Iraqi Journal for Computer Science and Mathematics

Manuscript 1301

IoT Flow Parameters Classification Based on Machine Learning Techniques

El-Sayed M. El-Kenawy

Marwa M. Eid

Ban Salman Shukur

Amel Ali Alhussan

Doaa Sami Khafaga

IRAQI JOURNAL FOR COMPUTER SCIENCE AND MATHEMATICS 2025;6:453–462

ORIGINAL STUDY

IoT Flow Parameters Classification Based on Machine Learning Techniques

El-Sayed M. El-Kenawy [a,b,*], **Marwa M. Eid** [c,d], **Ban Salman Shukur** [e], **Amel Ali Alhussan** [f], **Doaa Sami Khafaga** [f]

[a] School of ICT, Faculty of Engineering, Design and Information & Communications Technology (EDICT), Bahrain Polytechnic, PO Box 33349, Isa Town, Bahrain
[b] Applied Science Research Center, Applied Science Private University, Amman, Jordan
[c] Faculty of Artificial Intelligence, Delta University for Science and Technology, Mansoura 11152, Egypt
[d] Jadara University Research Center, Jadara University, Jordan
[e] Computer Engineering Techniques Department, Technical Engineering College, Al-Bayan University, Baghdad 10011, Iraq
[f] Department of Computer Sciences, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, P.O. Box 84428, Riyadh 11671, Saudi Arabia

ABSTRACT

In recent years, there has been a highly remarkable convergence of artificial intelligence (AI) and the Internet of Things (IoT), which has made rapid progress in smart city initiatives by developing smart devices for such cities. Since these devices are increasingly diversified, they require a resilient communication network to demonstrate high performance in managing consistent traffic flows. A machine learning model intended for identifying network parameters from diverse devices, in addition to proposing modifications meant for network performance enhancement, is developed in this study. In relation to packet data as a network traffic parameter, employing gateway devices can facilitate its transmission and reception. In applying classification and prediction, the model can employ six various machine learning approaches, comprising Decision Tree (DT), Random Forest (RF), Support Vector Machines (SVM), K-Nearest Neighbor (KNN), Naive Bayes (NB), and Stochastic Gradient Descent Classifier (SGDC). We have employed 40 different IoT devices in a real-time smart laboratory setup for the purpose of testing the model's performance. The study indicates the effectiveness of the model, which achieved an average accuracy of 92.2%, F1-score of 92%, recall of 92%, and precision of 91.7%. The Decision Tree classifier reached the best effectiveness by achieving accuracy at 99.9% with an F1-score of 99.8% and precision at 98.8%. The success rate of 99.9% from the proposed model evidences its strong capacity to correctly identify IoT device traffic across different circumstances, thus improving network security and performance.

Keywords: IoT, Network traffic classification, Machine learning

1. Introduction

IoT is growing increasingly significant across economic sectors, with 92% of enterprises anticipating it to be crucial by 2020 [1]. Despite its benefits, security, privacy, cost, and regulation remain difficulties. According to Gartner, IoT devices were mostly used in smart buildings before 2017. Since 2017, smart homes have dominated IoT implementation [2]. IHS Markit reports that the smart home industry comprised 822.6 million IoT devices, with an anticipated annual growth rate of 19.6% by 2021, positioning it as one of the most rapidly expanding sectors, alongside industrial IoT. The accurate categorization of IoT devices is crucial for detecting unwanted devices and enhancing network security and traffic management [3].

Received 21 November 2024; revised 15 April 2025; accepted 5 May 2025.
Available online 20 August 2025

* Corresponding author.
E-mail addresses: skenawy@ieee.org (E.-S. M. El-Kenawy), mmm@ieee.org (M. M. Eid), ban.s@albayan.edu.iq (B. S. Shukur), aalhussan@pnu.edu.sa (A. A. Alhussan), dskhafga@pnu.edu.sa (D. S. Khafaga).

https://doi.org/10.52866/2788-7421.1301

The quickly expanding IoT environment brings rewarding opportunities and important management obstacles to networks. More advanced data flow management systems have become essential because IoT devices continue expanding into different industries. The network traffic patterns from IoT devices in intelligent cities healthcare facilities, and industrial operations outstrip conventional traffic management solutions because these devices need to maintain seamless communication.

The rapid expansion of IoT networks still leads to many current traffic management systems that inadequately recognize and forecast behavioral patterns of IoT devices during real-time operations. Traditional approaches depend on static rules and easy traffic attributes because they cannot manage IoT devices' diverse behaviors.

The Internet of Things (IoT) has had a considerable influence on the management of network traffic, the security of networks, and the performance of networks in industrial and smart home contexts. Classification issues can affect network efficiency, security, and QoS. This study develops a machine learning-based classification model to assess and categorize IoT traffic metrics for network performance and security.

Numerous research studies examine machine learning models for network traffic analysis, although most of them utilize small data scales or exclude the diverse IoT device assortment. The analysis of IoT traffic complexity across different use cases remains incomplete through research that implements only single algorithm methods. Research examining IoT device performance in real-time with diverse data collection is minimal.

The research develops a novel IoT traffic classifier that utilizes a Decision Tree, Random Forest and Support Vector Machines, K-nearest neighbor, Naive Bayes, and Stochastic Gradient Descent Classifier. The approach creates novelty by implementing its techniques on real-time traffic collected from diverse IoT devices spanning multiple vendors. This model stands apart from previous studies that studied particular IoT devices or restricted datasets because it shows versatility in accurately classifying traffic from other real-world IoT devices, effectively serving diverse IoT networks.

This study preserves IoT network traffic flow control and security on the environment through a machine learning tool. Six machine learning algorithms are compared to find the best one for IoT traffic classification. The research assesses real IoT devices traffic and provides helpful recommendations for network security, illegitimate device identification, and superior quality of service in IoT systems. The results offer significant insights into the actual application of machine learning in IoT network management.

The core goal of this study involves developing a machine-learning model that precisely categorizes and evaluates IoT network traffic. We use six diverse machine learning algorithms to identify which approach provides the most efficient improvement for IoT network performance and security measures. The proposed model should help develop IoT networks with increased resilience as it handles extensive traffic loads, detects unapproved devices, and delivers optimal QoS. The research results from this study would direct upcoming work in bettering IoT traffic management systems while establishing essential components for adaptive network development.

The paper is organized as follows: The second section mentions the related work, Section 3 presents the materials and methods, The Fourth section discusses the analysis and interpretations of the results; finally, conclusion and future work is in the fifth part.

2. Related work

This part of our paper introduces some studies related to IoT traffic classification problem.

The classification models are characterized by a cost-effective, efficient normal established by Shukla et al. [4] through utilizing integrated feature reduction. They used K-fold cross-validation on four IoT traffic scenarios to assess their models. The outcomes indicated an 84.4% decrease in features and a 5.19% increase in classification accuracy relative to existing methodologies utilizing a publicly accessible Bot-IoT dataset.

The shallow neural network of 110 ReLU-activated neurons by Ehmer et al. [5] was able to identify representative communication network threats. They presented an enhanced attack-sharing loss function to address unbalanced learning. The solution can identify network assaults with an F1 score over 99%, concentrating on IoT device connectivity. It decreases false negative detection rates, enhancing network security and line rate processing in low-complexity systems.

Luo et al. [6] utilized in three separate classification tasks, provides simplified yet representative samples, improving the baseline performance by at least 6.02% and up to 182.66%. It significantly decreases resource utilization with sample quantities reduced to a ratio of no less than 83.53%. They established a basis, illustrating the effectiveness of HSS in enhancing security protocols in IoT networks, possibly informing the creation of more proficient and resource-efficient solutions.

Table 1. Summary of some related study.

Ref.	Method	Outcome	Objective	year of Publication
Shukla et al. [4]	Integrated feature reduction using K-fold cross-validation on four IoT traffic scenarios, Bot-IoT dataset	84.4% decrease in features, 5.19% increase in classification accuracy	To develop EIoT-DDoS, an embedded classification approach for detecting and classifying DDoS attacks in IoT traffic using lightweight and efficient models.	May 2023
Ehmer et al. [5]	Shallow neural network with 110 ReLU-activated neurons, enhanced attack-sharing loss function	F1 score over 99%, reduced false negative detection rates	To implement a shallow neural network to classify and differentiate various network attacks in both Internet and IoT traffic environments.	Aug 2024
Luo et al. [6]	Simplified representative samples in three classification tasks, HSS to enhance security protocols	Improved baseline performance by 6.02% to 182.66%, reduced resource utilization by 83.53%	To enhance malicious IoT traffic classification using a hybrid sampling strategy (HSS) to balance datasets and improve classification accuracy.	Nov 2024
Chowdhury et al. [7]	Device fingerprinting (DFP) using Random Forest on UNSW dataset, supervised machine learning	99.81% accuracy on UNSW dataset, 99.50% for IoT device identification	To identify Smart Home IoT (SH-IoT) devices through analysis of network traffic characteristics using a Random Forest classifier.	Aug 2023
Wang et al. [8]	Hybrid deep learning model with GDC and CA-LSTM, ISCX VPN-nonVPN public dataset	Accuracy above 95%, recall beyond 90%	To propose a network traffic classification model that utilizes spatio-temporal feature extraction to improve accuracy in dynamic IoT environments.	Mar 2024
Abbas S. et al. [9]	Deep learning models (RNN) on CICDIoT2023 dataset for cyberattack detection	RNN achieved 96.56% accuracy	To evaluate the performance of multiple deep learning models for detecting cyber-attacks and performing multi-class classification in IoT networks.	Aug 2023
Shukla et al. [10]	Distributed detection methodology using DDoS attack approach, Apache Storm and Hadoop	Over 99% accuracy for DDoS detection in real-time	To introduce SDDA-IoT, a storm-based distributed detection approach for identifying DDoS attacks in IoT network traffic.	Feb 2024
Yaras and Dener [11]	Hybrid deep learning method using PySpark and Apache Spark, CICIoT2023 and TON_IoT datasets	99.995% accuracy for binary classification, 99.96% for multiclass classification	To provide a comprehensive review and comparative analysis of various machine learning algorithms for classification and prediction tasks.	Jan 2020

Chowdhury et al. introduced the study [7], which illustrated a device fingerprinting (DFP) methodology grounded in network traffic characteristics. The system employs a supervised machine learning Random Forest classifier to categorize device kinds with an accuracy of 99.81% on the UNSW dataset. It attained an accuracy of 99.50% for IoT devices and 97.10% for non-IoT device identification. Although utilizing fewer characteristics and packets, the DFP technique exhibited enhanced performance, positioning it as a viable tool for bolstering network security in diverse contexts.

Wang et al. [8] created a hybrid deep learning model for multi-classification tasks, integrating dilated convolution and gating unit techniques. The model employs a Gated Dilated Convolution (GDC) module for spatial feature extraction and a CA-LSTM module for temporal network traffic feature extraction. The model guarantees diversity in feature extraction, resilience, and improved performance rate. The model surpassed current methodologies, achieving an accuracy rate above 95% and a recall rate beyond 90%, utilizing the ISCX VPN-nonVPN public dataset.

Abbas S. et al. [9] employed several deep learning models to identify and mitigate cyberattacks threatening the network environment across many data stream traffics. The CICDIoT2023 dataset was utilized to evaluate the effectiveness of the strategy. The RNN model attained a peak accuracy of 96.56%, demonstrating its efficacy in detecting assaults inside the IoT ecosystem.

The study developed a distributed detection methodology by Shukla et al. [10] for the attack that use DDoS approach on IoT network traffic with Apache Storm. The methodology has two components: model creation and deployment. The building of models includes the creation of five models utilizing a Hadoop cluster. The model deployment utilizes the Apache Storm stream processing framework to

Table 2. Statistical analysis of IoT devices traffic.

F/M	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*
Mean	0.39	0.68	0.59	0.38	0.35	0.38	0.37	0.07	0.16	0.74	0.46
Median	0.50	0.85	0.75	0.11	0.06	0.13	0.26	0.02	0.03	0.86	0.39
S. D	0.39	0.28	0.25	0.34	0.36	0.34	0.20	0.18	0.30	0.28	0.18

evaluate incoming streaming data and categorize it into seven types in real-time. The SDDA-IoT methodology identifies attacks that use DDoS with enhanced speed and precision, achieving over 99% accuracy.

PySpark and Apache Spark with Colab platform employed by Yaras and Dener [11] to create a hybrid deep learning method for binary and multiclass classification. The 'CICIoT2023' and 'TON_IoT' datasets were utilized, with feature reduction conducted via the correlation approach. The model's performance was assessed using accuracy, precision, recall, and F1 metrics. The model attained an accuracy rating of 99.995% for binary classification and 99.96% for multiclass classification in the 'CICIoT2023' dataset.

Table 1 displays a summary of some related studies.

3. Materials and methods

3.1. Dataset

This study makes use of a dataset consisting of network trace traffic records from 40 Internet of Things devices, which together form a network of devices that generate traffic flows. Each communication flow comprises distinct packets, encompassing interarrival time, IP address, transport protocol, port, Time to Live value, window size, and source and destination Ethernet addresses. Studying these distributions can help pinpoint the most crucial elements for classification. This paper examined three statistical properties of each feature's distribution: mean, median, and standard deviation. Table 2 outlines the statistical properties of each attribute.

3.1.1. Data preprocessing

A structured processing pipeline converted raw network traffic data to make it fit for analysis while optimizing data quality through such measures before machine learning algorithms were applied. Data preprocessing ensures the reduction of noise, inconsistency management, and the conversion of diverse IoT traffic for reliable learning model processing. The preprocessing phase protected essential behavioral patterns by minimizing computational errors, although it accommodated diverse IoT device communication formats. The pipeline executed several main stages during its operation.

The data cleaning process excluded packets with header field failures and redundant records. The process also removed any packets with corrupted payloads. The checksum validation method removed incomplete packets stemming from communication transmission failures.

A feature engineering process calculated statistical values, including standard deviation and median, along with mean value for inter-arrival time and TTL and window size fields and packet size metrics among each network flow. The statistical data gathering demonstrates the standard operational behavior patterns of IoT devices.

One-hot encoding techniques transformed IP addresses, port numbers, and protocol types into numerical values for data processing. The continuous features received Min-Max normalization, transforming them into the 0 to 1 value range to manage feature magnitude distortions.

The dataset split happened by dividing information into a training segment (70%) and a testing portion (30%), which maintained class proportions through stratified sampling methods.

3.2. ML classification models

ML, as a subfield of artificial intelligence and data science [11, 12], uses statistical methodologies and principles to derive patterns and conclusions based on the behavior of the given data. It plays a crucial role in the development and acquisition of knowledge by intelligent agents through their experiences. This paper used different supervised ML techniques for classifying the identification of IoT devices.

3.2.1. SVM

SVM is a classifier technique aims to identify the most suitable hyper-plane that effectively separates distinct classes within the input data. The utilization of support vectors enables the maximization of the margin between the two nearest data points belonging to distinct classes. SVM have the ability to effectively handle data that is not linearly separable. This is achieved by employing a kernel function to translate the data into a higher-dimensional space. By doing so, SVMs are able to identify the ideal hyperplane in this converted space by a combination of the kernel functions evaluated at different support as in

Eqs. (1) and (2) [13].

$$f(x) = \sum_{i \epsilon A} \alpha_i y_i k(x, x_i) \quad (1)$$

Let A represent the collection of active constraints and α_i signify the solutions of the quadratic algorithm described below:

$$min_{w,b,\xi} \frac{1}{2}||w||^2 + C\sum_{i=1}^{n} \xi_i$$

$$\text{subject to } y_i\left(W.X_i + b\right) \geq 1 - \xi_i \; \xi_i \geq 0 \quad (2)$$

The matrix G is a $n \times n$ matrix with elements $G_{ij} = (x_i, x_j)$. The bias 'α' is the value of the Lagrange multiplication coefficient associated with the equality constraint at the optimal solution.

3.2.2. DT

The DT algorithm is a ML technique that constructs a hierarchical model, like a tree structure, to represent decisions and their corresponding outcomes. The purpose of this technique is to address classification challenges by categorizing input data into several classes using rules derived from training data. DT repeatedly divides the data into subsets using features that effectively tell the difference between classes, until a set stopping condition is met [14].

$$I_G(f) = \sum_{i=1}^{m} f_i(1 - f_i) = \sum_{i=1}^{m} (f_i - f_i^2)$$
$$= \sum_{i=1}^{m} f_i - \sum_{i=1}^{m} f_i^2 = 1 - \sum_{i=1}^{m} f_i^2 v \quad (3)$$

3.2.3. RF model

The RF technique is a form of supervised learning that utilizes combined learning algorithms. The suggested method combines "bagging" and DT induction to make a strong classifier that uses the power of many weak classifiers working together. The technique involves the aggregation of many DT to create patterns that enhance overall performance. The stochastic construction approach guarantees a minimal level of correlation among the trees [15]. RF is renowned in the field for its exceptional precision and remarkable capability to handle datasets that include a limited number of observations yet contain numerous features. Consider a set of tree predictors, denoted as $\hat{h}_{RF}(x_1, \theta_1)$, …, $\hat{h}_{RF}(x_1, \theta_q)$, where $\theta_1, \ldots, \theta_q$ are q independent and identically distributed random variables, unrelated to L_n.The RF predictor $\hat{h}_{RF}$ is derived by combining a set of random trees in the following manner:

$$\hat{h}_{RF}(x) = \frac{1}{q}\sum_{l=1}^{q} \hat{h}(x_1, \theta_l)$$

$$\hat{h}_{RF}(x) = argmax \sum_{l=1}^{q} \Pi_{\hat{h}(x_1,\theta_l)} = k \; avec \; 1 \leq k \leq K \quad (4)$$

3.2.4. K-nearest neighbor

The KNN algorithm is a widely employed supervised learning technique in the field of agriculture, utilized for both regression and classification tasks. The system utilizes datasets that have been trained based on their respective classes and relies on a distance computation algorithm to determine the similarity between observations. Various distance calculation methods are utilized in academic research, such as Minkowski distance, Manhattan distance, Euclidean distance, and Hamming distance are often used metrics in several fields of study. These distance measures play a crucial role in quantifying the dissimilarity or similarity between objects or data points in a given dataset. The selection of a distance approach is contingent upon nature of the dataset and maximum value of K for predictive purposes. The effectiveness of KNN in the classification of various cereal cultivars has been demonstrated [16]. Several distance metrics are employed during the comparison phase of the KNN algorithm, including:

1) The Euclidean distance metric has been employed in many identification systems that utilize the K-nearest neighbors (KNN) algorithm [16]. The Euclidean distance $d_E(X, Y)$ between the two vectors X and Y is defined as follows:

$$d(X, Y) = \sqrt{\sum_{i=1}^{n} (x_i - y_i)^2} \quad (5)$$

Where:
d(X,Y) is the Euclidean distance between samples X and Y, X_i,Y_i are the i^{th} features, and n is the total number of features

2) The approximate distance from a city block, which is defined by the following formula:

$$d_E(X, Y) = \sum_{i=1}^{m} |x_i - y_i| \quad (6)$$

3) The cosine distance, often known as the angular distance, is a metric based on the similarity of

cosine. It quantifies the angle between two vectors as follows:

$$d_{cos}(X,Y) = 1 - \frac{\sum_{i=1}^{m} X_i Y_i}{\sqrt{\sum_{i=1}^{m} X_i^2}} \frac{1}{\sqrt{\sum_{i=1}^{m} Y_i^2}} \quad (7)$$

4) The correlation's distance is calculated by the following formula:

$$d_{cor}(X,Y) = 1 - \frac{\sum_{i=1}^{m}(x_i - y_i)}{\sqrt{\sum_{i=1}^{m}(x_i - y_i)^2}} \frac{(x_i - y_i)}{\sqrt{\sum_{i=1}^{m}(x_i - y_i)^2}} \quad (8)$$

3.2.5. NB model

The NB classification algorithm is an approach for supervised ML that depends on the principles of Bayes' hypothesis, and it is particularly advantageous for the task of text classification. The aforementioned statement delineates the establishment of guidelines for categorizing observations derived from a given dataset and thereafter employing such guidelines to make predictions based on the data. The primary purpose of this function is to establish a robust priori hypothesis regarding the independence of attributes, disregarding any correlations [16]. Non-blocking algorithms are extensively utilized in various applications such as the topics of interest include spam detection filtration systems, systems for recommendations, and marketing via the internet.

$$p(C|F_1, \ldots, F_n|)$$

The class variable C is dependent and is associated with a limited number of instances or classes. Its association is determined by several characteristic variables $F_1, \ldots,$ F_n. Applying Bayes' theorem, we express the equation as:

$$p(C|F_1, \ldots, F_n|) = \frac{p(c)\,\Pi_{i=1}^{n} p(, F_i|C)}{p(F_1, \ldots, F_n)} \quad (9)$$

3.2.6. SGDC model

Stochastic Gradient Descent Classifiers (SGDC) Supervised Gradient Descent with Coordinate-Wide Minimization is a ML method that uses gradient descent to update the model parameters over and over again until the objective function is minimized. An objective function is characterized as the summation of differentiable functions computed on datasets that are randomly picked. A lot of different ML models, like SVM, logistic regression, and graphical models, are trained with this method. The SGD algorithm approximates the real gradient of (w) by using the gradient of a single part of the total.

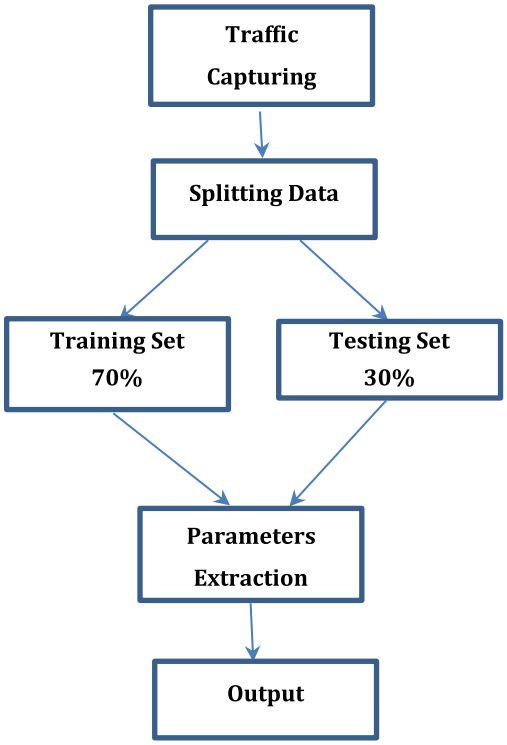

Fig. 1. The proposed model's framework.

$$Q(w) = \frac{1}{n}\sum_{i=1}^{n} Q_i(w) \quad (10)$$

The SGD method can be represented in pseudo-code.

1. Select an initial parameter vector w and a learning rate η.
2. Iterate until an approximate minimum is achieved: Perform a random permutation of the data in the training set, and for each value of i from 1 to n, inclusive, do:

$$w^{(t+1)} = w^{(t)} - \eta \nabla l\left(w^{(t)}, x_i, y_i\right) \quad (11)$$

3.3. The proposed model

The proposed model is designed to find the IoT objects in its surroundings. The first phase of this procedure entails the acquisition of network traffic data, while the subsequent phases encompass the progress of classification and prediction algorithm models. The identification module utilizes network traffic flows as input by mirrored traffic through a capturing tool in order to identify packet nodes, as illustrated in Figs. 1 and 2. The framework acquires network packet statistics through the inception of the device under

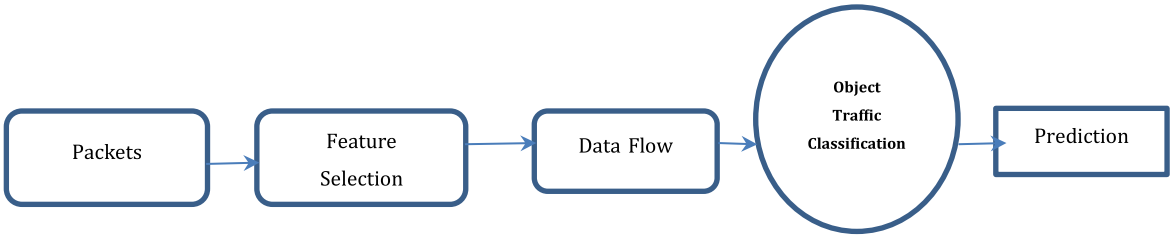

Fig. 2. Pipeline of proposed model.

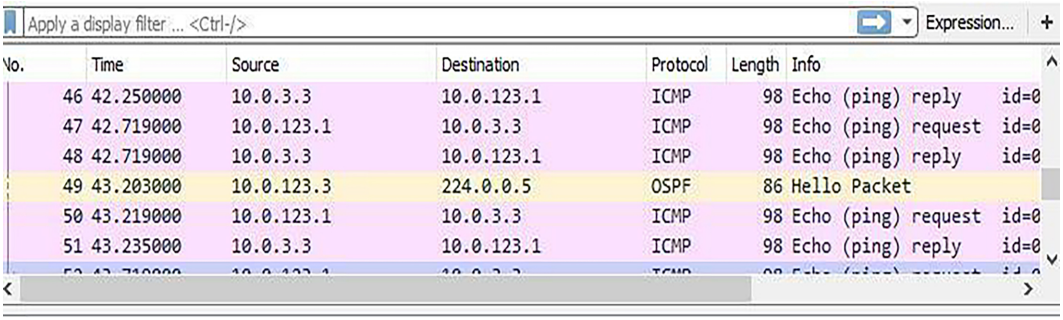

Fig. 3. Process of capturing network traffic using Wireshark.

consideration. Subsequently, by harnessing the traffic generated by the IoT, a computational procedure is executed to extract the parameters that delineate the distinct classes. The third step is the classification of all the captured parameters to ascertain the authenticity of the item being examined. The task can be accomplished by utilizing one or more classifiers, such as SVM, KNN, RF, and DT. The present classification strategy takes into account the models belonging to different classes that have undergone prior training within a designated period known as the learning phase.

The information in the packet header and payload of Transmission Control Protocol (TCP) packets contains traffic flow characteristics like throughput, length, and idle time. It aims to uncover disparities that reflect unique patterns. Network traffic is captured using Wireshark on the host system as seen in Fig. 3.

That host serves as a gateway node for network traffic. In which, human observations and a series of network traffic captures, involving the monitoring of incoming and outgoing data inside the local network, were performed using several iterations on Windows 10. When IoT device doesn't interact with any outside entities, the amount of packet volume it sends and receives usually changes. The lack of network activity pertaining to the temperature sensor is particularly evident. Nevertheless, while engaging with these stated sensors, the level of network activity increased.

The data collection process involves converting traces into ML algorithms-usable formats using a Python script to extract network flow characteristics from the transmission of data packets between computer addresses through specific protocols such as (TCP, UDP, ARP. . .etc).

IoT devices engage in regular data exchange with servers, commonly distinguished by their respective domain addresses. Periodic exchanges might take place, for instance, through the utilization of Network Time Protocol (NTP) for time stamping or Domain Name System (DNS) requests. According to the second source, many IoT devices exhibit a distinct pattern in specific Transmission Control Protocol/Internet Protocol (TCP/IP) protocols.

4. Results and discussion

The analysis section compares six machine learning classifiers for IoT traffic flow classification by evaluating Decision Tree (DT), Random Forest (RF), K-Nearest Neighbors (KNN) and Naive Bayes (NB), Support Vector Machine (SVM) and Stochastic Gradient Descent Classifier (SGDC). The assessment of each model included six performance metrics, which included Accuracy together with Sensitivity (True Positive Rate), Specificity (True Negative Rate), Positive Predictive Value (PPV) and Negative Predictive Value (NPV), as well as F1-Score. The metrics provide an extended representation of assessment metrics,

Table 3. Comparative performance of machine learning models on IoT traffic classification.

Models	Accuracy	Sensitivity (TRP)	Specificity (TNP)	Pvalue PPV	Pvalue NPV	FScore
RF	0.998098136	0.99707887	0.998751561	0.998050682	0.998128509	0.99756454
DT	0.998961297	0.99707887	0.999529633	0.998439938	0.999118425	0.99775894
NB	0.913443831	0.881239243	0.95049505	0.953445065	0.87431694	0.915921288
SGDC	0.804757185	0.761904762	0.890207715	0.932604736	0.652173913	0.838656839
SVM	0.886505809	0.83797054	0.94488189	0.948148148	0.829015544	0.889661164
KNN	0.963809524	0.949907236	0.978473581	0.978967495	0.948766603	0.964218456

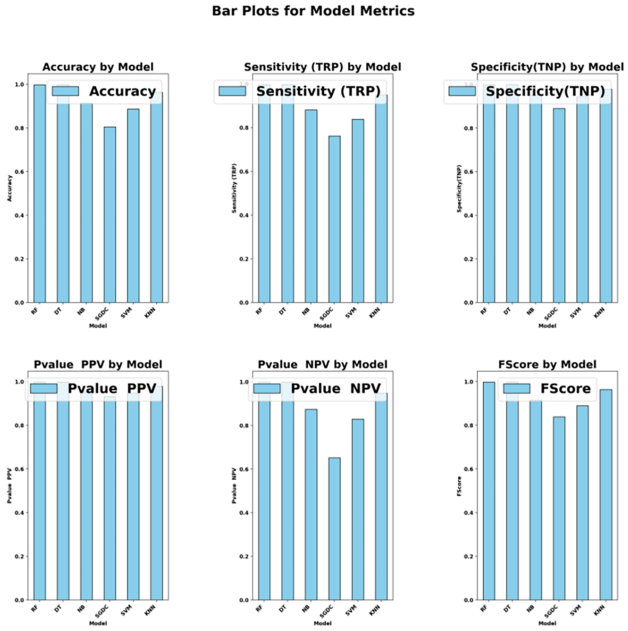

Fig. 4. Bar plots for model metrics.

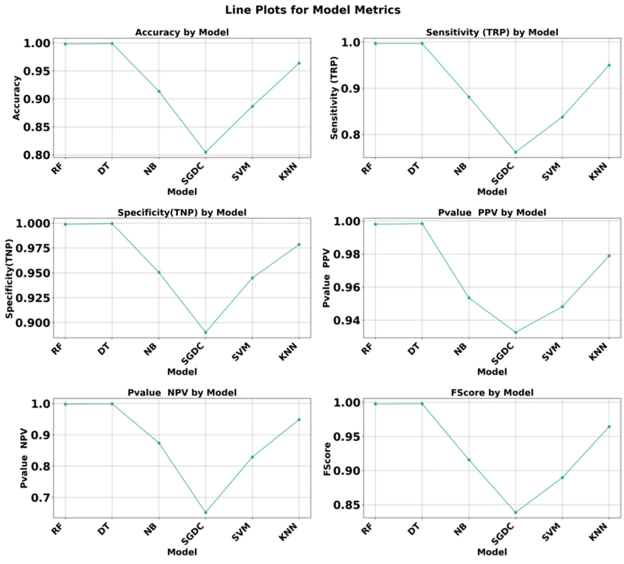

Fig. 5. Line plots for model metrics.

specifically evaluating classifier reliability under IoT conditions where data becomes unbalanced and contains noise.

The Table 3 shows that tree-based models, including DT and RF, deliver superior performance on all evaluation measures. The Decision Tree model delivered peak performance by establishing almost perfect classification results with 99.90% accuracy and an F1-score of 99.78% due to its strong capability to retrieve complex decision boundaries in IoT traffic behavior.

Bar and Line Plots (Figs. 4 and 5) show that DT and RF consistently rank highest across all metrics, with a notable drop-off observed for SGDC and SVM.

A Correlation Heatmap (Fig. 6) indicates strong positive correlations among most evaluation metrics, especially between Accuracy, Sensitivity, and F1-Score. These correlations validate internal consistency in model performance.

A Q-Q plot of Accuracy (Fig. 7) and a regression plot between Accuracy and F1-Score (Fig. 8) indicate a strong linear relationship, suggesting high internal consistency across evaluation criteria.

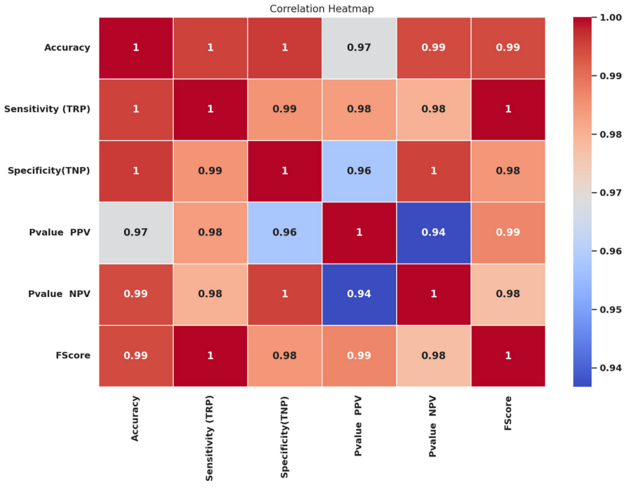

Fig. 6. Correlation heatmap of evaluation metrics.

A **Metric Comparison Heatmap** (Fig. 9) provides a consolidated view of each model's standing across all criteria, visually reinforcing the superiority of DT and RF.

Both DT and RF achieve excellent results because of their ability to track feature relevancy with their categorical and numerical attribute processing and

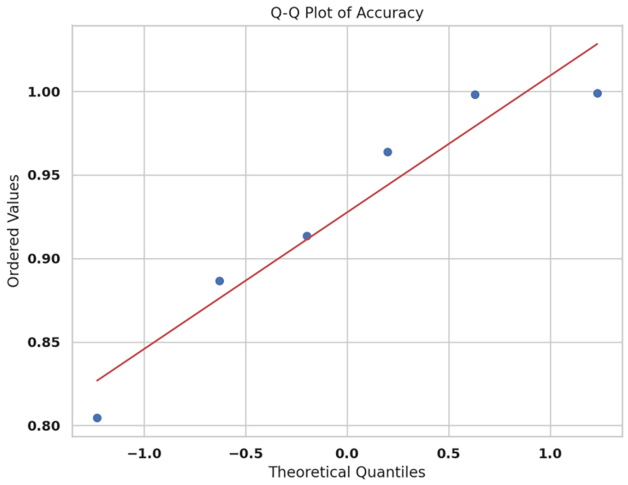

Fig. 7. Q-Q plot of accuracy values across models.

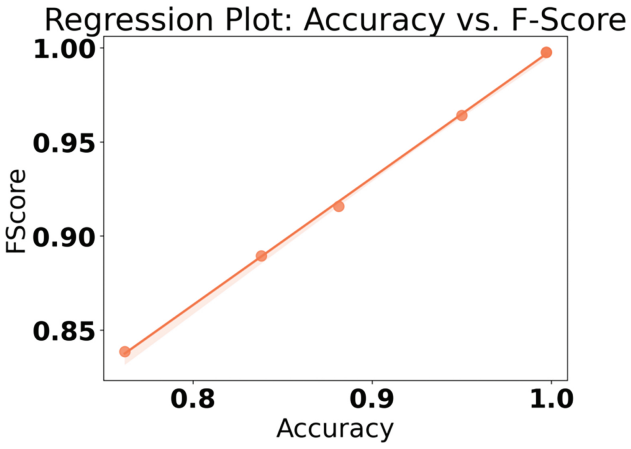

Fig. 8. Regression plot: Accuracy vs. F1-score.

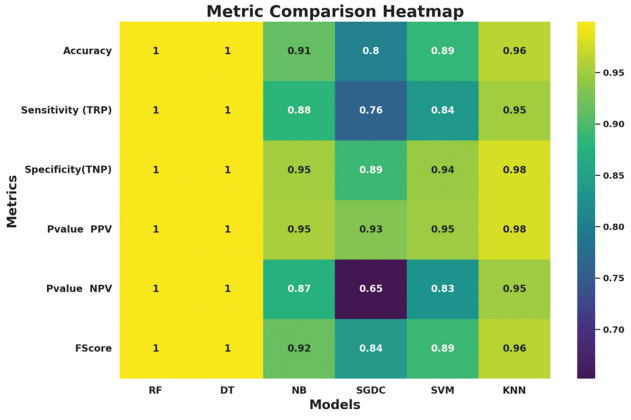

Fig. 9. Metric comparison heatmap across all models.

improved stability from RF ensemble learning. KNN reached strong performance levels with Sensitivity at 94.99% and Specificity at 97.85%, thus making it suitable for implementations requiring straightforward computation. The linear decision boundaries used by SGDC produced its worst performance rate due to the inability of this method to handle complex IoT traffic patterns.

Research data analysis indicates Decision Tree-based approaches deliver optimal results in running IoT traffic analytics because they achieve high accuracy alongside strong interpretation ability and low CPU requirements. Future researchers can improve model enhancement by combining ensemble methods with deep learning technologies and implementing a domain-specific feature selection approach.

5. Conclusion and future work

A machine learning-based IoT device traffic classification system was introduced to help smart environment security and network management. Six supervised learning models, namely Decision Tree (DT), Random Forest (RF), K-Nearest Neighbor (KNN), Support Vector Machine (SVM), Naive Bayes (NB) along with Stochastic Gradient Descent Classifier (SGDC), were implemented to evaluate real-time IoT traffic data collected from multiple devices.

The classification metrics for Decision Tree and Random Forest proved most reliable in identifying patterns because they delivered accuracy rates of 99.90% and 99.81%, respectively. The identification of both regular and anomalous device activities by these models proved exceptionally strong through their consistent F1-score and sensitivity and specificity measurements. The results from KNN were promising, but SVM, along with NB and SGDC, presented moderate performance because of their reaction to IoT traffic attributes.

The practical implementation of understandable computational models stands as the main value of this study because it operates on real-world conditions. This adaptable and scalable proposed approach supports real-time traffic classification because such capability detects unauthorized devices while preserving the network's operational integrity.

The authors plan to upgrade this framework by adding deep learning structures and combined optimization features for selecting attributes. Broader device inclusion in combination with diverse network situations must be added to the dataset to strengthen the proposed system's validation process.

The research supports IoT traffic intelligence development by establishing lightweight machine learning capabilities that achieve accurate reliability and scalability for application in contemporary connected systems.

Funding statement

No funding.

Conflict of interest

The authors declare that they have no conflicts of interest to report regarding the present study.

Acknowledgment

Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2025R 308), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia.

Author contribution

Conceptualization, S.K Data Collection, BSS Analysis and Interpretation of results, BSS; A.A.A; Manuscript Preparation, M.M.E; and D.S.K project administration, S.K. review & editing M.M.E.

Data availability

The data that support the findings of this study are available on request from the corresponding author.

References

1. IDC research *et al.*, "State of IoT Security Survey 2018," 2018, www.digicert.com/wp-content/uploads/2018/11/StateOfIoTSecurity_Report_11_02_18_F_am.pdf.
2. S. Kejriwal and S. Mahajan, "Smart buildings: How IoT technology aims to add value for real estate companies," *Deloitte Center for Financial Services*, 2016.
3. A. Tewari and B B. Gupta, "Security, privacy and trust of different layers in Internet-of-Things (IoTs) framework," *Future generation computer systems*, vol. 108, pp. 909–920, 2020.
4. P. Shukla *et al.*, "EIoT-DDoS: embedded classification approach for IoT traffic-based DDoS attacks," *Cluster Computing*, May 2023. https://doi.org/10.1007/s10586-023-04027-5.
5. J. Ehmer *et al.*, "Network Attack Classification with a Shallow Neural Network for Internet and Internet of Things (IoT) Traffic," *Electronics*, vol. 13, no. 16, p. 3318, Aug. 2024. https://doi.org/10.3390/electronics13163318.
6. Y. Luo, J. Tao, Y. Zhu *et al.*, "HSS: enhancing IoT malicious traffic classification leveraging hybrid sampling strategy," *Cybersecurity*, vol. 7, no. 11, 2024. https://doi.org/10.1186/s42400-023-00201-9.
7. R. R. Chowdhury, A. C. Idris, and P. E. Abas, "Identifying SH-IoT devices from network traffic characteristics using random forest classifier," *Wireless Netw*, vol. 30, pp. 405–419, 2024. https://doi.org/10.1007/s11276-023-03478-3.
8. C. Wang *et al.*, "Network Traffic Classification Model Based on Spatio-Temporal Feature Extraction," *Electronics*, vol. 13, no. 7, p. 1236, Mar. 2024. https://doi.org/10.3390/electronics13071236.
9. S. Abbas, I. Bouazzi, S. Ojo, A. Al Hejaili, G. A. Sampedro, A. Almadhor, and M. Gregus, "Evaluating deep learning variants for cyber-attacks detection and multi-class classification in IoT networks," *PeerJ Computer Science*, vol. 10, p. e1793, 2024. https://doi.org/10.7717/peerj-cs.1793.
10. P. Shukla, C. R. Krishna, and N. V. Patil, "SDDA-IoT: storm-based distributed detection approach for IoT network traffic-based DDoS attacks," *Cluster Comput*, vol. 27, pp. 6397–6424, 2024. https://doi.org/10.1007/s10586-024-04297-7.
11. B. Mahesh, "Machine learning algorithms -A review," *International Journal of Science and Research (IJSR)*, vol. 9, no. 1, pp. 381–386, 2020. doi: 10.21275/ART20203995.
12. Priyanka and D. Kumar, "Decision tree classifier: a detailed survey," *International Journal of Information and Decision Sciences*, vol. 12, no. 3, pp. 246–269, 2020.
13. A. O. Ok, O. Akar, and O. Gungor, "Evaluation of random forest method for agricultural crop classification," *European Journal of Remote Sensing*, vol. 45, no. 1, pp. 421–432, Jan. 2012. doi: 10.5721/EuJRS20124535.
14. A. K. Mohamed, S., W. Gee, W. Zhang, and M. Adel, "Advancing Parking Space Surveillance using A Neural Network Approach with Feature Extraction and Dipper Throated Optimization Integration," *Journal of Artificial Intelligence and Metaheuristics*, pp. 16–25, 2023. DOI: https://doi.org/10.54216/JAIM.060202.
15. G. Gültekin and O. Bayat, "A Naïve Bayes prediction model on location-based recommendation by integrating multi-dimensional contextual information," *Multimedia Tools and Applications*, vol. 81, no. 5, pp. 6957–6978, Feb. 2022. doi: 10.1007/s11042-021-11676-4.
16. M., E. H., F. Mohamed, A. Elshabrawy, M. Ibrahim, A. A., A. Khodadadi, N. M., E. M., and M., "Football Optimization Algorithm (FbOA): A Novel Metaheuristic Inspired by Team Strategy Dynamics. *Journal of Artificial Intelligence and Metaheuristics*, pp. 21–38, 2024. DOI: https://doi.org/10.54216/JAIM.080103.