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.

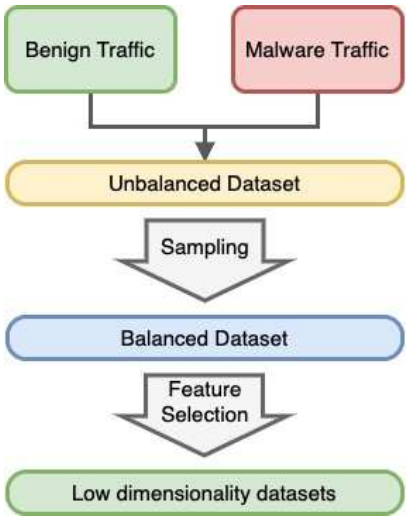

Fig. 3 Data Processing Stage

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.

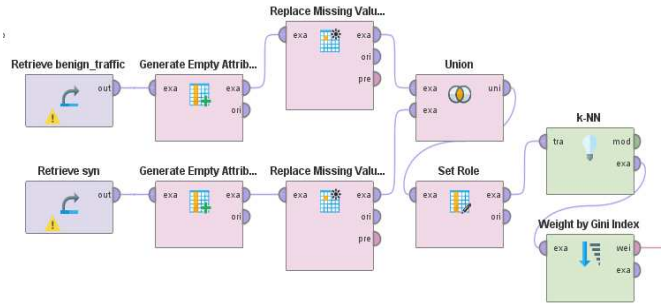

Fig. 4 Modeling Features Selection

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.

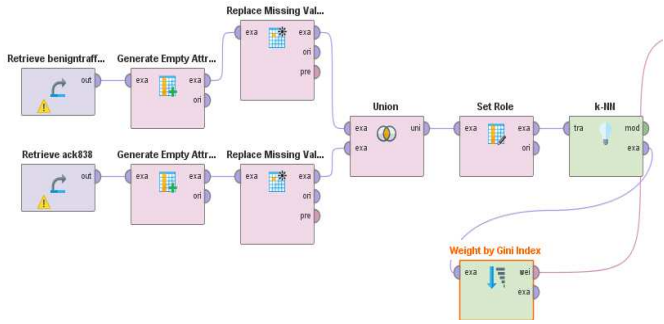

Fig. 5 Modeling Selection Feature

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.

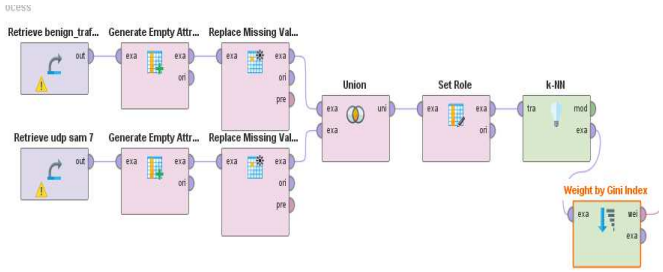

Fig. 6 Modeling Selection Feature

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.

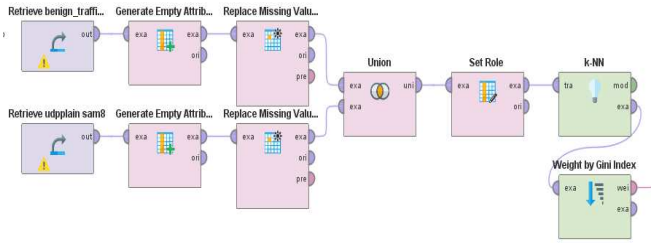

Fig. 7 Modeling Selection Feature

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.