JOIV : Int. J. Inform. Visualization, 6(3) - September 2022 623-628

INTERNATIONAL JOURNAL
ON INFORMATICS VISUALIZATION

journal homepage : www.joiv.org/index.php/joiv

Identification of Mirai Botnet in IoT Environment through Denial-of-Service Attacks for Early Warning System

Alam Rahmatulloh [a], Galih Muhammad Ramadhan [a], Irfan Darmawan [b,*], Nur Widiyasono [a], Dita Pramesti [b]

[a] *Department of Informatics, Faculty of Engineering, Siliwangi University, Tasikmalaya, Indonesia*
[b] *Department of Information System, Faculty of Industrial Engineering, Telkom University, Bandung, Indonesia*
*Corresponding author: *irfandarmawan@telkomuniversity.ac.id*

***Abstract*—The development of computing technology in increasing the accessibility and agility of daily activities currently uses the Internet of Things (IoT). Over time, the increasing number of IoT device users impacts access and delivery of valuable data. This is the primary goal of cybercriminals to operate malicious software. In addition to the positive impact of using technology, it is also a negative impact that creates new problems in security attacks and cybercrimes. One of the most dangerous cyberattacks in the IoT environment is the Mirai botnet malware. The malware turns the user's device into a botnet to carry out Distributed Denial of Service (DDoS) attacks on other devices, which is undoubtedly very dangerous. Therefore, this study proposes a k-nearest neighbor algorithm to classify Mirai malware-type DDOS attacks on IoT device environments. The malware classification process was carried out using rapid miner machine learning by conducting four experiments using SYN, ACK, UDP, and UDPlain attack types. The classification results from selecting five parameters with the highest activity when the device is attacked. In order for these five parameters to be a reference in the event of a malware attack starting in the IoT environment, the results of the classification have implications for further research. In the future, it can be used as a reference in making an early warning innovative system as an early warning in the event of a Mirai botnet attack.**

***Keywords*— Classification; DDOS; Internet of Things; k-nearest neighbor; Mirai botnet.**

Manuscript received 7 Jan. 2022; revised 19 Mar. 2022; accepted 25 Apr. 2022. Date of publication 30 Sep. 2022.

I. INTRODUCTION

Internet of Things (IoT) is one of the new trends in the technology world. Simply put, IoT connects physical devices such as CCTV, lights, televisions, refrigerators, and even house doors to the Internet continuously and can be controlled remotely via a smartphone [1], monitor it [2], [3], or issue information to other devices [4], [5]. Recently, many reports of attacks on IoT device vulnerabilities have been reported [6]–[8]. However, due to its rapid development, a problem emerged that harmed IoT devices, one of which was a DDOS attack of the Mirai malware [9]–[11]. The Mirai botnet exploits current IoT device firmware vulnerabilities in the market to turn them into a network of remotely controlled bots. After being infected, Mirai IoT devices scan the network for other vulnerable devices, focusing on internet devices like IP cameras and home routers. Along with the development of DDOS attacks [12] on IoT devices that have become increasingly varied, research is needed that examines the characteristics of an attack carried out on an IoT device [13], one of which is in this study which classifies the Mirai malware attack to know the characteristics of the attack so that it can be used as an early warning system parameter.

Mirai malware attack is a malicious program [14], one of the most dangerous malwares in recent years is Mirai malware. It has even been used for the most significant DDoS attack ever recorded [15]. DDoS attacks using the Mirai botnet launched by IoT devices tend to be large and annoying [16], so addressing the Mirai botnet threat is a pressing issue.

RapidMiner learning machine is one solution to create a mechanism for detecting and identifying attacks [17]. In addition, this machine learning provides data identification functions in IoT networks [18].

This study uses a public dataset from the UCI Repository. The data tested is only the Mirai malware attack on the Internet of IoT devices, a type of security camera. The BaIoT N dataset is collected from raw network traffic data in packet capture format. Each security camera device has six datasets, and one Benign dataset is traffic data when regular traffic while the other five file types are attack traffic, namely SCAN, ACK, SYN, UDP, and UDPplain [19].

In research by Čolaković and Hadžialić [13], the classification process was carried out manually, not by machine learning, so e process became less effective and inefficient. A striking difference was also found in the data set used. The data processing is very different from the data in the study of Meidan et al. [19] in the form of packet capture on each IoT device. However, research by Čolaković and Hadžialić [13] has the advantage that the information data obtained is more complete than research by Meidan et al. [19].

This research's primary purpose is to apply the K-Nearest Neighbor algorithm in identifying Mirai botnet malware attacks, including Scan, ACK, SYN, UDP, and UDPlain, on IoT devices with security camera types. In the future, the classification results can be used as reference data for an Early warning system (EWS) on an IoT device to identify and prevent Mirai malware attacks.

II. Materials and Method

A. Related Works

Research by Čolaković and Hadžialić [13] that has been done before is a study by performing direct calculations using the K-nearest neighbor algorithm formula in detecting botnet traffic using the CTU-13 dataset. The algorithm in the study of Čolaković and Hadžialić [13] was used to detect the Mirai malware attack anomaly. In contrast to the research by Meidan et al. [19], which was used to detect the characteristics of the attack as an early warning system [13], using eight types of botnets/malwares (Zeus, Conficker, Dridex, Necurs, Miuref, Bunitu, Upatre, and Trickbot. Research by Čolaković and Hadžialić [13] has the advantage that the results can be measured at the level of accuracy due to manual calculations.

Research by Čolaković and Hadžialić [13] and Meidan et al. [19] employed the same public datasets, namely from the UCI library. However, the attacks and the data content are different. For example, research by Meidan et al. [19] uses a dataset from network traffic logs, while the research that will do the dataset is in the form of packet capture logs of the Mirai malware attack on the Internet of Things device architecture, a security camera.

B. Method

The method used in implementing this algorithm uses four stages in Figure 1: literature study, data collection, process data, and modeling.

Fig. 1 Research Flowchart

1) Study of literature: This literature study's stage describes the theory, findings, and other research materials obtained from international journals and national journals [20]. This literature study will be used as the basis for research activities in developing a clear frame of mind from the formulation of the problem to be studied. The literature study used is a journal on malware attack analysis and machine learning.

2) Data Collection: at this stage, data collection is collected from various sources [21]. The sources used are only public datasets from the UCI Repository. All information in the dataset is collected and organized by function and type. The process of collecting data in the study is described in Figure 2.

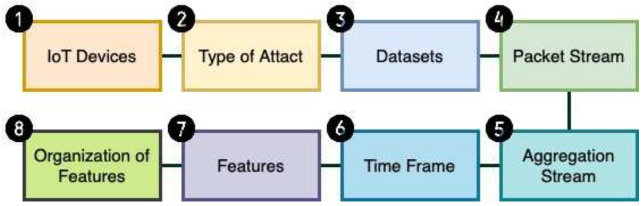

Fig. 2 Data Collection Stages

- IoT Devices: At this stage, collect and determine the Internet of things devices selected for research.

TABLE I
IoT DEVICES

IoT Devices	Specifications
Provision PT-737E	- Wireless support 802.11b/g/n - Port 80 UDP - Camera Quality 1MP(720p) - Kode Pro 7
Provision PT-838	- Wireless support 802.11b/g/n - Port 80 UDP - Camera Quality 2MP(1080p) - Kode Pro 8
SimpleHome XCS7-1002-WHT	- Wireless support 802.11b/g/n - Port 80 UDP - Camera Quality 1MP(720p) - Kode Sam 7
SimpleHome XCS7-1003-WHT	- Wireless support 802.11b/g/n - Port 80 UDP - Camera Quality 1MP(720p) - Kode Sam 8

Table 1 is a list of IoT devices infected with the Mirai botnet. Four IoT devices are infected with the Mirai Botnet in the N-BaIoT dataset.

Type of Attack: at this stage, collects and determines the type of DDOS attack be investigated. Mirai attack is the choice chosen for research.

TABLE II
TYPE OF ATTACK

Attack	**Description**
Scan	Scanning vulnerable IoT devices
ACK	Flooding IoT devices by sending spoofed ACK packets
SYN	Flooding IoT devices by sending SYN packets
UDP	Flooding IoT devices with IP packets that contain UDP datagrams
UDPplain	UDP attacks but with a higher number of packages

Table 2 is a type of Mirai botnet attack launched on IoT devices. The four types of Mirai botnet attacks on how they work are flooding the IoT device server, and the remaining type of attack is scanning vulnerable IoT devices automatically.

Datasets: at this stage, collect and determine the data set in which there is already a collection of research source data and instructions for conducting research.

Table 3 shows the number of attacks on the dataset detection of IoT botnet attacks (N-BaIoT) on each IoT device. Each device has six datasets, consisting of one standard traffic dataset (Benign) and five Mirai attack traffic datasets (Scan, ACK, SYN, UDP, and UDPplain).

TABLE III
DATASET

Kode	Benign	Scan	ACK	SYN	UDP	UDPPlan
Pro 7	✓	✓	✓	✓	✓	✓
Pro8	✓	✓	✓	✓	✓	✓
Sam 2	✓	✓	✓	✓	✓	✓
Sam 3	✓	✓	✓	✓	✓	✓

Packet Stream: this is the sub-data residing in the data set. Eight statistics are extracted from the packet stream in the N BaIoT dataset.

TABLE IV
PACKET STREAM

Packet Stream	Description
Weight	The flow is big
Mean	Average incoming flow
Variance	Incoming flow variation
Std	Standard deviation
Magnitude	The sum of the square roots of the two streams mean
Radius	The sum of the square roots of the two variance streams
Covariance	The estimated covariance between the two streams
Pcc	The estimated correlation coefficient between the two streams

Table 4 lists the various types of packet flows and their descriptions. This packet flow is contained in the aggregation. The packet flow value is a numeric number converted from raw network traffic. Aggregation Stream: table 5 shows the breakdown of aggregation streams. These five aggregations are the most recent traffic recorded.

TABLE V
AGGREGATION STREAM

Code	**Category**	**Description**
MI	Host-MAC&IP	Latest traffic statistics from the packet host (MAC and IP address)
H	Host-IP	Recent traffic statistics from packet hosts (IP address)
HH	Channel	Latest traffic statistics from the packet host (IP address) to the packet destination host
HH_jit	Network Jitter	Jitter statistics of the traffic that occurs from the packet host (IP address) to the packet destination host
HpHp	Socket	Recent traffic statistics from host + port (IP address) of packets to host + port of destination of packets.

Time Frame: This table 6 is the time frame contained in the features in the dataset. The five-times time frame is used to detect the Mirai malware in real time.

TABLE VI
TIME FRAME

Item	Description
L5	1 minute
L3	10 second
L1	1,5 second
L0.1	500 millisecond
L0.01	100 millisecond

Features: the features contained in each dataset this feature consists of 23 main features and five frames (1 minute, 10 seconds, 1.5 seconds, 500 milliseconds, and 100 milliseconds). The number of features in each dataset is 115 features.

TABLE VIII
FEATURES

Code	Time Frame	Packet Stream							
		Weight	Mean	Variance	Std	Magnitude	Radius	Covariance	PCC
MI	L5	✓	✓	✓					
	L3	✓	✓	✓					
	L1	✓	✓	✓					
	L0.1	✓	✓	✓					
	L0.01	✓	✓	✓					
H	L5	✓	✓	✓					
	L3	✓	✓	✓					
	L1	✓	✓	✓					
	L0.1	✓	✓	✓					
	L0.01	✓	✓	✓					
HH/Jit	L5	✓	✓	✓					
	L3	✓	✓	✓					
	L1	✓	✓	✓					
	L0.1	✓	✓	✓					
	L0.01	✓	✓	✓					
HH	L5	✓	✓		✓	✓	✓	✓	✓
	L3	✓	✓		✓	✓	✓	✓	✓
	L1	✓	✓		✓	✓	✓	✓	✓
	L0.1	✓	✓		✓	✓	✓	✓	✓
	L0.01	✓	✓		✓	✓	✓	✓	✓
HpHp	L5	✓	✓		✓	✓	✓	✓	✓
	L3	✓	✓		✓	✓	✓	✓	✓
	L1	✓	✓		✓	✓	✓	✓	✓
	L0.1	✓	✓		✓	✓	✓	✓	✓
	L0.01	✓	✓		✓	✓	✓	✓	✓

Table 7 lists features in the database, which contains a combination of a packet stream, aggregation stream, and time frame. The organization of feature datasets based on package statistics can be seen in table 8. The organization of these features has four groups.

TABLE VIII
ORGANIZATION OF FEATURE

Aggregate	Count	Jitter	Outbound Size	Combined Size
MI	Weight	-	Mean, Variance	-
H	Weight	-	Mean, Variance	-
HH	Weight	Weight, Mean-Variance	Mean, Variance	Magnitude, Radius, Covariance, PCC
HpHP	Weight	Network Jitter	Mean, Variance	Magnitude, Radius, Covariance, PCC

3) Data Process: Data Processing is the second stage in the research, namely processing large amounts of data and unbalanced data into datasets that can be used for testing. Figure 3 shows the stages of data processing, the beginning of entering the regular traffic and traffic attack datasets. The combination produces an unbalanced dataset. Then the dataset is sampled, so the combined traffic and traffic attack datasets become balanced. However, the dimensionality of the dataset is still high. So, the features in the dataset are chosen so that the dataset becomes of low dimensionality and the level of accuracy becomes optimal. The stages of data processing use the Rapidminer application to perform data processing.

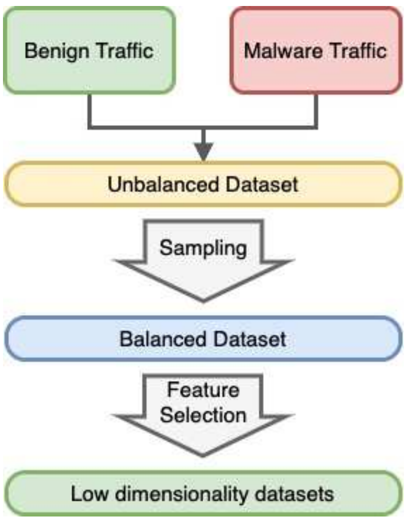

Fig. 3 Data Processing Stage

4) *Modeling:* This part is explained in next section.

III. RESULT AND DISCUSSION

A. Identification Scenario Process

The identification process involves 2 data in each data device, regular traffic (Benign) and attack traffic (ACK, SYN, UDP, UDPplain) because after testing all devices, the test results produced the same results in every type of attack on the device. So IoT then, to save time, each IoT device carries out testing against one attack.

TABLE IX
TESTING SCENARIO

Code	**Data Traffic Type**				
	Benign	**ACK**	**SYN**	**UDP**	**UDPplain**
Pro7	✓	✓	✓	✓	✓
Pro8	✓	✓	✓	✓	✓
Sam2	✓	✓	✓	✓	✓
Sam3	✓	✓	✓	✓	✓

Table 9 is a scenario of each device's identification process against the attack type; the scan data cannot be identified because it is not DDoS attack data. Instead, the scan data is only traffic data for weaknesses on IoT devices.

B. Modeling

1) *Provision PT-737E device modeling (benign & SYN attack):* Device modeling aims to make the two processed data (benign & SYN attack) into balanced data to identify them. Figure 4 is a model for selecting five parameters with the highest activity to identify syn attack-type Mirai attacks. Table 10 selects features that produce the three highest activity parameters for the Host-MAC&IP category and the two highest activity parameters for Host-IP. The five highest activity parameters have three different periods, 1.5 seconds, 500 milliseconds, and 100 milliseconds. Packet flow on the five highest activity parameters also produces 1 type, namely Weight. The five selected parameters can be interpreted as a network traffic condition of an IoT device that is attacked by the DDOS Mirai botnet. For example, if a network device is in a condition such as the five highest activity parameters selected, it can be interpreted that a DDOS Mirai syn attack has attacked the device.

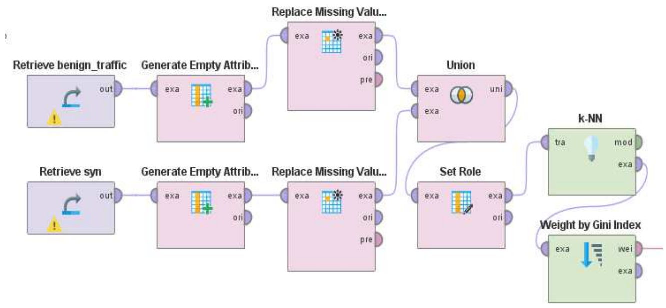

Fig. 4 Modeling Features Selection

TABLE X
SYN ATTACK CLASSIFICATION RESULTS

No	Features	Description
1	MI_dir_L0.1_Weight	Host MAC&IP 500ms
2	MI_dir.L0.01_Variance	Host MAC&IP 100ms
3	H_L0.1_Weight	Host IP 500ms
4	H_L0.01_Variance	Host IP 100ms
5	MI_dir_L1_Weight	Host MAC&IP 1,5s

2) *Provision PT-838 device modeling (benign & ACK):* Two data are processed, namely benign & ACK, to become balanced data to identify it. The feature selection model is shown in Figure 5.

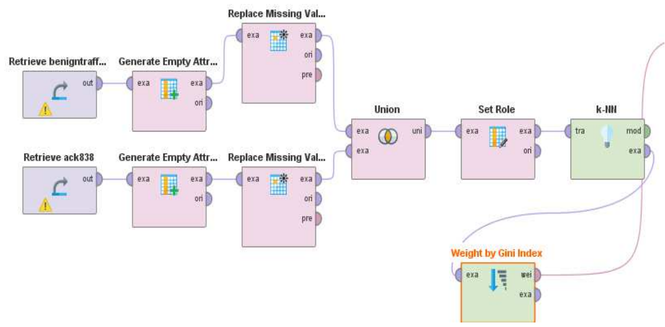

Fig. 5 Modeling Selection Feature

TABLE XI
ACK ATTACK CLASSIFICATION RESULTS

Features	**Description**
H_L0.01_Variance	Host IP 100ms
H_L0.1_Mean	Host IP 500ms
H_L0.1 Weight	Host IP 500ms
MI_dir_L0.01_Variance	Host MAC&IP 100ms
MI_dir_L0.1_Weight	Host MAC&IP 500ms

Table 11 is a selection feature that produces the two highest activity parameters for the Host-MAC&IP category and the three features Host-IP. The five highest activity parameters have two different periods, 500 milliseconds and 100 milliseconds. The packet flow on the five highest activity parameters also produces three types, namely Weight, mean, and variance. The five highest activity parameters selected can be interpreted as a network traffic condition of an IoT device attacked by a DDOS Mirai botnet ack attack. If a network device is in a condition such as the five highest activity parameters selected, a Mirai DDOS botnet ack attack can be interpreted as an attack on the device.

3) Simple Home XCS7-1002-WHT (benign & UDP attack) device modeling: Device modeling aims to make the two processed data (benign & UDP attack) into balanced data to identify them.

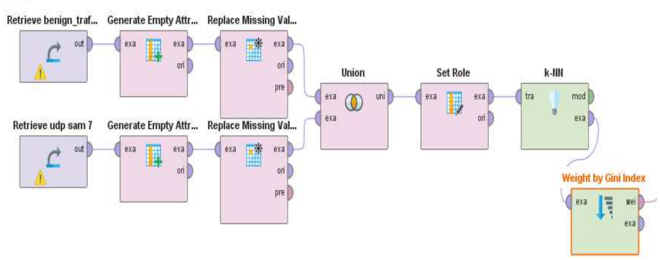

Fig. 6 Modeling Selection Feature

Fig. 6 is a model for selecting the five highest activity parameters to identify DDOS attacks. The results can be seen in Table 12.

TABLE XII
UDP ATTACK CLASSIFICATION RESULTS

Features	Description
H_L0.1_Variance	Host IP 500ms
H_L0.1_Mean	Host IP 500ms
MI_dir_L0.1_Variance	Host MAC&IP 500ms
MI_dir_L0_1_Mean	Host MAC&IP 500ms
MI_dir_L0.1_Weight	Host MAC&IP 500ms

Table 12 is a selection feature that produces the two highest activity parameters for the Host-IP category and the 3 for the Host MAC&IP category. The five highest activity parameters have one time period, namely 500 milliseconds. The packet flow on the five highest activity parameters also produces three types, namely Weight, mean, and variance. The five highest activity parameters selected can be interpreted as a network traffic condition of an IoT device attacked by the DDOS Mirai botnet UDP attack. If a network device is in a condition such as the five highest activity parameters selected, it can be interpreted as being attacked by the DDOS Mirai botnet UDP attack.

4) Simple Home XCS7-1003-WHT (benign & UDPplain attack) device modeling: The modeling of the processed device is benign & the UDPplain is seen in Figure 7.

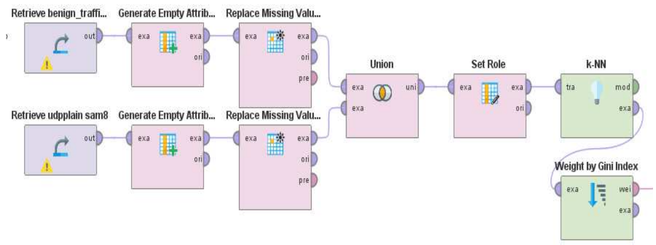

Fig. 7 Modeling Selection Feature

TABLE XIII
UDP PLAIN ATTACK CLASSIFICATION RESULTS

Features	Description
H_L0.01_Weight	Host IP 100ms
H_L0.01_Weight	Host IP 100ms
H_L1_Weight	Host IP 1,5s
MI_dir_L0.01_Weight	Host MAC&IP 100ms
MI_dir_L0.1_Weight	Host MAC&IP 500ms

Table 13 is a selection feature that produces one parameter of the highest activity in the Host-MAC & IP category. The five highest activity parameters have three time periods, 500 milliseconds, 100 milliseconds, and 1.5 seconds. Packet flow on the five highest activity parameters also produces 1 type, namely Weight. The five highest activity parameters selected can be interpreted as a network traffic condition of an IoT device attacked by the DDOS Mirai botnet.

C. *Overall Classification Results*

Table 14 is the result of classifying the five highest activity parameters as device parameters when exposed to DDOS attacks. The selection of the highest activity parameter can be used for the Early warning system on a device because it can be used as a parameter for the condition of the device being attacked by DDOS or not. So that prevention and control can be carried out optimally.

TABLE XIV
CLASSIFICATION RESULTS

Attack Type	Type IoT	Device Description
Provision PT-737E	SYN Attack	- Host IP&MAC 500ms (Weight) - Host MAC&IP 100ms (Weight) - Host IP 500ms (Weight) - Host IP 100ms (Weight) - Host MAC&IP 1,5s (Weight)
Provision PT-838	ACK Attack	- Host IP 100ms (Varians) - Host IP 100ms (Weight) - Host IP 500ms (Weight) - Host MAC&IP 100ms (Varians) - Host MAC&IP 500ms (Weight)
simple home XCS7-1002-WHT	UDP Attack	- Host IP 100ms (Varians) - Host IP 100ms (Mean) - Host IP 100ms (Weight) - Host IP 500ms (Mean) - Host IP 500ms (Weight)
SimpleHome XCS-1003-WHT	UDP plain	- Host IP 100ms (Weight) - Host IP 100ms (Weight) - Host IP 1,5s (Weight) - Host MAC&IP 100ms (Weight) - Host MAC&IP 500ms (Weight)

IV. Conclusion

Based on the test results, the K-Nearest Neighbor algorithm has successfully classified DDOS attacks from all types of attacks, namely SYN, ACK, UDP, and UDPplain. Furthermore, all test results on these IoT devices have the same characteristics when tested with several DDOS attacks. This proves that the identification of the Mirai malware has been successfully carried out so that further development of the parameters obtained can be used for the Early Warning System for detecting the Mirai botnet malware in the IoT environment.

References

[1] A. A. Karia, L. V. Budhwani, and V. S. Badgujar, "IoT-Key Towards Automation," *2018 International Conference on Smart City and Emerging Technology, ICSCET 2018*, pp. 1–5, 2018. DOI: 10.1109/ICSCET.2018.8537261.

[2] A. Rahmatulloh, F. M. S. Nursuwars, I. Darmawan, and G. Febrizki, "Applied Internet of Things (IoT): The Prototype Bus Passenger Monitoring System Using PIR Sensor," in *2020 8th International Conference on Information and Communication Technology (ICoICT)*, 2020, pp. 617–622.

[3] F. M. S. Nursuwars and A. Rahmatulloh, "RFID for nurse activity monitoring in the hospital's nurse call system with Internet of Thing (IoT) concept," in *IOP Conference Series: Materials Science and Engineering*, 2019, vol. 550, p. 012025 [Online]. DOI: 10.1088/1757-899X/550/1/012025.

[4] A. Rahmatulloh, R. Gunawan, H. Sulastri, I. Pratama, and I. Darmawan, "Face Mask Detection using Haar Cascade Classifier Algorithm based on Internet of Things with Telegram Bot Notification," in *2021 International Conference Advancement in Data Science, E-learning and Information Systems (ICADEIS)*, 2021, pp. 1–6. DOI: 10.1109/ICADEIS52521.2021.9702065.

[5] N. Widiyasono, A. Rahmatulloh, and H. Firmansah, "Automatic Email Alert on the Internet of Things-based Smart Motion Detection System," in *Selected Papers from the 1st International Conference on Islam, Science and Technology, ICONISTECH-1 2019, 11-12 July 2019, Bandung, Indonesia*, 2020. DOI: 10.4108/eai.11-7-2019.2297829.

[6] K. Angrishi, "Turning Internet of Things(IoT) into Internet of Vulnerabilities (IoV) : IoT Botnets," Feb. 2017 [Online]. Available: http://arxiv.org/abs/1702.03681.

[7] E. Bertino and N. Islam, "Botnets and Internet of Things Security," *Computer*, vol. 50, no. 2, pp. 76–79, Feb. 2017. DOI: 10.1109/MC.2017.62.

[8] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "DDoS in the IoT: Mirai and Other Botnets," *Computer*, vol. 50, no. 7, pp. 80–84, 2017. DOI: 10.1109/MC.2017.201.

[9] G. B. Gunawan, P. Sukarno, and A. G. Putrada, "Pendeteksian SeranganDenial of Service(DoS) pada Perangkat Smartlock Berbasis WifiMenggunakan SNORT IDS," *e-Proceeding of Engineering*, vol. 5, no. 3, 2018.

[10] O. Toutsop, S. Das, and K. Kornegay, "Exploring The Security Issues in Home-Based IoT Devices Through Denial of Service Attacks," in *2021 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/IOP/SCI)*, 2021, pp. 407–415. DOI: 10.1109/SWC50871.2021.00062.

[11] A. Marzano *et al.*, "The Evolution of Bashlite and Mirai IoT Botnets," in *2018 IEEE Symposium on Computers and Communications (ISCC)*, 2018, pp. 00813–00818. DOI: 10.1109/ISCC.2018.8538636.

[12] M. Antonakakis *et al.*, "Understanding the Mirai Botnet," in *Proceedings of the 26th USENIX Security Symposium*, 2017.

[13] A. Čolaković and M. Hadžialić, "Internet of Things (IoT): A review of enabling technologies, challenges, and open research issues," *Computer Networks*, vol. 144, pp. 17–39, 2018 [Online]. DOI: 10.1016/j.comnet.2018.07.017.

[14] K. B. Aswathi, S. Jayadev, N. Krishna, R. Krishnan, and G. Sarath, "Botnet Detection using Machine Learning," in *2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, 2021, pp. 1–7. DOI: 10.1109/ICCCNT51525.2021.9579508.

[15] "Mirai IoT botnet code release raises fears of surge in DDoS attacks." [Online]. Available: https://www.computerweekly.com/news/450400311/Mirai-IoT-botnet-code-release-raises-fears-of-surge-in-DDoS-attacks.

[16] H.-D. Huang, T.-Y. Chuang, Y.-L. Tsai, and C.-S. Lee, "Ontology-based intelligent system for malware behavioral analysis," in *International Conference on Fuzzy Systems*, 2010, pp. 1–6. DOI: 10.1109/FUZZY.2010.5584325.

[17] D. P. Ismi, S. Panchoo, and M. Murinto, "K-means clustering based filter feature selection on high dimensional data," *International Journal of Advances in Intelligent Informatics*, vol. 2, no. 1, p. 38, Mar. 2016. DOI: 10.26555/ijain.v2i1.54.

[18] B. Abraham, A. Mandya, R. Bapat, F. Alali, D. E. Brown, and M. Veeraraghavan, "A Comparison of Machine Learning Approaches to Detect Botnet Traffic," in *2018 International Joint Conference on Neural Networks (IJCNN)*, 2018, pp. 1–8. DOI: 10.1109/IJCNN.2018.8489096.

[19] Y. Meidan *et al.*, "N-BaIoT: Network-based Detection of IoT Botnet Attacks Using Deep Autoencoders," May 2018 [Online]. DOI: 10.1109/MPRV.2018.03367731.

[20] T. P. Setia, A. P. Aldya, and N. Widiyasono, "Reverse Engineering untuk Analisis Malware Remote Access Trojan," *Jurnal Edukasi dan Penelitian Informatika (JEPIN)*, vol. 5, no. 1, p. 40, Apr. 2019. DOI: 10.26418/jp.v5i1.28214.

[21] S. Nomm and H. Bahsi, "Unsupervised Anomaly Based Botnet Detection in IoT Networks," in *2018 17th IEEE International Conference on Machine Learning and Applications (ICMLA)*, 2018, pp. 1048–1053. DOI: 10.1109/ICMLA.2018.00171.