Securing IoT Devices in e-Health using Machine Learning Techniques

Haifa Khaled Alanazi[1], A. A. Abd El-Aziz[2], Hedi Hamdi[3]
Department of Computer Science, Jouf University, Al Jouf, Saudi Arabia[1]
Department of Information Systems, College of Computer and Information Science, Jouf University, Aljouf, KSA. Department of Information Systems & Technology, Faculty of Graduate Studies for Statistical Research Cairo University, Cairo, Egypt[2]
Department of Computer Science, Jouf University, Sakaka, KSA. University of Manouba, Tunisia[3]

***Abstract*—The Internet of Things (IoT) has gained significance over the past several years and is currently one of the most important technologies. The capacity to link everyday objects, such as home appliances, medical equipment, autos, and baby monitors, to the internet via embedded devices with a minimum of human interaction has made continuous communication between people, processes, and things feasible. IoT devices have established themselves in many sectors, of which electronic health is considered the most important. The IoT environment deals with many private and sensitive health data that must be kept safe from tampering or theft. If safety precautions are not implemented, these dangers and assaults against IoT devices in the health sector might completely destroy this industry. Detecting security threats to an IoT environment requires sophisticated technology; these attacks can be identified using machine learning (ML) techniques, which can also predict snooping behavior based on unidentified patterns. In this paper, it is proposed to apply five strategies to detect attacks in network traffic based on the NF-ToN-IoT dataset. The classifiers used are Naive Bayes (NB), Random Forest (RF), Decision Tree (DT), Artificial Neural Network (ANN), and Support Vector Machine (SVM) models. These algorithms have been used instead of a centralized method to deliver compact security systems for IoT devices. The dataset was pre-processed to eliminate extraneous or missing data, and then a feature engineering approach was used to extract key features. The results obtained by applying each of the listed classifiers to a maximum classification accuracy of 98% achieved by the RF model showed our comparison to other work.**

***Keywords*—IoT; ML; DL; attack classification; e-health**

I. INTRODUCTION

A network of physical items, or "things," that have sensors, software, and other technologies built into them that can connect to and exchange data with other systems and devices through the Internet is referred to as the "Internet of Things" (IoT) [1]. These devices range from basic household goods to cutting-edge industrial equipment. More than 7 billion IoT devices are currently online. IoT Analytics experts predict that by 2023, there will be 14.4 billion linked IoT devices, an increase of 18%, and that by 2025, there may be 27 billion connected IoT devices [2].

The Internet of Things has applications in many different industries. It has proven important in a number of different industries, but the healthcare industry has seen it hard. The medical industry has benefited from modern technology and digital transformation. As mobile medical devices, mobile health applications, and services have helped improve healthcare services, they are expected to rely more and more on IoT technology in the coming years [3].

The use of the IoT in healthcare is constantly evolving. This fundamental change positively affected patient care because it allowed the clinician to provide a more accurate diagnosis and thus achieve better treatment outcomes [4]. The quality and efficiency of medical services have greatly improved due to the integration of IoT elements into medical devices. Today, IoT technology is widespread in hospitals. It has gotten to the point that many doctors, nurses, and healthcare professionals have abandoned paper in favor of tablets and other Wi-Fi-connected devices [3]. With all these changes and developments, the digital transformation of healthcare has created several difficulties affecting patients, healthcare workers, technology innovators, policymakers, and others. Data interoperability is an ongoing difficulty due to the massive amounts of data generated from various systems that store and encode data differently [5]. These concerns, in turn, raise questions about security and privacy. For example, what if medical devices are hacked? Or what if this sensitive patient data is accessed, leaked, or tampered with?

Data and information are among the most important considerations that must be considered when developing and building IOT to avoid any potential risks related to security. The primary concern of network devices is data protection. Security is paramount in the field of IoT because unauthorized access to or interference with IoT equipment, especially when used for major IoT applications, can endanger human life [6]. The IoT environment deals with a huge amount of private and sensitive health data that must be kept safe from tampering or theft. If safety precautions are not implemented, these dangers and assaults against IoT devices in the health sector might completely destroy this industry. These attacks are often carried out to make money, either by selling the stolen data or by holding the victim's data at ransom to release their data.

The main objective of this research is to build and design a suitable model based on machine learning techniques to increase the accuracy of detecting malicious and benign attacks in an IoT environment using the standard NF-ToN-IoT dataset consisting of network traffic attributes based on different protocols to analyze traffic tracking and behavior of networks and identify malicious attacks. Then, using a

preprocessing and feature selection step, the most important features were extracted, and the dimensionality of the dataset was reduced. Supervised classification algorithms were then applied, which included RF, SVM, DT, ANN, and NB classification algorithms that allow the identification of malicious and benign traffic, which helped in developing an effective intrusion detection system (IDS) that can identify a variety of attacks. The proposed model was then evaluated based on the most appropriate metrics. Finally, compare the proposed model with the latest developments in this field. The contributions of our technology are listed below as detailed previously:

- Proposing an appropriate Machine learning (ML) model for Cyber-attack intrusion detection, by using the NF-ToN-IoT dataset and applying classification techniques that include RF, SVM, DT, ANN, and NB algorithms.
- Evaluation of the proposed model based on the most suitable metrics.
- Comparing the proposed model with state-of-the-art in this field.

The remainder of this research is organized as shown below. The literature review on intrusion detection through the application and use of machine learning and deep learning techniques based on different datasets is summarized in Section II. Section III contains a comprehensive explanation of the methodology proposed for this research. The model implementation and evaluation of the machine learning algorithms implemented in this work and the results of each of them are presented in Section IV, while the obtained result and discussion compared to previous studies are presented in Section V. Finally, the conclusion and future work is presented in Sections VI and VII, respectively.

II. Literature Review

This section will provide an overview of the available studies and research related to the issue of securing the Internet of Things device in the e-Health system.

Zhu et al. [7] recommend using a nonlinear kernel support vector machine (SVM) to build the e-Diag framework, an efficient and privacy-preserving online medical prediagnosis tool, in an IoT-based e-Health environment. When utilizing e-Diag for online prediagnosis services, sensitive personal health data may be processed without privacy disclosure. On the basis of an improved expression for the nonlinear SVM, a powerful and privacy-preserving classification approach is created, using lightweight multiparty random masking and polynomial aggregation techniques. The SVM classifier and data are hence secure. The approach was tested using the PID database of the UCI machine learning repository.

The focus of the study [8] was on how machine learning affected flow-based anomaly detection in SDN. The authors offered two distinct approaches to intrusion detection systems based on deep neural networks (DNN) and machine learning. The NSL-KDD dataset was employed in the first technique, and feature selection based on the RF classifier led to an accuracy rate of 82%. However, when paired with DNN-based IDS, the second technique had an accuracy of 88%.

The authors of this study [9] compare the performance of ANN and Random Forest models using a dataset created by combining the benign and malicious datasets for detecting the Mirai virus in relation to seven IoT devices. The NBaloT dataset, which contains information on the features infected with the Mirai virus, is used to propose a novel technique that relies primarily on machine learning technology. In order to avoid over-fitting, the data partitioning approach known as mutual validity was applied, and ANN was used to conduct the experiment. The accuracy attained is 92.8%. The Opcode data collection, which includes 69,860 harmful programs and 70,140 examples of common malware, was employed in this study.

The study [10] is built on a deep learning-based technique for Internet of Things intrusion detection. The researchers discovered that security vulnerabilities rise as the number of Internet of Things devices rises. As a result, a Bot-IoT data set was utilized to compare deep learning techniques like CNN with machine learning techniques like RF and MLP. Through their expertise, CNN attained the maximum accuracy of 91% and the lowest accuracy of 88%.

A novel deep learning-based intrusion detection system for IoT networks and devices is presented by the authors in another paper [11]. A four-layer fully connected (FC) deep network architecture is used by this system to identify malicious traffic that may be used to target linked IoT devices. In order to simplify deployment, the suggested system was created as a communication protocol-independent solution. The ground-breaking IDS powered by deep learning maintain an average detection rate of 93.21%. It made use of the DID dataset.

With the use of outside resources, the authors of this study [12] suggest a comprehensive multi-level, privacy-preserving SVM training and illness diagnosis system. For encrypted data, certain efficient fundamental operational algorithms have been developed. Next, a model training procedure that is effective and protects privacy was created utilizing fundamental operational methods. Then, using the BFV coding system and cryptography method, they created a successful Internet-assisted illness diagnostic scheme. The user only needs to execute a limited number of encryption and decryption operations under their suggested method, which uses cloud servers to accomplish the majority of the illness diagnoses. The efficiency of Internet-assisted illness diagnosis has increased by 85.4% with a total computing cost of 0.175 seconds.

In [13] their study Detecting Cyber Intrusion Using Machine Learning Classification Techniques, the authors demonstrate how artificial intelligence, in particular machine learning techniques, may be utilized to develop a workable data-driven intrusion detection system. Numerous well-known machine learning classification algorithms, such as the Decision Tree, Random Decision Forest, Random Tree, Decision Table, and Artificial Neural Network, have been used to detect intrusions as a result of providing intelligent services in the field of cybersecurity. They conducted studies

to achieve an accuracy of 94% in RF using KDD'99 cup datasets.

The authors of [14] proposed an algorithm to predict patients' current health status in addition to continuing professional monitoring. Additional parameters and methods, such as K-nearest neighbor, logistic regression, support vector machines, random forests, and Adaboost classifiers, are considered using the UCI heart disease dataset. They were successful in providing a tool that would aid patients, medical professionals, and the healthcare system. This way of decision-making is 93% accurate.

IoMT systems are described in [20] as having to manage a sizable amount of data that might be utilized for illness diagnosis, prediction, and monitoring. Medical data about patients should be transferred to cloud storage and external computer devices, respectively, as certain IoMT devices have limited storage and processing capabilities. Security and privacy risks may arise as a result of this approach. A swarm neural network-based approach for identifying intruders in IoMT has been offered as a solution to these problems. The suggested model explores the possibility of properly and effectively evaluating healthcare data as well as identifying intruders during data transfer. An NF-ToN-IoT dataset was used to assess the system's performance, and the findings show that the suggested model achieves 89.0% accuracy.

Based on the above, after examining all the previous studies that were collected and explaining their work and results in detail, it becomes clear that all of them achieved different results through the use of different data sets and algorithms, but the highest accuracy result among them was 94%, while the methodology proposed in our work achieved accuracy higher than all previous studies, reaching 98%.

III. Methodology

In this section, the choice of the dataset, as well as the description of its specifics, is discussed. In addition, the dataset pre-processing techniques as well as the feature selection are deliberated. Finally, the model implementation is described.

A. Dataset Selection and Description

NF-ToN-IoT was chosen as the data set for this research since it contains a variety of heterogeneous data sources collected from Telemetry datasets of IoT sensors. It contains ten features, and nine types of attacks, namely, (XSS, DDoS, DoS, password cracking attacks, reconnaissance, or verification, MITM, ransomware, backdoors, and injection attacks) [15] [16]. The assaults detected in the dataset used in this study may be classified and defined using the terms below:

1) XSS attack: Using XSS technology, malicious code can be injected into trusted Internet applications, such as the web pages of Internet of Things services. In XSS assaults, the attacker transmits malicious code to several end users via an online application, typically a browser-side script.

2) DDOS attack: Most of the time, a botnet—a collection of compromised machines—conducts this kind of attack. The victim's IoT resources are flooded and depleted by this attack's many connections.

3) DoS attack: A DoS attack is any attempt to compromise the resources and services of an IoT network. Making IoT services inaccessible is the goal of such an attack.

4) Password cracking attack: This hacking approach is used to guess potential password combinations until the precise password is found. Examples include dictionary attacks and brute force assaults. Passwords for IoT services, operating systems, and web apps placed on the test bench can be cracked using this technique.

5) Scanning attack: This attack seeks to gather details about test bed network victims' computers, such as active IP addresses and open ports. This assault is the initial phase of a penetration test, often known as an investigation or a cyber-death chain model.

6) MITM attack: This kind of attack may happen when hackers place themselves in the middle of users and programs to watch over them or appear to be one of them, creating the false impression that information is flowing normally. Data about networks, online apps, and IoT services might be taken in these hacking scenarios.

7) Ransomware attack: It is an advanced form of malware assault that encrypts systems or services and renders them inaccessible to regular users until they pay a ransom. IoT devices and applications might be the target of ransomware attacks since they carry out essential functions.

8) Backdoors attack: An attacker can use backdoor malware to obtain unauthorized remote access to infected IoT systems. By controlling infected IoT devices, this threat may launch botnet-based DDoS attacks.

9) Injection attack: Attackers use injection techniques to introduce real or fake input data from clients into their targets' systems, such as SQL injection to attack ASP and PHP programs.

Compared to other datasets, the NF-ToN-IoT dataset is appropriate for IoT since it captures the heterogeneous character of contemporary IoT networks. Regarding the statistics of the dataset, the NF-ToN-IoT dataset comprises a total of 1,157,994 rows. The number of rows varies for each attack type, with injection attacks having the highest number of rows (460,812) and ransomware attacks having the lowest number of rows (142). Here is a breakdown of the number of rows for each attack type and benign type in Table I:

TABLE I. Statistics of Dataset

Label	*Count*
Benign	198450
Backdoor	17243
Ddos	197680
Dos	17056
Injection	460812
Mitm	1288
Password	144792
Ransomware	142
Scanning	20618
Xss	99913

The NF-ToN-IoT includes telemetry data from linked devices, Linux operating system data, Windows operating system logs, and IoT network traffic, among other data sources acquired from the entire IoT system. A medium-scale IoT network provides diverse data. The UNSW Canberra IoT Labs and the Cyber Range designed NF-ToN-IoT. Furthermore, the NF-ToN-IoT is represented in CSV format with a labeled column indicating attack or normal and a sub-category attack type. A CSV is a comma-separated value file, which allows data to be saved in a tabular format. CSV files can be used with most any spreadsheet program, such as Microsoft Excel.

B. Exploratory Data Analysis

Exploratory Data Analysis (EDA) is one of the essential procedures that can be done on a dataset for several reasons. EDA aims to familiarize the user with the data and provide an understanding of how the data is distributed. Additionally, EDA allows the identification of patterns and relationships between parameters present in the data. EDA is also important because it provides insight into the selection of data and aids in the perfect execution of machine learning tasks [17]. This research used different visualizations as an EDA procedure to understand the NF-ToN-IoT dataset.

The bar graph in Fig. 1 illustrates the different categories of attacks that are present in the selected NF-ToN-IoT dataset, where it contains benign attacks, dos, injection, DDoS, scanning, password, Mitm, XSS, backdoor, and ransomware attacks. The bar graph representation of the dataset shows that the dataset is imbalanced, where different counts of the categories can be seen.

The attack with the most count in the NF-ToN-IoT dataset is the injection, where there are more than 400,000 attacks belonging to it. The second most common attacks are DDoS and benign attacks, where there are approximately 200,000 of each one of them. The other attacks vary in number, whereas the Mitm and the ransomware attacks are absent in this dataset (zero count).

Furthermore, several features within the dataset can be visualized through histograms to show their form of distribution. For instance, Fig. 2 above represents the distribution of TCP_FLAGS, FLOW_DURATION, IN_PKTS, OUT_PKTS, PROTOCOL, OUT_BYTES, L4_DST_PORT, and L4_SRC_PORT. The representations in Fig. 2 show that all of the features have skewed distributions, whereas only L4_SRC_PORT and TCP_FLAGS have a relatively uniform distribution. The skewness of the features means that they are not well-rounded around the mean value of the feature, which could affect the output results. For this reason, the features with skewness might be subjected to transformation in order to be suitable for use in ML techniques.

C. Model Architecture

The models were trained using the chosen features representing attack behaviors in this phase. The proposed models were then tested by comparing test data to training data to determine the accuracy of each of the models. The model was only considered ready if the accuracy test was satisfactory; otherwise, the model was retrained until an acceptable accuracy was reached .For performance comparison, algorithms like ANN, RF, SVM, DT, and NB classification techniques were implemented.

These algorithms were chosen because researchers widely use them to detect unusual traffic. Furthermore, they are simple and light, they do not require many operations, they are highly accurate, and they have fewer input features. The architecture of our proposed framework is described in Fig. 3.

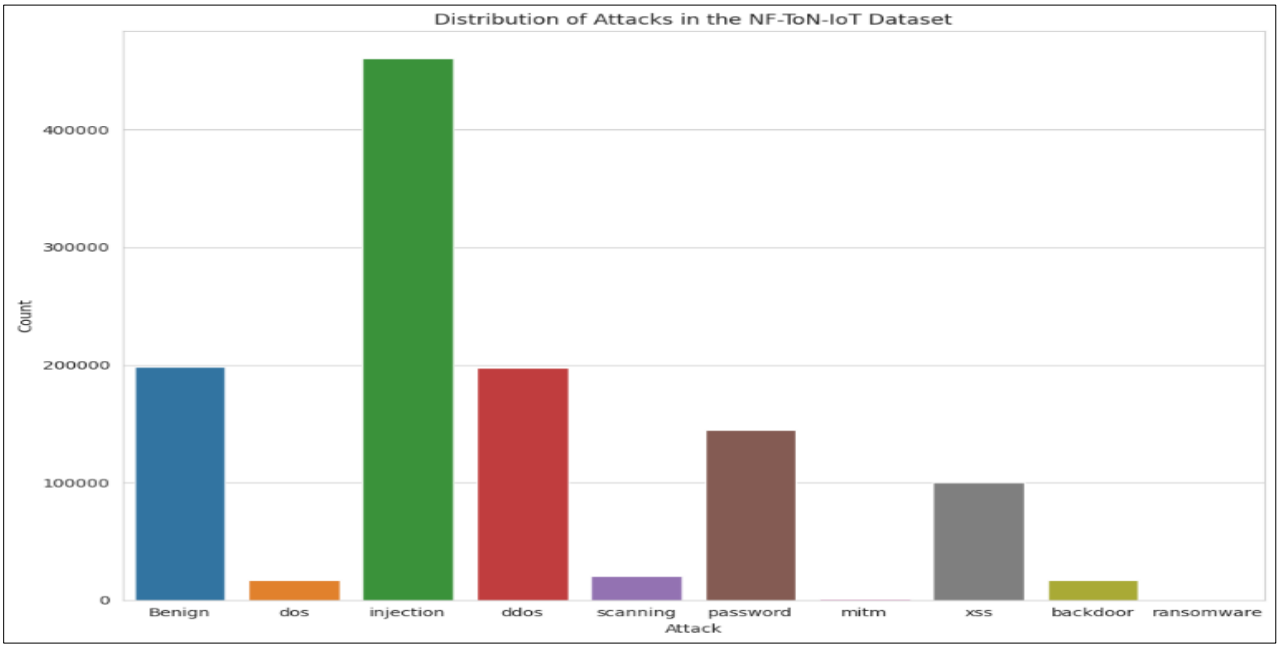

Fig. 1. Distribution of attacks in the NF-ToN-IoT dataset.

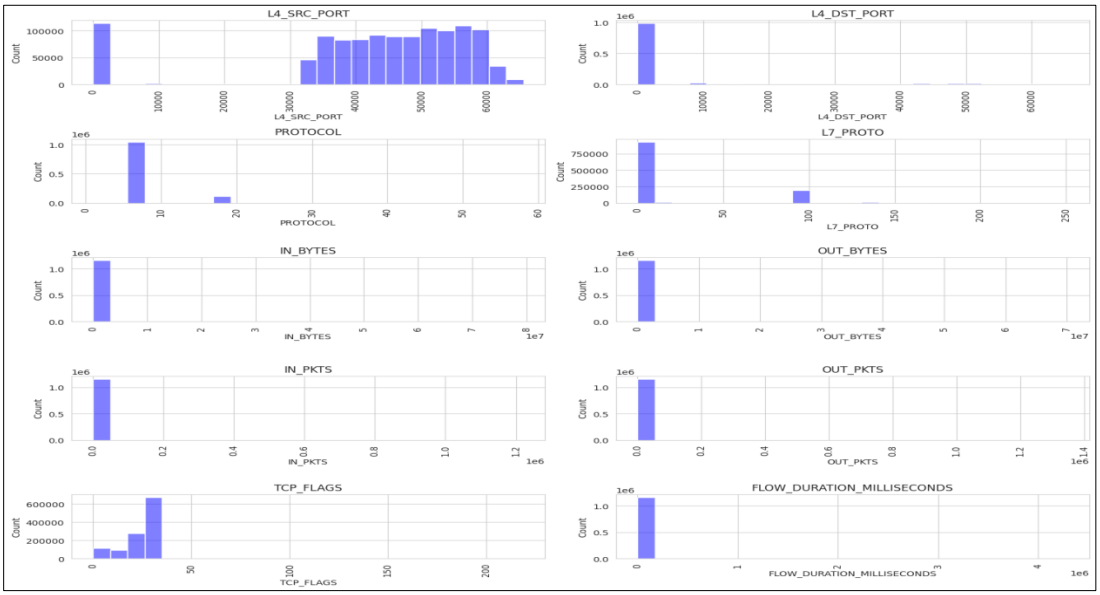

Fig. 2. Distribution of several features in the NF-ToN-IoT dataset.

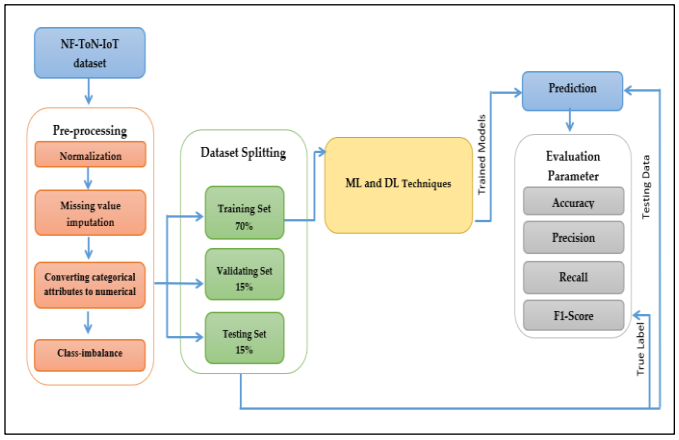

Fig. 3. Architecture of the proposed framework.

As shown in Fig. 3, our framework starts with the acquisition of the NF-ToN-IoT dataset. Then, an essential step is performed, which is the data pre-processing including normalization, imputation of missing values, conversion of categorical attributes to numerical ones, and fixing class imbalance. After the completion of pre-processing, the dataset is subjected to splitting into three different sets: training set (70%), validation set (15%), and testing set (15%). The training set is used for training the ML models (namely, NB, RF, DT, ANN, and SVM). After the training step, the models performed predictions on the testing set in order to find out if the model could accurately generate a result. Different parameters were used for evaluation, such as accuracy, precision, recall, and F1 score.

D. Dataset Pre-Processing

Converting unprocessed data into a format that can be read, accessed, and analyzed is known as data pre-processing. Before using ML and DL algorithms, pre-processing is crucial for ensuring or improving any system's overall performance or accuracy. Data is cleaned during the pre-processing phase to serve a variety of purposes. Some ML algorithms need data in a specific format to ensure the data collection is suitable for many algorithms. The NF-ToN-IoT dataset used in this research presented several challenges, such as missing values, categorical attributes, and class imbalance. To address these issues, the following pre-processing steps were performed:

1) Missing value imputation: The NF-ToN-IoT dataset was checked for missing values, but after inspection, it was found that no missing values were found. Therefore, the data set was found to be of high quality and value.

2) Converting categorical attributes to numerical: As shown in Table II, the NF-ToN-IoT dataset contains different category features, and the category's attributes must be given numerical values. The conversion process was carried out through LabelEncoder.

TABLE II. CATEGORICAL ATTRIBUTES CONVERTED TO NUMERICAL

Label	*Encoded Labe*	*Count*
Benign	0	198450
Backdoor	1	17243
Ddos	2	197680
Dos	3	17056
Injection	4	460812
Mitm	5	1288
Password	6	144792
Ransomware	7	142
Scanning	8	20618
Xss	9	99913

3) Class imbalance: Distributions with class imbalances afflict the NF-ToN-IoT dataset. The problem of class imbalance often arises when some classes are far more prevalent than others. Standard classifiers frequently disregard the little classes in these situations because they are too overwhelmed with the large classes.

To address this issue, the SMOTENN (Synthetic Minority Over-sampling Technique and Edited Nearest Neighbors) method was applied to balance the classes in the dataset. The SMOTENN method oversamples the minority class using synthetic data generation (SMOTE) and removes noisy samples using nearest neighbors (ENN) to balance the dataset. Table III shows the number of rows for each attack type before and after applying the SMOTENN method:

TABLE III. DISTRIBUTION OF CLASSES BEFORE AND AFTER SMOTENN

Label	*Before*	*After*
Benign	198450	434938
Backdoor	17243	456873
Ddos	197680	200376
Dos	17056	268998
Injection	460812	126022
Mitm	1288	405380
Password	144792	62216
Ransomware	142	457791
Scanning	20618	220336
Xss	99913	114330

E. Feature Selection

Giving each potential feature a score before choosing the top features is the feature selection procedure. For intrusion detection, many factors must be examined; certain features will be useful, while others will be useless. Each prospective feature is given a score as part of the selection process, which selects the best (k) attributes [18].

A function of both is obtained by independently calculating the frequency of a feature in training for each positive and negative class occurrence. Removing non-essential features improves performance by reducing overfitting, speeding up the calculation, and enhancing accuracy. We'll utilize the filter method Chi2 for the feature selection technique. A statistical method called the Chi2 technique filters out features that aren't as dependent on the class labels as others, and it calculates a score based on feature dependency [19]. The selected features and their scores obtained from the Chi2 technique are presented in Table IV. The scores are calculated based on the frequency of each feature in the training data for both positive and negative class occurrences. The top (k) attributes with the highest scores are chosen for the final feature set.

The selected features contribute significantly to the intrusion detection task by improving the model's performance. Therefore, the seven features shown in Table IV were chosen and were considered the best in terms of influencing the classification process, while if the number of features were increased, they would not have an impact on the classification process. Removing non-essential features reduces overfitting, speeds up computation, and enhances model accuracy.

TABLE IV. SELECTED FEATURES AND THEIR SCORES

Feature	*Score*	*Selected*
L4_SRC_PORT	124913.19	Selected
L4_DST_PORT	1021455.86	Selected
PROTOCOL	75773.79	Selected
L7_PROTO	163804.13	Selected
IN_BYTES	104.95	Selected
OUT_BYTES	86.81	Not selected
IN_PKTS	105.52	Selected
OUT_PKTS	28.62	Not selected
TCP_FLAGS	46235.03	Selected

IV. MODEL IMPLEMENTATION AND EVALUATION

In this section, the obtained results of the proposed models are discussed, starting with exploratory data analysis, followed by an evaluation of each of the proposed models. In this study, the proposed models to be evaluated are Random Forest RF, Support Vector Machine SVM, Decision Tree DT, Artificial Neural Network ANN, and Naïve Bayes NB classifier.

A. Evaluation Metrics

A variety of methodologies for assessing the effectiveness of the ML techniques employed are chosen and specified in order to offer a thorough and accurate description of the findings achieved. In this paper, the used models were trained on an NF-TON-IoT dataset, and then a collection of data isolated from these models was utilized to assess the trained models' accuracy by correctly separating all the data into its various labels. Accuracy, Precision, F1-Score, and Recall are the measures used to evaluate the algorithms' efficacy. Each equation can be defined separately as follows:

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{TN} + \text{FP} + \text{FN}}$$

$$\text{Precision} = \frac{\text{TP}}{\text{TP} + \text{FP}}$$

$$\text{Recall} = \frac{\text{TP}}{\text{TP} + \text{FN}}$$

$$\text{F1 Score} = \frac{2\times(\text{Precision} \times \text{Recall})}{\text{Precision} + \text{Recall}}$$

1) Accuracy: if the classifier can correctly classify the data points, then it is said to have a high accuracy. Accuracy is

represented by the number of correctly predicted instances divided by the total number of predictions.

2) Precision: Precision takes into consideration the positive outcomes by the model in comparison to all of the positive outcomes whether they were correctly predicted or not. For this reason, the equation of precision is the ratio of correctly predicted positive outcomes (TP) over all of the positive outcomes (TP and FP).

3) Recall: Recall is also known as sensitivity, which represents the fraction of the truly identified positive predictions over the total number of positive instances (represented by TP and FN) because FN should have been predicted as positive results.

4) F1 Score: The F1 score combines both precision and recall into a single metric that provides a balanced evaluation of the model's performance. It is a useful metric when there is an uneven class distribution such as in the NF-ToN-IoT dataset.

In all of these equations:

TP stands for True Positive which represents the number of correctly predicted positive instances.

TN stands for True Negative which represents the number of correctly predicted negative instances.

FP stands for False Positive which represents the number of falsely predicted positive instances.

FN stands for False Negative which represents the number of falsely predicted negative instances.

B. *Models' Evaluation*

The evaluation of the different algorithms used is presented separately in this section, which includes RF, SVM, DT, ANN, and NB classifiers. Based on their outcomes on the test dataset, the suggested algorithms' performance is assessed. The performance of models may be assessed using a number of measures, including accuracy, precision, recall, and F1 score. This is how it appears:

- Naïve Bayes:

A supervised machine learning method called the Naive Bayes NB classifier is utilized for classification tasks like text categorization. It also belongs to the family of generative learning algorithms, which implies that it attempts to simulate how an input's distribution varies depending on the class or category.

Upon testing, the Naïve Bayes classifier was able to achieve 72.75% accuracy, which is equivalent to 0.7275. This value indicates that 72.75% of the instances were correctly predicted by the NB classifier. The NB classifier also achieved 0.7567 precision values, which means that out of all of the positively identified instances, 75.67% of them were correctly predicted by the model. A 0.7275 value for recall indicates that the NB model identified 72.75% of the actual positive instances as true positive. Finally, the F1 score achieved by NB was 0.7051 which is a low value, and it means that the overall performance of the model was around 70% well. These numbers are illustrated in Table V. In addition, a Confusion Matrix Heatmap was generated for the Naive Bayes Classifier in Fig. 4:

TABLE V. NAIVE BAYES CLASSIFIER PERFORMANCE METRICS

Metric	Value
Accuracy	0.7275
Precision	0.7567
Recall	0.7275
F1 Score	0.7051

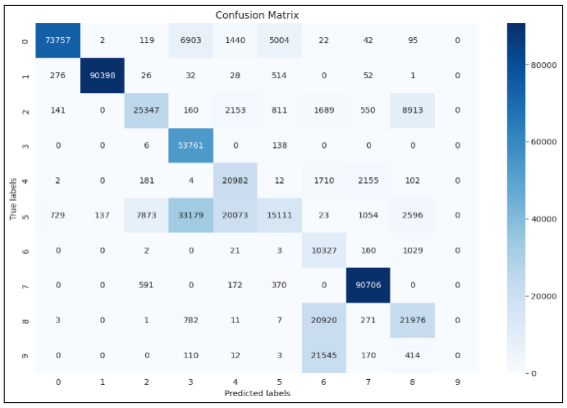

Fig. 4. Confusion matrix heatmap for the naïve bayes classifier.

- Random Forest:

Classifier with Random Forests This classifier is utilized because of its improved accuracy and because it bases its final prediction on predictions from several decision trees rather than just one. Even if the settings are left alone, this supervised machine-learning method produces great results. In order to establish a final categorization of the attack and normal data, tree prediction was also applied.

The random forest model achieved 98.41% accuracy, a 0.9840 precision value, a 0.9841 recall value, and a 0.9840 F1 score, as shown in Table VI. The values shown in the table indicate that the RF classifier achieves a high accuracy rate, where it correctly classified 98.4% of all of the instances in the data. Similarly, it correctly identified the true positives in 98.4% of the total positive instances and the actual positive instances (precision and recall, respectively). Furthermore, the overall performance of the RF model is represented by the high F1 score, which is 0.9840. Fig. 5 shows the Confusion Matrix Heatmap for the Random Forest classifier.

TABLE VI. RANDOM FOREST CLASSIFIER PERFORMANCE METRICS

Metric	Value
Accuracy	0.9841
Precision	0.9840
Recall	0.9841
F1 Score	0.9840

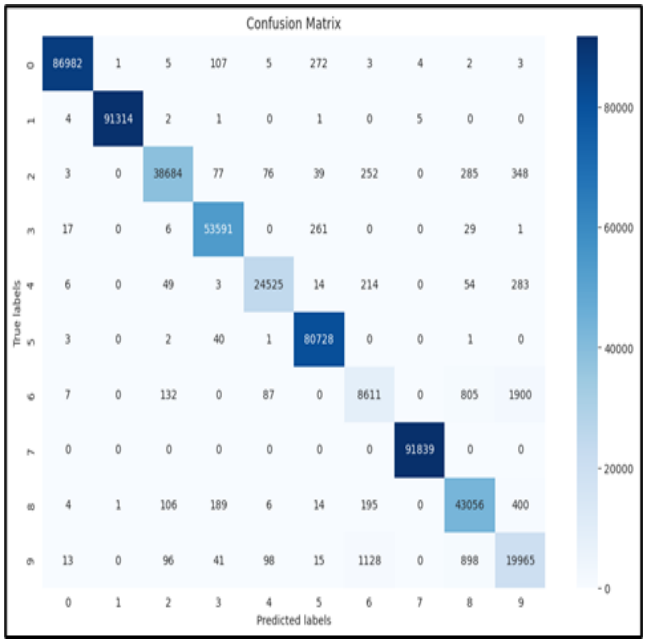

Fig. 5. Confusion matrix heatmap for the random forest classifier.

- Decision Tree:

DT is a well-known construction method that interpolates leaves and branches to resemble a decision tree, where the inner node stands in for the classification rule and the leaves for the class label. The branch also indicates the outcomes. Using the information gained the best branch and root node properties are chosen during the training phase. A decision node is then constructed using the most information gained. As a result, a new sub tree is established beneath the decision node. As the final value will be determined and utilized as the output value, this method will only end if all items in the chosen subgroups have the same value. If there is just one node in the subgroup and no other options, the cycle may also come to an end.

The evaluation metrics for the DT classifier are shown in Table VII and the confusion matrix heat map is in Fig. 6. The Decision Tree classifier accomplished an accuracy of 97.08%, suggesting that the model accurately classified most of the data instances. With a precision score of 97.06%, it showed a high level of correctness when predicting instances as attacks. The recall score of 97.08% indicates the classifier's ability to identify actual attacks accurately from all the positive instances as well. The F1 Score of 97.07% was high, showing a good performance of the DT model.

TABLE VII. DECISION TREE CLASSIFIER PERFORMANCE METRICS

Metric	Value
Accuracy	0.9708
Precision	0.9706
Recall	0.9708
F1 Score	0.9707

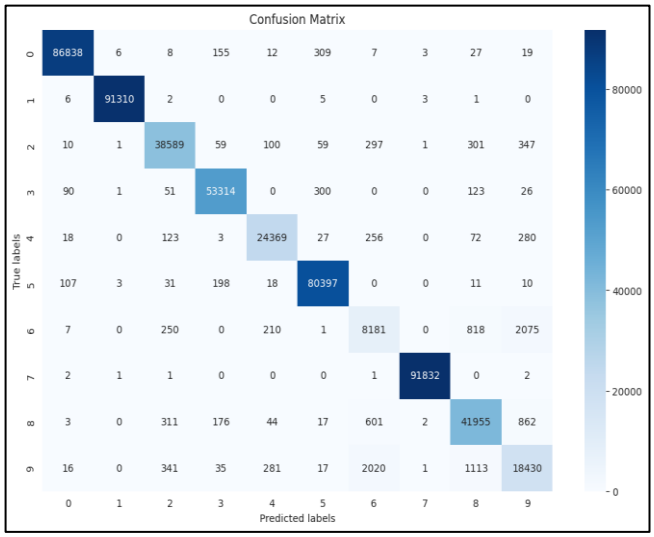

Fig. 6. Confusion matrix heatmap for the decision tree classifier.

- Artificial Neural Network:

An ANN is a collection of linked input-output networks with a weight assigned to each network. As an affiliation, one input layer and one or more intermediary layers make up this structure and only one output layer. The Artificial Neural Network reached an accuracy of 93.20%, demonstrating its ability to classify data instances with a high level of correctness. With a precision score of 93.16%, the classifier presented a strong accuracy when predicting instances as attacks. The recall score which is also the sensitivity value is 93.20%, meaning that the classifier is very effective in identifying actual true attacks in the dataset. The F1 Score of 93.09% shows a good overall performance of the model. The evaluation metrics for the ANN classifier are shown in Table VIII and the confusion matrix heatmap is in Fig. 7.

- Support Vector Machine:

A well-known classification method that can handle both linear and non-linear datasets is Support Vector Machine SVM. It is founded on the idea of separation between hyperplanes, with SVM's main objective being to find the optimal hyperplane that widens the gap between groups. In general, several kernel functions, ranging from linear to nonlinear kernels, may be utilized to describe the hypersurface. It is an approach to supervised machine learning that may be applied to classification or regression issues. It transforms your data using a method known as the kernel trick and then determines the best boundaries between potential outputs based on these alterations.

TABLE VIII. ARTIFICIAL NEURAL NETWORK PERFORMANCE METRICS

Metric	Value
Accuracy	0.9320
Precision	0.9316
Recall	0.9320
F1 Score	0.9309

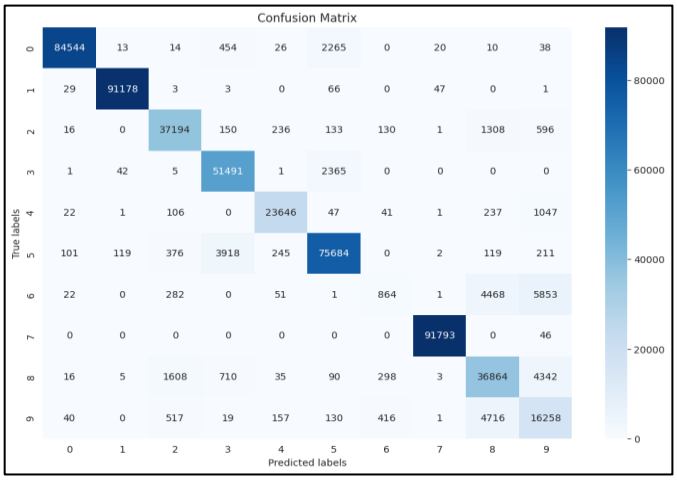

Fig. 7. Confusion matrix heatmap for artificial neural network.

The Support Vector Machine classifier was able to accurately predict 77.09% of the overall instances in the data. In addition, it accurately predicted 79.2% of the True positive instances compared to all of its predicted positive instances (0.79 precision), and it truly identified 77% of the actual positive instances (0.77 recall). Finally, the overall performance was evaluated by the F1 score, achieving a 75.27% value. Table IX shows the performance of the Support Vector Machine classifier and the confusion matrix heatmap for SVM is shown in Fig. 8.

TABLE IX. SUPPORT VECTOR MACHINE (SVM) PERFORMANCE METRICS

Metric	Value
Accuracy	0.7709
Precision	0.792
Recall	0.7709
F1 Score	0.7527

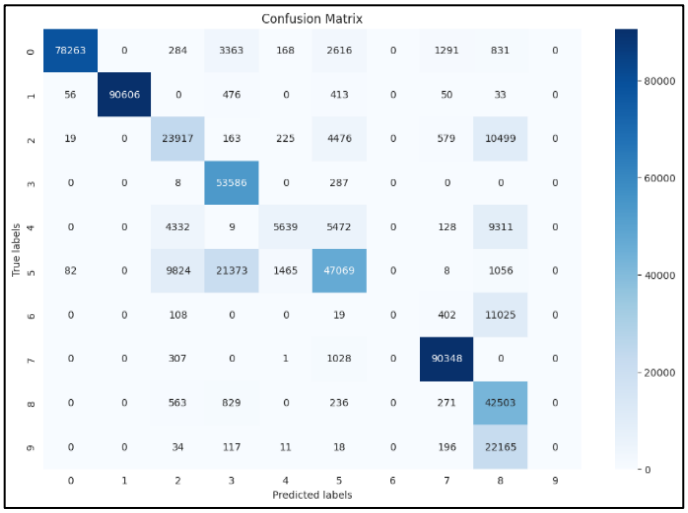

Fig. 8. Confusion matrix heatmap for SVM classifier.

Finally, from the obtained results, the performance of all five classifiers can be compared to selecting the model that is best suited for the task of identifying attacks in the NF-ToN-IoT dataset. Table X shows that the Random Forest RF classifier was able to score the highest accuracy (0.98), followed by the Decision Tree DT classifier (0.97) and the Artificial Neural Network ANN model (0.93). On the other hand, the Support Vector Machine SVM model scored a low accuracy of 0.77, whereas the lowest accuracy was achieved by the Naïve Bayes NB classifier (0.72). As for the other metrics, such as precision and recall, they can be summed up by the F1 score. The highest F1 score was achieved by the Random Forest RF Model (0.98), followed by the Decision Tree DT and Artificial Neural Network ANN (0.97 and 0.93, respectively). A low F1 score was attained by the Support Vector Machine SVM model (0.75), but the lowest F1 score was for the Naïve Bayes NB classifier, where it scored only 0.7051. A visual representation of the performance of the 5 classifiers in terms of accuracy, precision, recall, and F1 score is shown in Fig. 9.

TABLE X. COMPARISON OF THE PERFORMANCE OF THE 5 DIFFERENT CLASSIFIERS ON THE NF-TON-IOT DATASET

Classifier	Accuracy	Precision	Recall	F1 Score
NB classifier	**0.7275**	**0.7567**	**0.7275**	**0.7051**
RF classifier	**0.9841**	**0.9840**	**0.9841**	**0.9840**
DT classifier	**0.9708**	**0.9706**	**0.9708**	**0.9707**
ANN classifier	**0.9320**	**0.9316**	**0.9320**	**0.9309**
SVM classifier	**0.7709**	**0.792**	**0.7709**	**0.7527**

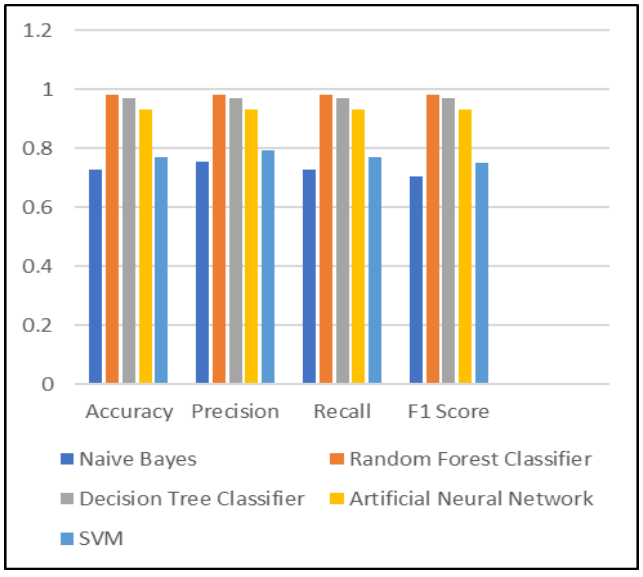

Fig. 9. Comparison of performance of the different classifiers on the NF-ToN-IoT dataset.

V. Result and Discussion

The inability of standard security systems relying on signatures and rules to identify complex breaches is well recognized. Therefore, utilizing ML and deep learning techniques and various datasets, a number of architectures and algorithms have been created in the prior literature to identify assaults and aberrant behaviors in IoT networks. The studies cited in the literature review were able to achieve relatively good and other not-so-good results. Some studies achieved low accuracy of 85%, 88%, and 89% through RF, DNN, SVM, BFV, and swarm NNs techniques in both [8], [12], and [20]. Other results were able to achieve higher accuracies. For instance, Other studies achieved higher accuracy, ranging from 91% to 92%, by using CNN, RF, and ANN techniques in both [10] and [9], while studies in [11], and [14] achieved an accuracy of 93%. Through IDS and KNN, RF, SVM. On another hand, the studies in both [7] and [13] achieved an accuracy of 94%, which is considered the highest accuracy among the studies through the use of SVM and RF algorithms.

When comparing our methodology, a higher accuracy than all previous studies was achieved by 98% with the RF model. While it achieved accuracy for both the Decision Tree classifier (0.97) and the artificial neural network model (0.93). On the other hand, the Support Vector Machine model scored a low accuracy of 0.77, while the lowest accuracy was achieved by the Naïve Bayes classified as 0.72. Additionally, the bulk of the researches mentioned in the table used ML and DL systems that were deemed untrustworthy since they were trained mostly on an outdated and unreliable dataset with low accuracy. A more current data set was produced to address this issue and published in [15] [16], which were included in our technique.

The diverse character of the Internet of Things is reflected in this dataset, also known as NF-ToN-IoT. Even though NF-ToN-IoT is better suited for IoT contexts, earlier literature was found to lack data-gathering implementation. Because there aren't many references that utilize the same dataset that we used in our study, a variety of references were employed. A number of references were used that apply to and use different datasets. The following Table XI shows a comparison of our models with other work in the literature review. Also, the visual representation of these results can be seen in Fig. 10.

TABLE XI. Compared Literature Review with Proposed Model's Results

Ref.	Author & year	Study name	Method or Technique	Dataset	Accuracy
[7]	Zhu, Hui et al. **2017**	Efficient and Privacy-Preserving Online Medical Prediagnosis Framework Using Nonlinear SVM.	ML, SVM	PID	94%
[8]	by Samrat Kumar Dey and Md. Mahbubur Rahman. **2019**	Effects of Machine Learning Approach in Flow-Based Anomaly Detection on Software-Defined Networking.	ML, RF,DNN	NSL-KDD	82%-88%
[9]	Palla, Tarun Ganesh, and Shahab Tayeb. **2021**	Intelligent Mirai malware detection for IoT nodes.	ML, ANN, RF	NBaloT	92.8%
[10]	Susilo, Bambang, and Riri Fitri Sari. **2020**	Intrusion detection in IoT networks using deep learning algorithm.	DL, CNN, ML, RF, MLP	Bot-IoT	88%-91%
[11]	Awajan, Albara. **2023**	A novel deep learning-based intrusion detection system for IOT networks.	DL, FC, IDS	DID	93.21%
[12]	Ruoli Zhao, Yong Xie, Xingxing Jia,Hongyuan Wang, and Neeraj Kumar. **2017**	Practical Privacy Preserving-Aided Disease Diagnosis with Multiclass SVM in an Outsourced Environment	SVM, BFV	UCI dermatology	85.4%.
[13]	Alqahtani, Hamed, et al. **2020**	Cyber intrusion detection using machine learning classification techniques	ML, RF	KDD'99 cup	94%
[14]	Chola, Channabasava, et al. **2021**	IoT based intelligent computer-aided diagnosis and decision making system for health care.	KNN, SVM, RF, LR and AB	UCI heart disease	93.54%
[20]	Awotunde, Joseph Bamidele, et al. **2021**	A deep learning-based intrusion detection technique for a secured IoMT system.	IoMT, swarm NNs	NF-ToN-IoT	89%
The proposed Model			**RF, NB, DT, ANN, SVM**	**NF-ToN-IOT**	**RF 98%**

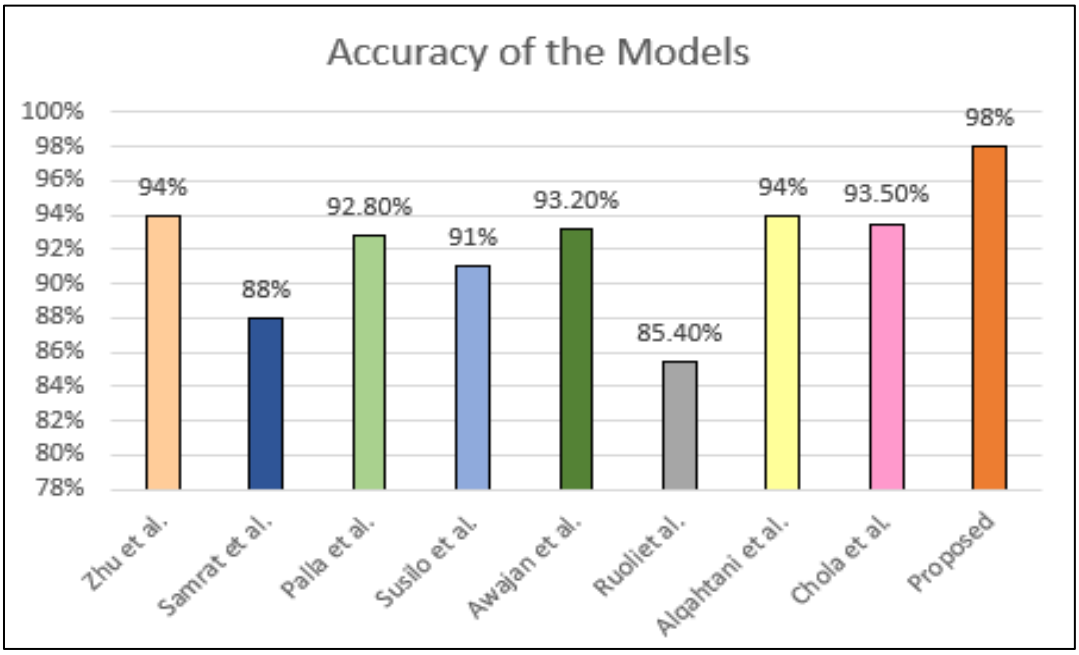

Fig. 10. Histogram showing the Accuracy of Different Models from Literature Review and the Proposed RF Model.

VI. Conclusion

The internet of things IoT environment deals with a huge amount of private and sensitive health data that must be kept safe from tampering or theft. If safety precautions are not implemented, these dangers and assaults against IoT devices in the health sector might completely destroy this industry. These attacks are often carried out to make money, either by selling the stolen data or by holding the victim's data at ransom to release their data. In the healthcare sector, using technology especially IoT technology can be a big leap forward towards providing a better service for patients and facilitating communications and sharing essential files or tasks. For this reason, implementing IoT in healthcare is essential.

However, several privacy and security concerns arise when using IoT. If safety precautions are not implemented, these dangers and assaults against IoT devices in the health sector might completely destroy this industry. These attacks are often carried out to make money, either by selling the stolen data or by holding the victim's data at ransom to release their data.

Thus, it becomes equally important to implement a system that can provide security while implementing IoT. In this research, five different classifiers were employed to predict the occurrence of attacks while using IoT services. For this purpose, the NF-ToN-IoT dataset was selected, where the data were pre-processed before being split into training and testing data. Upon testing the models, it was evident that the RF model achieved the best results; scoring the highest accuracy (0.98) and highest F1 score (0.98). The second-best model was DT classifier, followed by the ANN model.

VII. Future Work

The future works aim to experiment with models with different algorithms and different data sets, as well as to combine several deep and machine learning algorithms, in order to come up with models that give the highest possible accuracy rates and the lowest possible loss rates to obtain the best optimal results in classifying attacks in IoT devices in the electronic health sector and a comparison between data sets and algorithms.

Acknowledgment

The Vice Presidency for Graduate Studies and Scientific Research at Jouf University is funding this study as a part of its initiative to encourage scientific publications.

References

[1] Mustafa, Twana, and Asaf Varol. "Review of the internet of things for healthcare monitoring." 2020 8th International Symposium on Digital Forensics and Security (ISDFS). IEEE, 2020.

[2] Ibrahim, D., and N. Majma. "Improvement of Data Transfer Reliability in IoT-based Coronavirus Patients' Health Monitoring System using by IoT Analytics Expert Systems." CENTRAL ASIAN JOURNAL OF MATHEMATICAL THEORY AND COMPUTER SCIENCES 4.3 (2023): 18-38.

[3] Kelly, Jaimon T., et al. "The Internet of Things: Impact and implications for health care delivery." Journal of medical Internet research 22.11 (2020): e20135.

[4] Zeadally, Sherali, et al. "Smart healthcare: Challenges and potential solutions using internet of things (IoT) and big data analytics." PSU research review 4.2 (2020): 149-168.

[5] Kadhim, Kadhim Takleef, et al. "An overview of patient's health status monitoring system based on internet of things (IoT)." Wireless Personal Communications 114.3 (2020): 2235-2262.

[6] Alenoghena, Caroline Omoanatse, et al. "eHealth: A survey of architectures, developments in mHealth, security concerns and solutions." International Journal of Environmental Research and Public Health 19.20 (2022): 13071.

[7] Zhu, Hui et al. "Efficient and Privacy-Preserving Online Medical Prediagnosis Framework Using Nonlinear SVM." IEEE journal of biomedical and health informatics vol. 21,3 (2017): 838-850. doi:10.1109/JBHI.2016.2548248

[8] Dey, Samrat Kumar, and Md Mahbubur Rahman. "Effects of machine learning approach in flow-based anomaly detection on software-defined networking." Symmetry 12.1 (2019): 7.

[9] Palla, Tarun Ganesh, and Shahab Tayeb. "Intelligent Mirai malware detection for IoT nodes." Electronics 10.11 (2021): 1241.

[10] Susilo, Bambang, and Riri Fitri Sari. "Intrusion detection in IoT networks using deep learning algorithm." Information 11.5 (2020): 279.

[11] Awajan, Albara. "A novel deep learning-based intrusion detection system for IOT networks." Computers 12.2 (2023): 34.

[12] Zhao, Ruoli, et al. "Practical Privacy Preserving-Aided Disease Diagnosis with Multiclass SVM in an Outsourced Environment." Security and Communication Networks 2022 (2022).

[13] Alqahtani, Hamed, et al. "Cyber intrusion detection using machine learning classification techniques." Computing Science, Communication and Security: First International Conference, COMS2 2020, Gujarat, India, March 26–27, 2020, Revised Selected Papers 1. Springer Singapore, 2020.

[14] Chola, Channabasava, et al. "IoT based intelligent computer-aided diagnosis and decision making system for health care." 2021 International Conference on Information Technology (ICIT). IEEE, 2021.

[15] T.-I. D. N. Moustafa, 2020, [online] Available: https://cloudstor.aarnet.edu.au/plus/s/ds5zW91vdgjEj9i

[16] D'hooge, S.| L. (2023) NF-ton-IOT, Kaggle. Available at: https://www.kaggle.com/datasets/dhoogla/nftoniot

[17] Sahoo, Kabita, et al. "Exploratory data analysis using Python." International Journal of Innovative Technology and Exploring Engineering 8.12 (2019): 4727-4735.

[18] Khaire, Utkarsh Mahadeo, and R. Dhanalakshmi. "Stability of feature selection algorithm: A review." Journal of King Saud University-Computer and Information Sciences 34.4 (2022): 1060-1073.

[19] Dhal, Pradip, and Chandrashekhar Azad. "A lightweight filter based feature selection approach for multi-label text classification." Journal of Ambient Intelligence and Humanized Computing (2022): 1-13.

[20] Awotunde, Joseph Bamidele, et al. "A deep learning-based intrusion detection technique for a secured IoMT system." International Conference on Informatics and Intelligent Applications. Cham: Springer International Publishing, 2021.