney University, Sydney, Australia, in 2010. Dr. Mughaid received the PhD degree in Computer Science from Newcastle University – Sydney, Australia, in 2018. In 2018, Dr. Mughaid joined the Department of Information Technology, The Hashemite University, as assistant professor, Zarqa, Jordan. Dr. Mughaid's current research interests include but are not limited to Cyber Security, Cloud Computing, Image processing, Artificial Intelligence, Virtual reality, Data Mining. He is working voluntarily in many social services (E-mail: ala.mughaid@hu.edu.jo).

Salah Taamneh is currently Associate Professor at the Department of Computer Science and its Applications, The Hashemite University, Zarqa, Jordan. He received the B.S. degree in computer science from Jordan University of Science and Technology, Irbid, Jordan, in 2005, the M.S. degree in computer science from Prairie View A&M University, Prairie View, Texas, in 2011, and the Ph.D. degree in computer science from the University of Houston, Houston, Texas, USA, in 2016. His current research interests include parallel and distributed computing, machine learning and human-computer interaction (E-mail: taamneh@hu.edu.jo).

Fadi I. Wedyan joined the Department of Computer and Mathematical sciences at Lewis University, Illinois, in 2021. He was a visiting associate professor at the department of Math. and Computer Science, Duquesne University, Pittsburgh, Pennsylvania. He also was an associate professor at the department of she oftware engineering, Hashemite University. His research interests include: Evolutionary software testing, search-based software engineering, software quality metrics, and software design. His interests also include AI applications, mainly planning, scheduling, and classification. He is also interested in mobile computing and the design and development of smartphone applications for health care, educational, and social uses (E-mail: fadi.wedyan@hu.edu.jo).

Mamoon Obiedat received BSc in Computer Science and MSc in Computer Information Systems from Yarmouk University, Jordan, in 1992 and 2005, respectively. He was a lecturer at Al-Balqa Applied University in Jordan from 1998 until he received his PhD degree in Computer Science from Lincoln University, New Zealand, in 2014. He has been a member in the Centre for Advanced Computational Solutions (CFACS) at the Lincoln University since 2011. His research interests lie in soft computing, fuzzy cognitive maps, data mining, and decision support systems. He is also interested in 3D Image Processing with MATLAB & Simulink. Obiedat also works on modeling of complex real-world problems. He is currently an Associate Professor at the Department of Information Technology in the Hashemite University (E-mail: mamoon@hu.edu.jo).