Anomaly-Based Intrusion Detection System in Industrial IoT-Healthcare EnvironmentNetwork

***Abstract*—The Internet of Things (IoT) technology facilitates automation, monitoring, and control of tangible objects and surroundings by enabling connected devices to interact and exchange data over the Internet. Developments in edge computing, blockchain, and artificial intelligence (AI) are incorporated into IoT technologies for more reliable operations. Inadequate authorization, authentication, and encryption protocols could render IoT networks insecure and open the door to illegal access and data breaches which can have terrible consequences, most notably in the healthcare industry. In this regard, to identify malicious and incursion traffic, machine learning (ML) is crucial to Internet of Things (IoT) cybersecurity. The paper proposes a framework to detect intrusion or malicious traffic in IoT-enabled different medical equipment such as medical sensors, and controllers for real-time data collection, creating communication channels and data monitoring and analysis over locally available network nodes. IoT-Flock has been utilized for both normal and malicious traffic generation in a wide dataset found by the sensors connected to IoT integrated healthcare network. The feature selection-based proposed framework has been evaluated by three distinct machine learning classifiers, KNN, RF, and DT where corresponding accuracy, sensitivity, precision, and F1-score have been measured for performance analysis. With an accuracy of 99.74%, the KNN technique performed better than the other tactics used by RF and DT regarding intrusion detection in IoT networks. The suggested framework will be helpful in developing or analyzing security solutions in IoT-integrated network systems.**

Keywords—IoT,cybersecurity, IoT-Flock, intrusiondetection, healthcare, IIoT, IDS, malicious traffic, feature selection.

I. INTRODUCTION

TheInternet of Things (IoT) is a term that refers to a group of network-enabled gadgets able to gather and share information across the Internet [1]. This technology enables such devices to connect with one another, analyze real-time data, and take autonomous actions depending on the information gathered. Upon activation, these networked devices run real-time systems of operation to process the gathered data. The integration of diverse objects into networks has brought attention to communication in the Internet of Things [2]. Radiofrequency identification and wireless sensor networks with internet enabling small to big networks are among the technologies often used in communication with large numbers and a variety of applications [3]. By linking the real world with digital systems, IoT technology has the possibility of boosting efficiency, productivity, and quality of life across numerous industries. With 17 billion linked devices globally, it is projected that the consumer sector will account for the majority of Internet of Things (IoT) connected products by 2030. In the retail division, From 2019 levels, the amount of interconnected gadgets is predicted to more than quadruple [4]. This technology is moving towards a worldwide economic upswing for information development, which will have an enormous impact on industrial growth, innovation, and technical improvement. IoT-enabled devices include various aspects from household appliances to wearables and industrial gear. Specially, in the healthcare sector, this technology is revolutionizing patient care, remote monitoring, and medical infrastructure. Patients may continually monitor their blood pressure, blood sugar, and heart rate using wearable technology and sensors, which provide important information for early detection and preventative management [5]. By permitting remote monitoring systems, medical staff can maintain a watchful eye on their patient's health state, cutting down on the number of hospital visits required and facilitating prompt treatments for post-operative care or chronic diseases. Medical equipment and gadgets with Internet of Things capabilities help hospitals run more efficiently by optimizing resource allocation, guaranteeing prescription adherence, and automating inventory management [6]. Moreover, IoT makes it easier to integrate medical equipment and electronic health records (EHRs), enabling smooth data analysis and interchange that results in better-informed choices and customized treatment programs. In this regard, IoT devices are proliferating globally, and operations are needed to manage, test, debug, and secure these networked devices in real time. However, the majority of IoT devices are notorious for having security flaws and lacking in-device security measures to defend against cyberattacks [7]. The importance of attacking gadgets increases as more of them are connected to the internet with one another. The financial impact of cybercrime on American entities, including lost productivity, recovery expenses, and theft of intellectual property, was estimated by researchers to be $385 billion in 2012, which is currently about $945 billion [8]. Because of the most of incorporated IoT devices have compact operating systems, installing antivirus software cannot be ensured. This is because IoT devices have limited resources and poor processing power, which makes it possible for them to only perform a limited number of operations [9]. Since the data or control in IoT-linked medical equipment is directly tied to individual's health-related services, security is the main issue here. For example, patients are admitted to the ICU, if they are critically wounded or very ill and need ongoing medical attention. The slightest communication interruption brought on by cybersecurity issues in this kind of situation could potentially seriously compromise the patient's life, perhaps even resulting in death. When these devices are installed, they are normally linked to the common bus of the network having no protection measures or defensive line on the consumer end, and the majority of IoT device manufacturers are selling their products at very cheap rates without giving any importance to security issues [10]. Therefore, the most

pressing requirement for a reliable and secure data transmission network is an IoT-driven medical infrastructure that is immune to malicious attacks. For example, if an unauthorized person gains access to a pacemaker, a heart patient can soon suffer from bradycardia or tachycardia, which either slows down or speeds up the heartbeat, which ultimately results in death. Classifying any behavior that deviates from the expected behavior as an anomaly, artificial intelligence is employable by anomaly-based IDS systems to get around this restriction. Many researchers have used ML approaches to identify malicious attacks in IoT network monitoring systems as a result of recent advancements in ML.

II. LITERATURE SURVEY

An effective defense against cyberattacks is provided by intrusion detection systems (IDS). This detection is one of the numerous new applications brought out by machine learning's quick advancement. Nowadays, ML and AI are frequently employed in IDS. An attribute of a new data point is possibly classified or predicted using a model that is created by a machine learning (ML) algorithm using datasets where features set keep significance regarding the effective recognition of malicious traffic in the IoT environment [11]. Despite being well-established, the current IDS technology is insufficient for connected systems and devices. Thus, creating IoT-supported IDS is becoming essential. While a few studies have been conducted on IDS, very few are currently trying to provide the ideal IoT dataset over testing and validating the IoT-supported IDS. The paper [12] suggests a framework for creating context-aware IoT security solutions in which the performance of ML classifiers is assessed using widely used metrics including accuracy, recall, precision, and F1-score. The CAIDA dataset, which contains traffic header data without payload, is mentioned as an example but is not suitable for direct performance assessment of IDS due to lack of labeling. A model [13] combines two different sets of data, IoTID20 and UNSW-NB1, to increase the capability of detecting malicious traffic from both types of networks. The datasets were horizontally merged by using principal component analysis to lower the feature amount for each set of data to 30. The EBF algorithm exhibited great accuracy, according to the results obtained considering two and four classes, correspondingly, based on the dataset (multi-domain). Different methods, such as Naïve Bayes and DT classifiers on a cybersecurity dataset obtained from sensors measuring water level, pH, temperature, humidity, and soil moisture by the authors [14] where classifiers are able to identify the greatest quantity of IoT attack classes derived from several data sources within the identical dataset in IoT based irrigation or agri-harvesting environment. The results demonstrate that the accuracy achieved by Decision Tree is 72% and at its lowest 45% for Naïve Bayes. Another approach [15] in developing a network-IDS with constrained processing power for IIoT scenarios has been introduced. The UNSW-NB 15 dataset and the conventional KDD-CUP-99 dataset are used to verify the suggested approach, which performs better than earlier approaches with an accuracy rate of around 89.75%. The feature selection algorithm called CorrAUC, which is based on a wrapper technique to filter and predict traffic flow in IoT traffic detection was employed by the authors [16] and suggested the use of the VIKOR multicriteria decision method to validate the selected features for recognizing traffic flow errors in the network, achieving average results of >96%. Another paper [17] proposes a multitask deep learning model based on LSTM for detecting IoT malware, which efficiently performs two tasks, and extracts features where three different modalities were identified within the dataset. The flow-related and flag-related modalities showed the best testing accuracies for different tasks as well as multitask classification, with accuracies of 92.63%. The ACID approach has been evaluated using both synthetic and real intrusion datasets covering 20 years in [18]. Authors claim that this approach also shows a good outcome in addressing the difficulty of being sensitive to tiny variations in traffic features, ranging that frequently result in misinterpretation. It is based on low-dimensional embedded data acquired by the use of a minimal model made up of several kernel networks to separate samples of different classes. A framework [19] with a random neural network approach for anomaly identification in IoT network traffic tracking for smart cities shows improved computation performance and the simulation model demonstrates noticeable improvement in most of the categorical attacks. Nevertheless, the majority of these techniques from different literature are based on the outdated KDD-CUP-99 dataset, that's does not include many updated malicious traffic generation systems. Recently, the UNSW-NB 15 intrusion detection dataset has been developed in order to address this issue by [20]. The Random Forest-based classifier (RF) in the feature selection model generates the variable to predict both typical and abnormal IIoT activity [21]. The feature selection methodology was put out in [22], with the (RF) classification acquiring results for malicious traffic prediction. The suggested method, MNSWOA-IPM-RF, provides improved performance measured by the area under the ROC curve and accuracy, according to experimental findings using IIoT datasets. Another approach [23] has been proposed with a Random Forest Classification model in terms of DDoS attack recognition utilizing the fusion context of the model. In comparison to HMM and SVM methods for DDoS attack detection, the simulation of experimental findings demonstrates that the RFC model has a reduced rate of false alarms and a greater detection rate.

III. IOT ENVIRONMENT

The growing usage number of IoT devices in contemporary workplaces raises the possibility of a malware-infected IoT device getting with compromising an organization's network. An employee who brings their own attacked IoT device to the workplace and connects it to the network without realizing it might also be the source of this, as could an attacker attempting to access the primary systems of the organization. Healthcare is one of the industries that is putting massive operations of IoT-based ecosystems into execution, such as IIoT. Since these platforms rely on networks, they are susceptible to new attacks and breaches. Such systems must be made safe by creating feature selection that is integrated with reliable machine-learning models.

A. IoT integrated Network Environment

The proposed system has been developed in the healthcare environment. Using IoT-enabled medical equipment for real-time data collection, creating communication channels, connecting to cloud platforms for data storage and analytics, putting real-time alerts and notifications for medical professionals allowing remote observation, ensuring that smooth data exchange to enhance

patient outcomes and operational effectiveness in health care monitoring and control. Particularly, considering an IoT system network integrated with multiple patient monitoring sensors and devices and control units in the network. More particular, in this proposed IoT network, heart function is monitored using a remote electrocardiogram (ECG), which records heart rates every second between 0 and 200 bpm. An infusion pump delivers levels ranging from 10 to 100 mL. Every second, the pulse oximeter records the blood oxygen percentage. Mouth/Nasal Airflow, the sensor records the respiration rate. A blood pressure sensor captures the diastolic and systolic pressure. Every ten minutes, a glucose monitor tracks blood glucose. The body temperature sensor records readings between 0°F and 120°F whereas an electromyography (EMG) sensor records muscle contraction. Every five minutes, the skin conductance is determined using a GSR sensor.

B. *IoT Traffic Generation*

The proposed framework creates real-time IoT traffic from the IoT scenario that generates traffic to build a context of IoT integrated network security system for unusual traffic recognition in the IoT medical care scenario. The initial module of the suggested architecture is the IoT use case generator, composed of the publicly available IoT traffic-producing program IoT-Flock. The typical traffic producer methods are not able to generate the traffic relevant to IoT regulation because of the variety of IoT networks with respect to devices, applications, and protocols. Therefore, it is not possible to create and evaluate the effectiveness of IoT-specific safety measures using conventional traffic generation tools and COAP and MQTT are two different IoT protocols that are facilitated by IoT-Flock.

A real-time IoT healthcare monitoring scenario is considered as the use case environment in the proposed farmwork whileusing a local area Internet Service Provider (ISP) network (WLAN) setting, all of the devices and sensors interact with one another over the MQTT protocol. Using this technology, one can insert customized IoT devices, and produce both normal and malicious traffic.

IV. ALGORITHM OF THE PROPOSED SYSTEM

Based on machine learning and feature selection approaches, this research suggests a successful network intrusion detection solution. The ML approach (KNN, RF, DT) is used in the performance measurements where the dataset was created by combining artificially generated modern attack behaviors with actual daily activities.The dataset's relative balance between the two classes is favorable for both model training and validation andthe features are classified into "Abnormal_URL" and "Normal_URL".

A. *k-nearest Neighbors*

One of the simplest ML methods that can be utilized for both regression and classification issues is the KNN. Convergent items are assumed to be the same in this approach. The KNN approach measures the distance between each item in the training data and the item to be categorized in order to classify a new condition. The number of the substance to be classified's closest neighbors or K, is then calculated to get the highest possible value. To find the ideal value of k, many values are often attempted. The outcome of the categorization is decided by the neighbors casting in a majority. The Euclidean method is used by the KNN approach to calculate the distance between two points (Fig. 1).

$$\text{Distance(i, j)} = \sqrt{(X_{i1} - X_{j1})^2 + \cdots + (X_{in} - X_{jn})^2} \qquad (1)$$

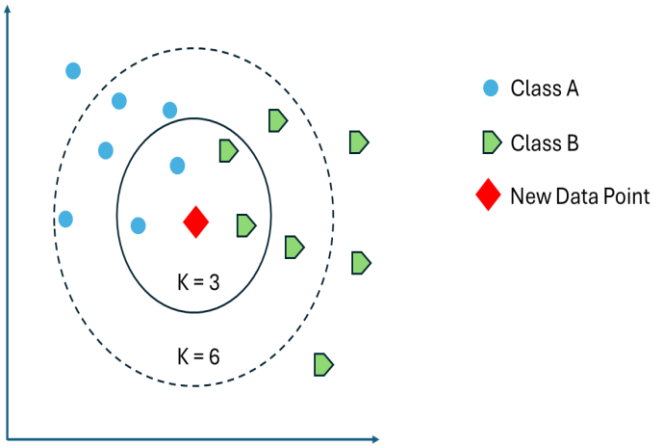


Fig. 1. Visual representation of KNN algorithm.

B. *Random Forest*

Numerous decision-tree models are included in the bagging model known as random forest. Every tree in a random forest is trained and capable of independent prediction. A voting system determines the ultimate choice (Fig. 2). Two random subsets are inserted into a random forest to ensure the variety of the base classifier and prevent overfitting: a random subset of the initial training set and a random subset of the initial feature set. For example, in a random forest with N decision trees, its initial training set (D) and feature set (V) are assumed. Random forest creates N subsets of D using a bootstrapping procedure. With the N number of subsets, N number of decision trees will be individually created.

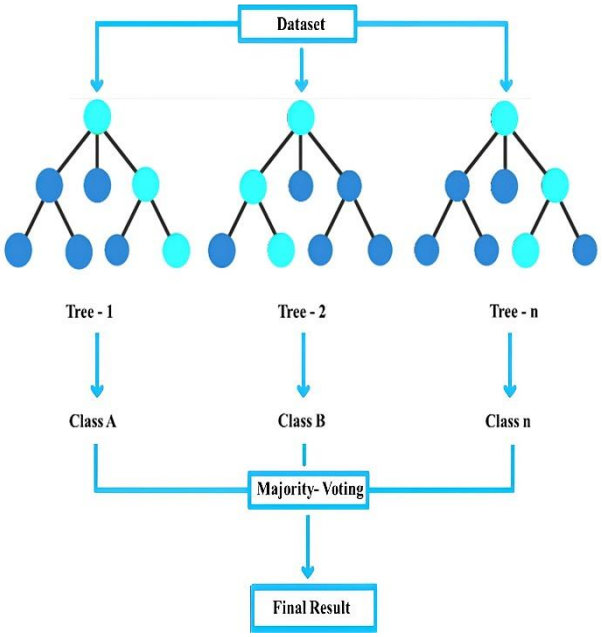


Fig. 2. Visual representation of RF algorithm.

$$\hat{y}_i = argmax \sum_{K=1}^{N} \mathrm{I}\,(T_k(x_i) = y)$$

Where, $I\,(T_k(x_i) = y) = \begin{Bmatrix} 1; & if\ \ T_k(x_i) = y \\ 0; & if\ \ T_k(x_i) \neq y \end{Bmatrix}$

Generally, the basic classifier in a random forest is a classification and regression tree (CART) decision tree. A splitting feature's information gain and value are assessed by the CART algorithm using the Gini index. Here's how to compute the Gini index assuming there are K classes and p_k as the probability of the k-th class:

$$Gini\ (p)\ = \sum_{K=1}^{K} P_k\ (1 - P_K) = \ 1 - \sum_{K=1}^{K} {P_k}^2$$

C. *Decision Tree*

Here, the trees are prominent machine-learning classifiers for categorization because of their effectiveness and performance. There are two processes involved in decision tree classification. Creating the tree is the first step. This tree is used to extract categorization rules in the second stage. Decision trees are primarily made up of roots, branches, and leaves. From the root to the leaf, decisions are made. Every subtree that is added to a new node undergoes this iterative process once again (Fig. 3).

The algorithm basically learns how to partition data efficiently such that the quantity of impurity in the leaf nodes is minimal.

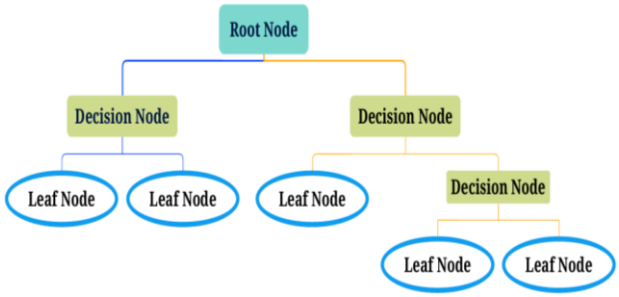


Fig. 3. Visual representation of DT algorithm.

V. DATA PROCESSING

Since raw data frequently tends to be uneven and noisy and may include missing, redundant, and unnecessary data, pre-processing before training is an important stage in machine learning approaches. The quality of the supplied data has a major impact on how effective the ML method is. Thus, precise pre-processing is necessary to create a model with excellent accuracy and high performance. The following stages provide a summary of the pre-processing of the data used in this investigation. Fig.4 illustrates the suggested structure.

Categorical characteristics in the dataset have been converted to integers using label encoding. The name encoding technique has been used to transform the three categorical characteristics in the dataset—protocol_type, service, and flag—to numbers.The dataset's numerical column values have been converted to a conventional scale between 0 and 1 using the min-max normalization approach, which prevented the value ranges from being distorted.In order to find outliers (observations for predictive variables) of levels in our dataset, we've used Cook's distance, an effective technique for detecting scaled variations in fit values. An outlier may be a result where Cook's distance is in excess of three of the average values.

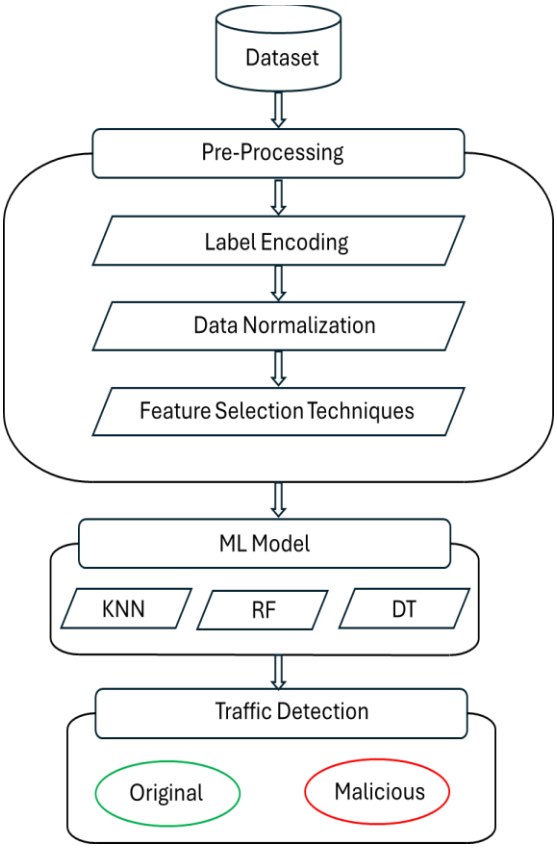


Fig. 4. Data processing and detection scheme.

$$D_i = \frac{\sum_{j=1}^{n} (Y_j - Y_{j(i)})^2}{P^{MSE}} \qquad (2)$$

Where, D_i=Cook's distance;

P = Coefficients number in the model

Yi = Fitted response (j times)

MSE = Mean Standard Error

A more accurate classification procedure depends on the crucial feature selection that influences the classification outcome. Using a DT methodology to ascertain the feature's relevance is one of the best methods for feature selection.

The DT technique's feature importance property is useful in assessing each feature's significance and impact on the classification outcome.

A. *Protection Scheme of Proposed Model*

Fig. 5.provides a broad framework of the system, which is essentially made up of three layers: the application data and the communication or network layer. IoT nodes or smart sensor data make up the data layer where the next layer receives aggregated data, which might be from sensors or any other kind of data user. This layer is made up of switching or gateway devices that are in charge of evaluating the network data that has been gathered. As the normal data packets are transmitted to the subsequent layer for processing and storage, the abnormal packets are examined using the suggested method and are then stopped. We provided a detailed, step-by-step explanation of the approach suggested in this section.

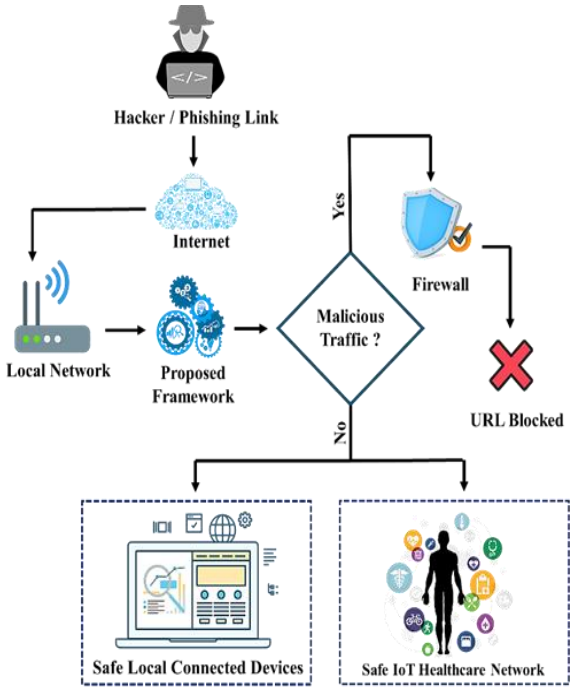


Fig. 5. Protection scheme by integrating the proposed model.

Safeguarding sensitive data from unwanted attacks requires individuals and business organizations to include safety features like firewalls, antivirus software, and malware detection systems in their networks. For commercial networks, especially in the healthcare sector, relying just on a traditional firewall is insufficient since certain harmful attack types cannot be prevented. By implementing the proposed model along with an additional algorithm of protection and alert system, network-based detection systems in online network traffic data can identify the majority of malware at the server or network gateway, protecting devices and access of data before it infects the end user.

VI. PERFORMANCE ANALYSIS

Accuracy, sensitivity, precision, and F1-score are the four quality metrics that were utilized to evaluate the algorithm's performance. Malicious samples are shown as a '1' and are regarded as positive. On the other hand, normal samples are denoted by a '0' and are regarded as negative in traffic detection.

TABLE 1: PERFORMANCE MEASUREMENTS MATRICES

Name	Measurements (Prediction)
True Positives (TP)	Malicious as malicious
True Negatives (TN)	Normal as normal
False Positives (FP)	Normal as malicious
False Negatives (FN)	Malicious as normal

Where, Accuracy $= \frac{(TN+TP)}{(TN+TP+FN+FP)}$ (2)

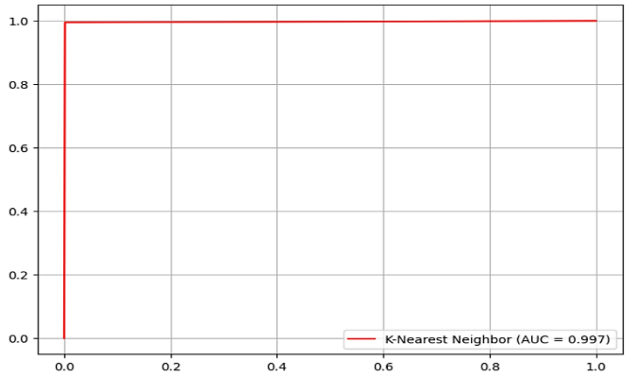
Sensitivity $= \frac{TP}{TP+FN}$ (3)

Precision $= \frac{TP}{TP+FP}$ (4)

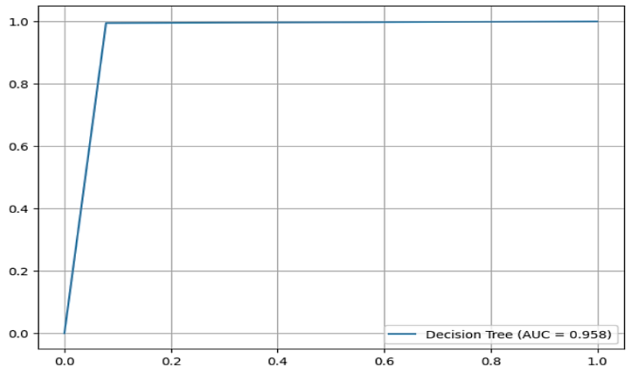
F1 Score $= \frac{2(Precesion \ * Sensitivity \ )}{(Precesion \ + Sensitivity \ )}$ (5)

VII. RESULTS

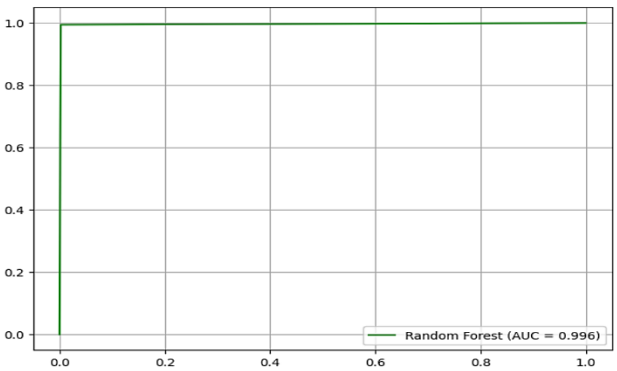
This section provides a detailed explanation of the experiment's findings and analysis, for efficient feature selection in the detection of anomalous and unauthorized IoT traffic.The three feature selection methods were compared on several features from the selected datasetin the context of an IoT network, including sufficient data to enable precise anomaly and intrusion detection. We used three distinct machine learning classifiers—KNN, RF, and DT Classifiers for performance assessment in this comprehensive study.In contrast to other applicable machine learning classifiers, the Decision Tree (DT) technique achieves lower accuracy results for IoT anomaly and intrusion detection in the healthcare environment when employing the selected features and provided machine learning classifiers.



(a)



(b)



(c)

Fig. 6. ROCCurve(AUC) of (a) KNN, (b) DT, and (c) RF algorithm.

In our investigation, The KNN method performed better than the other strategies with an accuracy of 99.74%, the highest of all the techniques. The DT approach had the poorest accuracy, at 95.87%, while the RF method finished second, at 99.61% (Fig.6).

TABLE 2: PERFORMANCE MEASUREMENTS

Algorithm	Accuracy	Precision	Sensitivity	F-1 Score
KNN	99.74%	99.79%	99.51%	99.65%
RF	99.61%	99.70%	99.46%	99.58%
DT	95.87%	90.35%	99.50	94.70%

Table 2 presents a performance comparison of the three machine learning classifiers based on their Accuracy, Precision, Sensitivity, and F-1 Score in identifying malicious and normal traffic in the online network of medical appliances context. It is noted that with 99.79% accuracy, 99.51% sensitivity, and 99.65% F1-score outcomes, the KNN classifier surpassed all other ML classifiers.

TABLE 3: COMPARISON WITH RELATED STUDIES

	Prop.	[15]	[14]	[20]	[16]	[17]
Acc (%)	99.74	89.90	72.00	99.95	99.00	71.49
Pre (%)	99.79	94.60	68.00	100	99.00	72.69
Tpr (%)	99.51	89.28	71.00	99.90	-	76.39
F1 (%)	99.65	91.87	68.00	99.95	-	73.69

A comparison with the recent studieshas been represented in Table 3.IoT traffic has been generated with an open-source IoT traffic-generating application called IoT-Flock in the proposed system for medical application datasetwhereasthese methods have been tested with different datasets and different algorithms. Therefore the above methods can not be compared directly with the proposed technique in a short description.When compared to all prior findings, the suggested strategy produces the best precision, F1-score, and forecast accuracy except [20] though this method has been tested with the UNSW-NB 15 intrusion detection dataset.

VIII. CONCLUSION

Cyberattacks against individuals, business entities, and other organizations have significantly increased. Because of the rapid advancements in technology, attackers are becoming more skilled, and conventional intrusion detection systems are unable to identify complex cyberattacks. Numerous research has used ML approaches to create IDS systems since the remarkable achievements of ML and DL methods in a wide variety of disciplines.Through experimental analysis, the suggested methods were able to identify anomalies and intrusion attempts in IoT networks. Among the applied three ML approaches KNN classifier achieved the most prominent outcomes followed by RF classifier with99.74 and99.61 percent of accuracy. The DT algorithm had the lowest accuracy about95.87%. However, the features selected by the suggested framework provide excellent outcomes in terms of sensitivity, accuracy, and precision.The only thing being addressed in this study is whether the IoT traffic is malicious or normal. It may be possible to categorize the many forms of cybersecurity assaults in future research. By combining many independent classifiers, and more advanced techniques may also increase classification accuracy.

REFERENCES

[1] Madakam, Somayya, Ramya Ramaswamy, and Siddharth Tripathi. "Internet of Things (IoT): A literature review." Journal of Computer and Communications 3.5 (2015): 164-173.

[2] Sharma, Neha, Madhavi Shamkuwar, and Inderjit Singh. "The history, present and future with IoT." Internet of things and big data analytics for smart generation (2019): 27-51.

[3] Willig, Andreas, Kirsten Matheus, and Adam Wolisz. "Wireless technology in industrial networks." Proceedings of the IEEE 93.6 (2005): 1130-1151.

[4] "IoT Connected Devices by Vertical 2030." Statista, www.statista.com/statistics/1194682/iot-connected-devices-vertically/. Accessed 16 Mar. 2024.

[5] Yuehong, Y. I. N., et al. "The internet of things in healthcare: An overview." Journal of Industrial Information Integration 1 (2016): 3-13.

[6] Ghosh, Uttam, et al., eds. Intelligent Internet of Things for Healthcare and Industry. Springer International Publishing, 2022.

[7] 7 Yang, Yuchen, et al. "A survey on security and privacy issues in Internet-of-Things." IEEE Internet of things Journal 4.5 (2017): 1250-1258.

[8] Zhanna Malekos Smith, Eugenia Lostri, and James A Lewis. The Hidden Costs of Cybercrime. McAfee, p. 38.

[9] Hassan, Wan Haslina. "Current research on Internet of Things (IoT) security: A survey." Computer networks 148 (2019): 283-294.

[10] Almolhis, Nawaf, et al. "The security issues in IoT-cloud: a review." 2020 16th IEEE International Colloquium on Signal Processing & Its Applications (CSPA). IEEE, 2020.

[11] Dasgupta, Dipankar, Zahid Akhtar, and Sajib Sen. "Machine learning in cybersecurity: a comprehensive survey." The Journal of Defense Modeling and Simulation 19.1 (2022): 57-106.

[12] Hussain, Faisal, et al. "A framework for malicious traffic detection in IoT healthcare environment." Sensors 21.9 (2021): 3025.

[13] N. Moustafa and J. Slay, "UNSW-NB15: a comprehensive data set for network intrusion detection systems (unsw-nb15 network data set)," in Proc. IEEE Military Communications and Information Systems Conf. (MilCIS), pp. 1-6, 2015.

[14] Samin, Omar Bin, et al. "Malicious Agricultural IoT Traffic Detection and Classification: A Comparative Study of ML Classifiers." Journal of Advances in Information Technology 14.4 (2023).

[15] Wang, Sying-Jyan, et al. "Feature selection for malicious traffic detection with machine learning." 2020 International Computer Symposium (ICS). IEEE, 2020.

[16] Hema, V. Sri Vigna, S. Devadharshini, and P. Gowsalya. "Malicious Traffic Flow Detection in IOT Using Ml Based Algorithms." International Research Journal on Advanced Science 3.5: 68-76.

[17] Ali, Sajid, et al. "Effective multitask deep learning for iot malware detection and identification using behavioral traffic analysis." IEEE Transactions on Network and Service Management (2022).

[18] Diallo, Alec F., and Paul Patras. "Adaptive clustering-based malicious traffic classification at the network edge." IEEE INFOCOM 2021-IEEE Conference on Computer Communications. IEEE, 2021.

[19] Rughoobur, Paavan, and Leckraj Nagowah. "A lightweight replay attack detection framework for battery depended IoT devices designed for healthcare." 2017 international conference on Infocom technologies and unmanned systems (trends and future directions)(ICTUS). IEEE, 2017.

[20] Diwan, Tarun Dhar, et al. "Feature entropy estimation (FEE) for malicious IoT traffic and detection using machine learning." Mobile Information Systems 2021 (2021): 1-13.

[21] Farnaaz, Nabila, and M. A. Jabbar. "Random forest modeling for network intrusion detection system." Procedia Computer Science 89 (2016): 213-217.

[22] Ikram, Sumaiya Thaseen, et al. "Prediction of IIoT traffic using a modified whale optimization approach integrated with random forest classifier." The Journal of Supercomputing 78.8 (2022): 10725-10756.

[23] Chen, Yini, et al. "DDoS attack detection based on random forest." 2020 IEEE International Conference on Progress in Informatics and Computing (PIC). IEEE, 2020.