Turkish Journal of Science & Technology
18(1), 113-122, 2023

Research Paper
https://doi.org/10.55525/tjst.1196878

Threats Detection in IoT Network

Hanan ABU KWAİDER [1*], Erdinç AVAROĞLU [2]
[1] Msc. Department of Computer Engineering, Mersin University, Mersin, TURKEY
[2] Associated Professor, Department of Computer Engineering, Mersin University, Mersin, TURKEY
[*1] hanan.abukwaider@gmail.com, [2] eavaroglu@mersin.edu.tr

(Geliş/Received: 31/10/2022; Kabul/Accepted: 08/02/2023)

Abstract: The recent growth in Internet of Things (IoT) deployment has increased the rapidness of integration and extended the reach of the internet from computers, tablets, and phones to countless devices in our physical world. This growth makes our life more convenient and industries more efficient. However, at the same time, it brought numerous challenges in terms of security and expanded the area of cyber-attacks, especially the DoS and DDoS attacks. Moreover, since many IoT devices run custom or outdated operating systems, and most do not have enough resources to run typical intrusion detection systems, it was necessary to search for alternative solutions. Therefore, many researchers have joined the race to develop new lightweight intrusion detection methods. In this study, we have investigated the detection of different DoS attacks on the IoT network using machine learning techniques. The studied attacks are TCP Syn-Flood Attack, UDP Flood Attack, HTTP Slowloris GET Attack, Apache Range Header DoS, and Port Scan attack. We have proposed a new dataset, namely HEIoT21, which was generated in a real smart home environment using a collective of IoT devices and non-IoT devices connected to a wireless network. The proposed dataset included normal and anomaly data, and using the CiCflowmeter application, we extracted 82 network features from the proposed dataset. The dataset was labeled and categorized into binary-class and multi-class. Our dataset underwent multiple feature selection methods to keep only enough features to produce a good detection accuracy; for that, we have used Anova F-value Feature Selection, Random Forest importance feature selection, and Sequential Forward Feature Selection. The feature selection techniques produced three new sub-datasets, which were evaluated using multiple machine learning algorithms like Logistic Regression (LR), J48 Decision Tree (DT), Naïve Bayes, and Artificial Neural Network (ANN). A comparison study was conducted on the result obtained from applying the different machine learning algorithms on the derived sub-datasets, which led to the finding that the most suitable feature selection technique for the proposed dataset was Anova F-value and the best-fit machine learning algorithm for the proposed dataset was The Decision Tree which produced an accuracy result of 99.92% for binary classification and 99.94% for multi-class classification.
In the end, our study was compared with other studies in the field of IoT intrusion detection, and we found that the result obtained through this study was higher than most others. Therefore, the proposed dataset could be of great use to those who want to work on the analysis and detection of the existing network security threats. Also, this study can be considered a cornerstone for a proper lightweight intrusion detection system, where the datasets can be expanded to include other types of attacks, new detection rules can be added, and an alert mechanism can be integrated to become a complete detection system.

Key words: Internet of things, IoT, machine learning, network security, attack detection.

IoT Ağında Saldırı Algılama

Öz: Nesnelerin İnterneti (IoT) dağıtımındaki son büyüme, entegrasyonun hızını artırdı ve internetin erişimini bilgisayarlardan, tabletlerden ve telefonlardan fiziksel dünyamızdaki sayısız cihaza genişletti.Bu gelişme hayatımızı daha rahat ve endüstrileri daha verimli hale getiriyor.Ancak güvenlik açısından da sayısız zorluğu getirdi ve başta DoS ve DDoS saldırıları olmak üzere siber saldırıların alanını genişletti.Dahası, birçok IoT cihazı özel veya yeni olmayan işletim sistemleri çalıştırdığından ve çoğu tipik Saldırı Tespit Sistemleri çalıştırmak için yeterli kaynağa sahip olmadığından, alternatif çözümlere bulmaya çalışmalıydı. Bu nedenle, birçok araştırmacı yeni hafif saldırı tespit yöntemleri ortaya atmak için yarışa katıldı.Bu çalışmada, makine öğrenimi teknikleri kullanılarak IoT ağında farklı DoS saldırılarının tespiti araştırıldı.üzerinde çalışılmış saldırıları , TCP Syn-Flood saldırı, UDP Flood saldırı , HTTP Slowloris GET saldırı , Apache Range Header DoS ve Port Scan saldırısıdır.Bir kablosuz ağa bağlı IoT cihazları ve IoT olmayan cihazlar kullanılarak gerçek bir akıllı ev ortamında oluşturulan HEIoT21 adlı yeni bir veri seti önerdik.Önerilen veri seti normal ve anomali verilerini içeriyordu, ve CiCflowmeter uygulamasını kullanarak, önerilen veri setinden 82 ağ özelliği çıkardık.Veri seti, ikili sınıf ve çoklu sınıf olarak etiketlendi ve kategorilere ayrıldı.Sınırlı IoT kaynakları sorununu çözmek için hafif bir saldırı tespit yöntemine ihtiyaç duyulduğundan.
Veri kümemizin, iyi bir tespit doğruluğu oluşturmak için yeterli olan çok az özelliğe sahip olması gerekiyordu; Bunun için üç Özellik Seçimi tekniği kullandık, Anova F-değeri özellik seçimi, Rastgele Orman önemi öznitelik seçimi ve Ardışık İleri Yönde özellik seçimi. Özellik seçimi teknikleri, Lojistik Regresyon (LR), J48 Karar Ağacı (DT), Naive Bayes ve Yapay Sinir Ağları (YSA) gibi çoklu Makine öğrenimi
algoritmaları kullanılarak değerlendirilen üç yeni alt veri kümesi oluşturdu. Türetilmiş alt veri kümesi üzerinde farklı makine öğrenimi algoritmalarının uygulanmasından elde edilen sonuç üzerinde bir karşılaştırma çalışması yapılmış ve önerilen veri

[*] Corresponding author: hanan.abukwaider@gmail.com. ORCID Number of authors: [1] 0000-0003-3887-2819, [2] 0000-0003-1976-2526

kümesi için en elverişli özellik seçim tekniğinin Anova a F değeri olduğu bulgusuna yol açmıştır. Önerilen veri kümesi için en uygun makine öğrenimi algoritması, ikili sınıflandırma için %99,92 ve çok sınıflı sınıflandırma için %99.94 doğruluk sonucu oluşturan an Karar Ağacı olmuştur.
Sonuç olarak, çalışmamız IoT saldırı tespiti alanında yapılan diğer çalışmalarla karşılaştırıldı ve bu çalışma ile elde edilen sonucun diğerlerinin çoğundan daha yüksek olduğunu gördük. Bu nedenle, önerilen veri kümesi , mevcut ağ güvenliği tehditlerinin analizi ve tespiti üzerinde çalışmak isteyenler için çok faydalı olabilir. Ayrıca, bu çalışma, veri kümelerinin diğer saldırı türlerini içerecek şekilde genişletilebildiği, yeni tespit kurallarının eklenebildiği ve eksiksiz bir tespit sistemi haline gelmek için bir uyarı mekanizmasının entegre edilebildiği, uygun bir hafif saldırı tespit sistemi için bir mihenk taşı olarak kabul edilebilir.

Anahtar kelimeler: Nesnelerin İnterneti, IoT, makine öğrenimi, ağ güvenliği, saldırı tespiti.

1. Introduction:

The security risks accompanied by the increasing demand and growth of the Internet of Things (IoT) are increasing. Some statistics mentioned that the number of IoT-connected devices is expected to grow from 15 billion in 2015 to around 75 billion devices in 2025 [1]. These numbers are raising many concerns as the area of the attacks is expanding, and the aim to access sensitive information without authorization has been troubling; Figure 1 presents IoT-connected devices worldwide.

In 2020, McAfee company reported that cybercriminals used the COVID-19 pandemic to increase the cyber-threat categories like mobile malware, IoT malware, and PowerShell malware. Moreover, McAfee has detected around 375 cyber threats per minute within the first quarter of 2020. Furthermore, as the disease spreads, critical systems such as medical IoT devices and healthcare networks become more susceptible to cyber-attacks [2].

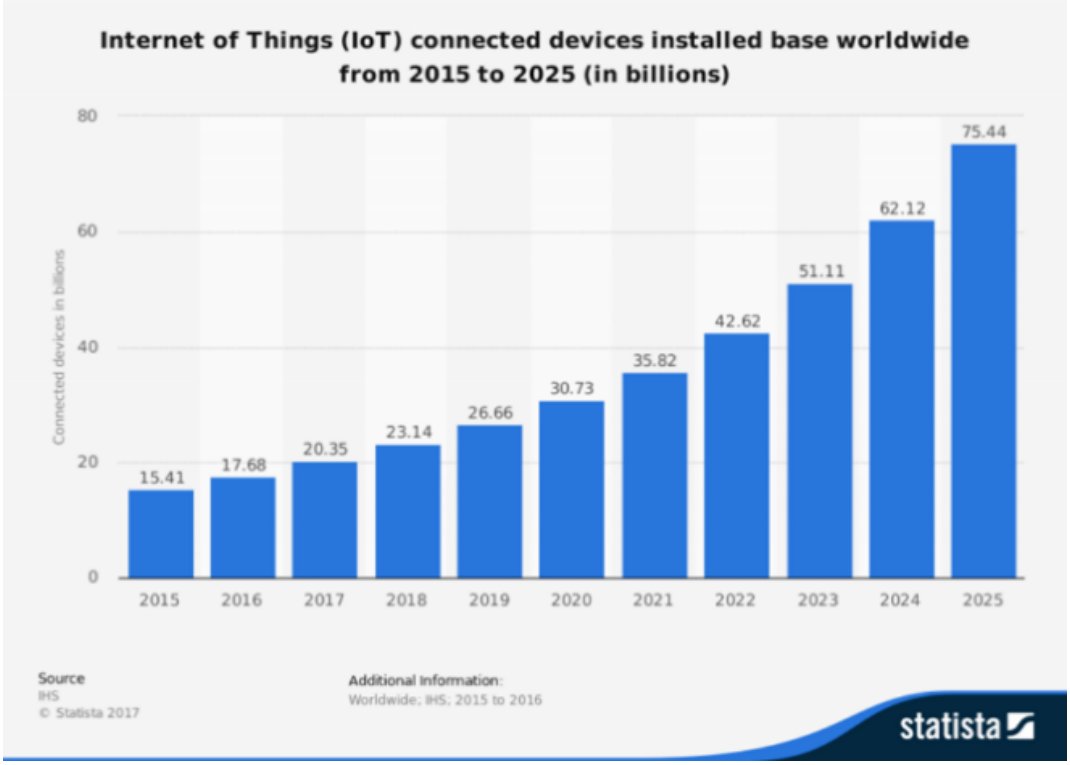

Figure 1. The number of IoT connected devices by the year

Following these facts, cybersecurity has become vital in today's research area. The need to build a detection method for IoT attacks has led many researchers to invest more time in this area, and for that purpose, many have used machine learning to achieve this goal.

In this study, the work will focus on detecting multiple IoT attacks by analyzing the packet flow in the network and extracting the needed metrics for the detection. The dataset used in this study is HEIoT21, a dataset created in a real smart home wireless environment containing normal and anomaly data with different attacks. The dataset underwent multiple feature selection methods to keep only the best features for classification. The newly created sub-datasets generated from applying the feature selections will be used as input for several machine learning algorithms to predict the probability that the IoT device is under attack or not. The result of the used algorithms will then be compared to determine the most suitable classification algorithm for the IoT network attack detection within the scope of the input. Thus, the contribution to knowledge obtained by this study is as follows:

- Building a new dataset in a smart home environment and making it available for public use to benefit other researchers [3].
- Implement and perform a performance evaluation of the used feature selection methods and the machine learning classification algorithms in terms of detecting the attacks.
- Create a comparison study between the results obtains in this study and others in the same field.

The rest of this study is structured as follows. Section two showcases a review of some related work in this field, section three discusses the methods and material used, section four presents the results obtained from this study, and finally, section five concludes the paper and shares ideas about future work.

2. Literature Summary

Since IoT network security has become an urgent matter that needs to be handled, multiple researchers have joined the race to tackle this issue either by studying the design challenges and the taxonomy of the security attacks from the network side or by using machine learning to find solutions to the current problem and against the attacks.

Teng Xu, James B. Wendt and Miodrag Potkonjak in [4] have done a brief survey on IoT challenges focusing on the security issues, they have also discussed the potential of hardware-based IoT security approaches and concluded by presenting several use case studies that advocate the use of stable PUFs (Physical Unclonable Functions) and digital PPUFs for several IoT security protocols.

The authors in [5] have proposed the use of SDN gateway as a distributed means of monitoring the traffic originating from and directed to IoT based devices. The gateway can then both detect anomalous behavior and perform an appropriate response (blocking, forwarding, or applying Quality of Service), they have successfully detected and blocked TCP and ICMP flood based attacks using the proposed gateway.

Farahnakian and Heikkonen [6] proposed a Deep Auto-Encoder-based Intrusion Detection System (DAE-IDS), and they used the KDD-CUP 99 dataset to evaluate their proposed scheme. Their schema resulted in an accuracy of 96.53% on binary classification.

Also, in [7] for DoS attack detection, Moukhafi proposed a novel hybrid genetic algorithm and support vector machine with the particle swarm optimization-based scheme. The authors used the KDD99 dataset and PSO for feature selection and got an accuracy of 96.38% on multi-class classification.

In [8], the authors used KDD CUP 99 dataset to implement their model for detecting and classifying IoT attacks using SVM and Bayesian. They achieved an accuracy of 91.50% on multi-class classification. The dataset went through feature reduction before applying the classification.

Moreover, in [9], the authors proposed a deep learning-based intrusion detection system for DDoS attacks based on three models: convolutional neural networks, deep neural networks, and recurrent neural networks. For each model, the performance was studied within two classification types (binary and multi-class) using two new real traffic datasets: the CIC-DDoS2019 dataset and the TON_IoT dataset. For the first dataset, they achieved an accuracy of 95.90% and 99.95% on multi-class classification and binary classification, respectively. For the second dataset, they achieved an accuracy of 98.94% for multi-class classification.

Furthermore, in [10], S. Latif, Z. Zou, Z. Idrees, and J. Ahmad proposed a novel lightweight random neural network (RaNN)- based prediction model capable of predicting different cybersecurity attacks. They used several evaluation parameters such as accuracy, in which they achieved 99.20% on multi-class classification, precision, recall, and F1 score, and applied their model in a dataset named DS2OS.

Also, in [11], the authors have proposed an anomalous activity detection system for IoT networks based on flow and control flags features using a feed-forward neural network. The model has been evaluated using BoT-IoT, IoT network intrusion, MQTT-IoT-IDS2020, MQTTset, IoT-23, and IoT-DS2 datasets for binary and multi-

class classification. The authors have achieved an accuracy of 99.97% and 99.99% for multi-class and binary classification, respectively.

In [12], the authors created a new dataset, IoTID20, consisting of two IoT devices and other interconnected devices such as laptops and smartphones in a typical smart home environment. Their dataset consisted of both normal and anomaly data. They removed the highly correlated features, and they used Shapira-Wilk to keep the high-ranking features only. Seven supervised machine learning algorithms were used for classification, and it was evaluated using the accuracy and F1 score. They got a high accuracy of 100% for both binary and multi-class classification.

3. Materials and Methods

This study was conducted in an IoT-based smart home environment, which provided a realistic setting for collecting and analyzing data on IoT devices and their vulnerabilities to different types of intrusions.

The first step in the study was to produce a dataset by collecting both normal and anomaly data from the network. This data was collected from various IoT devices such as smart cameras, smart appliances, and other connected devices. The collected data went through a pre-processing step to ensure that it was in the appropriate format for analysis. The data was then cleaned, and any irrelevant or redundant information was removed.

The next step was to perform feature selection, which involved identifying the most relevant features that would be used in the analysis. This step is crucial in reducing the dimensionality of the data and eliminating any irrelevant features that could negatively affect the results.

After the dataset was prepared, it was used to evaluate the results using multiple machine learning techniques. The results from these techniques were compared and analyzed to find the best-fitting machine learning algorithm for our dataset.

3.1. Proposed Dataset

For this research, we have proposed a new dataset called HEIoT21. The dataset was generated in a smart home environment; the environment consisted of a collection of real IoT devices and other non-IoT devices, such as laptops and mobiles, all connected to a Wifi router. The used IoT devices were WD MY Cloud running a plex server, Mi Home Security Camera 360°, Raspberry Pi 4 running an Apache server, and Lifx smart lamp, Figure 2 shows the ecosystem of the HEIoT21 dataset.

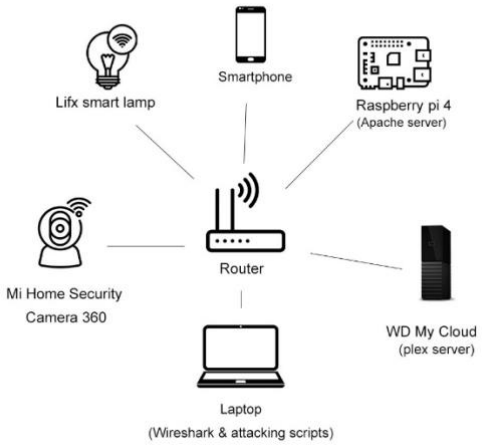

Figure 2. The ecosystem of the HEIoT21

The data was gathered in an interval of 7 days discontinuously. The dataset consists of normal and anomaly data; the normal data was collected by continuously sniffing the network packets of all the wireless network devices using Wireshark and without any attacks. For every 48 hours, the data will be saved as a Pcap file.

For the attack data, we used a laptop running Kali Linux to launch attacks on the IoT devices using the command line, and on the same laptop, we used Wireshark to collect the network packets and then save them as Pcap files as well.

The different types of attacks on the proposed dataset were generated as follows;

TCP SYN Flood Attack: This attack was generated using hping3 network tool by running the corresponding commands using the Kali Linux laptop.

The attacks were generated in two different modes; the first one was to send packets from a generated spoofed IP address to a victim IP address in order to cloak the original source and evade detection, with a packet of 460 bytes and a 64-byte TCP window size, the attack was generated in Flood mode, i.e., the packets will be sent as fast as possible. For the second mode, the packets were sent from a particular source IP Address with the same packet size and window size settings.

We have used the TCP SYN flood attack against two IoT devices; WD MY Cloud running a Plex server, and Raspberry Pi 4, running Apache Server.

UDP Flood Attack: For this attack also hping3 tool was used, but this time in UDP mode instead of TCP. The packets were sent from a spoofed IP address to hide the actual source and evade detection, the packet size was 120 bytes, and a window of 32 was used.

This attack was used against Lifx smart lamp and Mi Home Security Camera 360°.

HTTP-Slowris Attack: This attack was generated using the SlowHTTPTest tool. This tool was used from the Kali Linux command line and can simulate DoS attacks. For the attack generation, we have used the following configurations; the request type was set to GET, the mode was set to slow-header with a different number of connections for each run between 1500 to 3500 connections, the interval between packets was set to 10s, and the connection rate was set to 200 connection per seconds.

We have used this attack against websites running using an apache server on Raspberry Pi 4.

Port Scan: This attack scans all the network ports, looking for a specific port. It was generated using the Nmap tool against the WD My Cloud, Lifx Lamp, and Raspberry Pi 4.

The data generated from the above attacks were saved in separate Pcap files for each attack type, then an application named CICFlowMeter was used to extract network features and save the results as CSV files. CICFlowMeter extracts 82 features, and we added to them another two features for labeling, a -label- field that has two values (normal and attack), a -category- field that categorize the data according to the attack type (Normal, TCP Syn Flood, Apache Killer, Port Scan, UDP Flood and HTTP Slowloris GET). The CSV files were labelled separately and combined into a final CSV file using a Python script. The final CSV file was named HEIoT21, representing our dataset.

The HEIoT21 dataset has 125365 instances after being cleaned, 36346 instances for normal data, and 89019 instances for the different attacks. Table 1 shows the attack and normal data of the proposed dataset.

Table 1. The attack and normal instances in the HEIoT21 dataset

Label Distribution	
Normal	**36346**
Attack	**89019**
Category Distribution	
Normal	**36346**
UDP Flood	**53601**
TCP Syn Flood	**15009**
HTTP Slowloris GET	**9217**
Port Scan	**4136**
Apache Killer	**7056**

Figure 3 and Figure 4 represent the distribution of instances in the HEIoT21.

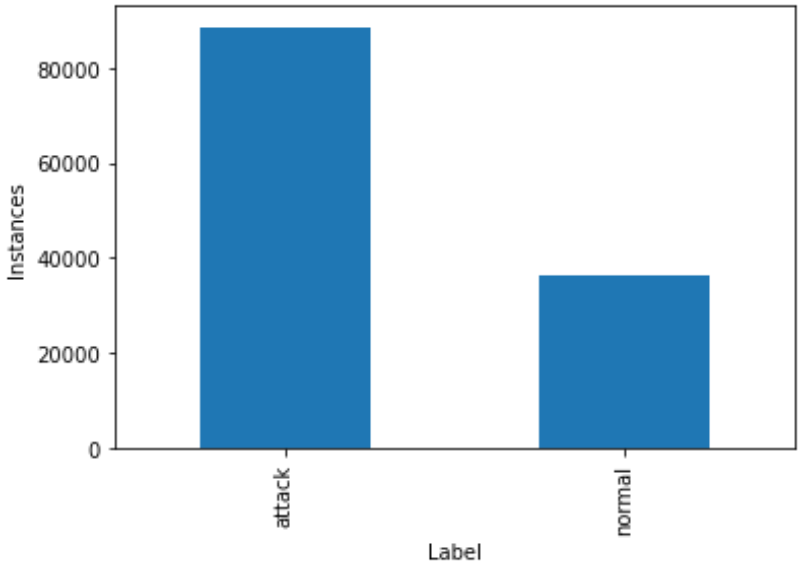

Figure 3. Distribution of instances by label

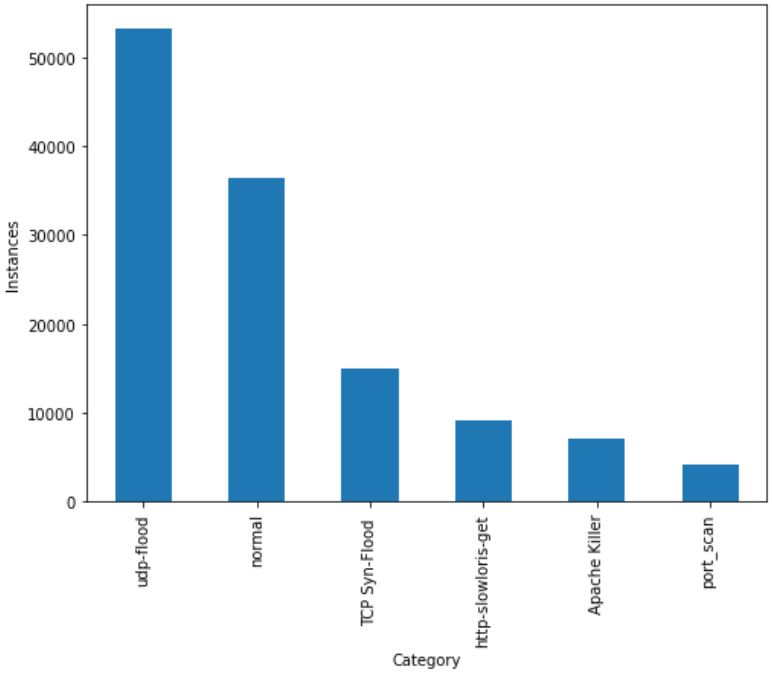

Figure 4. Distribution of instances by category

The dataset passed through different steps of pre-processing before using it for classifications. The steps were as follows

- Removing all NaN values and object type values since they are not useful for classification.
- Using StandardScaler to scale the data and convert the 'label' field into binary 1=normal, 0=attack.
- Converting the 'category' field into numerical as follows 5=udp-flood, 4=port_scan, 3=normal, 2=HTTP-Slowloris-get, 1=TCP Syn-Flood and 0= Apache Killer

- To avoid the overfitting caused by the high number of features, we used three different feature selection methods.
    - **ANOVA f-Value**; was used to select 20 features based on their highest score, and from those features, we removed the highly correlated ones, leaving a new sub-dataset consisting of 14 features instead of 84.
    - **Random Forest**; was used to select the top 20 features based on their highest score value. Then from those features we removed the highly correlated ones, creating a new sub-dataset made up of 17 features instead of 84.
    - **Forward Feature Selection**: used to select the top 20 features based on the best ROC_AUC score. The highly correlated features were then removed leaving a new sub-dataset made up of 20 features.
    - The previous process resulted in 3 different sub-datasets, which were used for modelling.

3.2. Dataset Modelling and Evaluation

Classification is a machine learning technique that assigns specific instances to a pre-defined category [13]. Classification takes a dataset as an input and uses machine learning algorithms to categorize instances to their best-fit label or category [13].

For this research, we have used J48 Decision Tree, Logistic Regression, Gaussian Naïve Bayes, and Neural Networks using Keras as supervised classification algorithms.

For classification, we have split the three sub-datasets derived from the original HEoIT21 after applying the feature selection techniques into training and testing datasets. The model was first trained for both binary and multi-class classification, and then was tested against the test datasets. Then the performance of each classification algorithm was evaluated using the performance measures such as Accuracy, Precision and F-Score.

Moreover, to diagnose the performance of our model, we have plotted the learning curve of the training sample for label classification against the accuracy using our classification algorithms as an estimator once at a time. The learning curve showed that in order to get a high classification accuracy, we need at least a minimum amount of forty thousand (40,000) instances, we plotted the same curve for multi-class classification and it showed that a minimum amount of (20,000) instances is needed to get a high accuracy rate. Figure 5 shows the learning and validation curve for DT of the training set against the predictive accuracy.

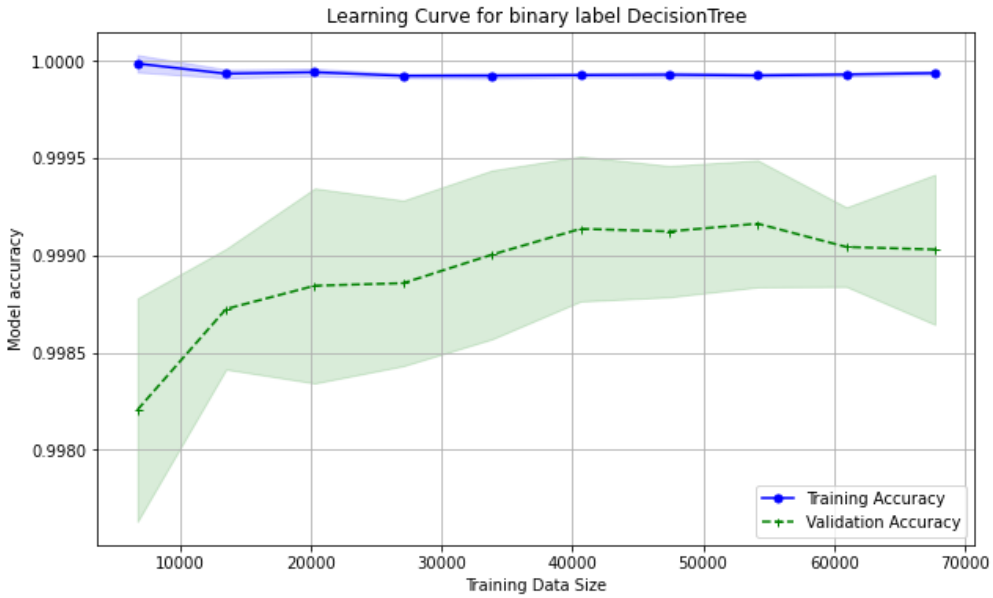

Figure 3. The learning and validation curve for DT of the training set against the predictive accuracy

4. Results and Discussions

We have concluded from the work done in this research that the features of the dataset play a massive role in the performance of the detection model, and the best feature selection technique for our proposed dataset was ANOVA F-Value which has generated a high accuracy rate for all the selected algorithms and in both multi-class and binary classification. Figure 6 shows a comparison of the evaluation accuracy for binary classification.

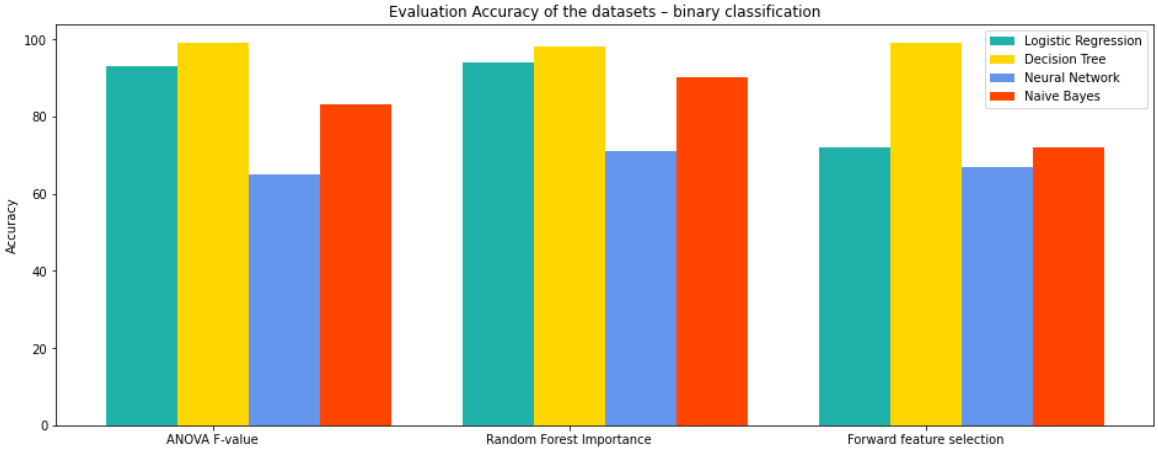

Figure 4. Comparison between the evaluation accuracy - binary classification

Also, from all the used classification algorithms (Decision Tree, Gaussian Naïve Bayes, Logistic Regression, and Neural Network), Decision Tree has performed the best on the three sub-datasets with an accuracy of 99.92% and 99.94% for both binary and multi-class classification, respectivly. Figure 7 shows a comparison between the evaluation accuracy for multi-class classification and confirms that Decision Tree has performed the best.

We have compared the results obtained in this research with other related studies in the same field as IoT network security and intrusion detection; Table 2 shows this comparison. Our results were higher than most other studies, and our proposed dataset might be promising for future work and studies.

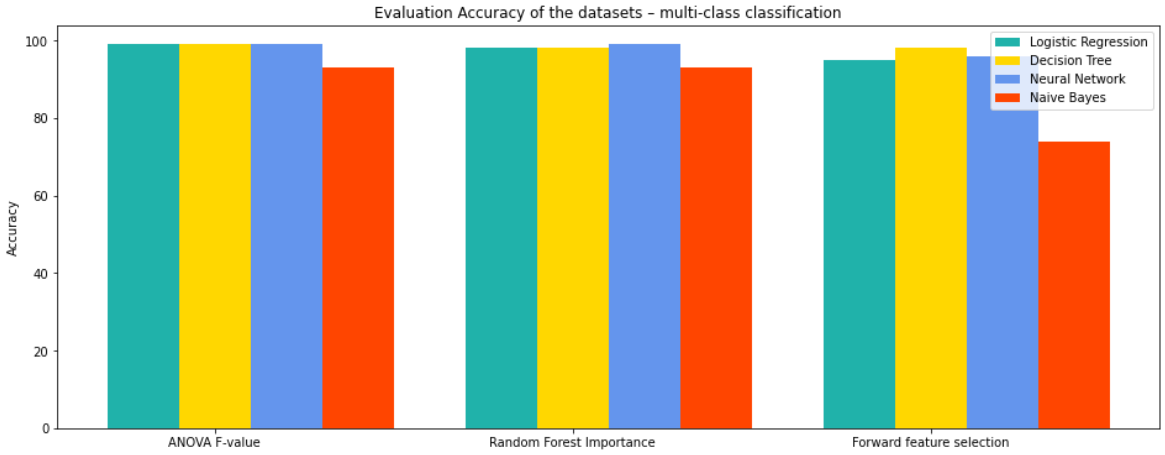

Figure 5. Evaluation accuracy comparison - multi-class

Table 2. Result comparison with other studies

Research	Dataset	Classification type	Model	Accuracy
Farahnakian and Heikkonen [6]	**KDD CUP 99**	Binary	Deep Auto-Encoder	96.53%
M. Moukhafi, K. El Yassini and S. Bri [7]	**KDD 99**	Multi-class	hybrid genetic algorithm and support vector machine	96.38%
Khalvati [8]	**KDD CUP 99**	Multi-class	SVM and Bayesian	91.50%
Ferrag, Mohamed Amine & Shu, Lei & Hamouda, Djallel & Choo, Raymond [9]	**CIC-DDoS2019 dataset**	Multi-class Binary	CNN CNN	95.90% 99.95%
Ferrag, Mohamed Amine & Shu, Lei & Hamouda, Djallel & Choo, Raymond [10]	**TON_IoT dataset**	Multi-class	RNN	98.94%
S. Latif, Z. Zou, Z. Idrees and J. Ahmad [11]	**DS2OS**	Multi-class	lightweight RaNN	99.20%
Imtiaz Ullah, Qusay H. Mahmoud [12]	**BoT-IoT, IoT network intrusion, MQTT-IoT-IDS2020, MQTTset, IoT-23, and IoT-DS2**	Multi-class Binary	feed-forward neural network	99.97% 99.99%
Imtiaz Ullah, Qusay H. Mahmoud [13]	**IoTID20**	Multi-class Binary	DT DT	100% 100%
Our Study	**HEIoT21**	Binary Multi-class	DT DT	99.92% 99.94%

5. Conclusion

In conclusion, this study was successful in achieving its two primary goals in a comprehensive manner. The first goal was to create a new IoT dataset that was composed of data obtained from real devices in different scenarios, rather than using simulated data. This dataset was collected in a real smart home environment, making it highly relevant and useful for researchers in the field as it provides a realistic representation of IoT devices and the attacks they are vulnerable to. This dataset will be helpful in training and testing other intrusion detection models and it will also be useful for researchers in the field of IoT security to better understand the behavior of real-world IoT devices.

The second goal was to identify the most effective model for detecting different types of intrusions within the scope of our dataset. This was accomplished by evaluating multiple models and selecting the one that achieved the highest accuracy rate. The chosen model was able to detect various types of intrusions with a high level of accuracy, reaching 99.9%.

In the future, the dataset will be expanded and updated to include a wider range of attack types, this will make the dataset more comprehensive and will help in detecting new and emerging attacks. Additionally, an alert mechanism will be integrated to create a more robust and efficient attack detection system. Overall, this study has made significant contributions to the field of IoT security by providing a realistic dataset and an effective intrusion detection model, and it will be of great use to researchers and practitioners in the area.

References

[1] Butun I, Österberg P, Song H. Security of the Internet of Things: vulnerabilities, attacks and counter measures. IEEE Commun Surv Tutorials 2019; 616-644.

[2] Alotaibi B, Alotaibi M. A stacked deep learning approach for IoT cyber attack detection. J Sens 2020.

[3] Abu Kwaider H. HEIoT2021. [Online]. Available: https://drive.google.com/file/d/1WAHorikhN9fw9T1YpOkH6Dwvnbwdji HC/view?usp=sharing. 2021.

[4] Xu T, Potkonjak M, Wendt J. Security of IoT systems: design challenges and opportunities. ACM International Conference on Computer-Aided Design 2014; IEEE. pp. 417-423.

[5] Bull P, Austin R, Popov E, Sharma M, Watson R. Flow based security for IoT devices using an SDN gateway. IEEE 4th International Conference on Future Internet of Things and Cloud 2016; IEEE. pp. 157-163.

[6] Farahnakian F, Heikkonen JA. Deep auto-encoder based approach for intrusion detection system. 20th International Conference on Advanced Communication Technology 2018; pp. 178-183.

[7] Moukhafi M, El Yassini K, Bri S. A novel hybrid GA and SVM with PSO feature selection for intrusion detection system. Int J Adv Sci Eng Technol 2018; 4(5): 129-134.

[8] Khalvati L, Keshtgary M, Rikhtegar N. Intrusion detection based on a novel hybrid learning approach. J AI Data Mining 2018; 6(1): 157-162.

[9] Ferrag M, Shu L, Hamouda D, Choo R. Deep learning-based intrusion detection for distributed denial of service attack in agriculture 4.0. Electronics 2021; 10(11): 1257.

[10] Latif S, Zou Z, Idrees Z, Ahmad J. A novel attack detection scheme for the industrial Internet of Things using a lightweight random neural network. IEEE Access 2020; (8): 89337- 89350.

[11] Ullah I, Mahmoud Q. An anomaly detection model for IoT networks based on flow and flag features using a feed-forward neural network. IEEE 19th Annual Consumer Communications & Networking Conference 2022; pp. 363-368.

[12] Ullah I, Mahmoud Q. A scheme for generating a dataset for anomalous activity detection in IoT networks. Advances in Artificial Intelligence: 33rd Canadian Conference on Artificial Intelligence, Canadian AI 2020, Ottawa, ON, Canada, 13–15 May 2020, Proceedings: pp. 508–520.

[13] Lopez Alma D, Mohan Asha P, Nair S. Network traffic behavioral analytics for detection of DDoS attacks. SMU Data Science Review 2019; 2(1): Article 14.