Online-Journals.org

iJOE International Journal of Online and Biomedical Engineering

iJOE | eISSN: 2626-8493 | Vol. 21 No. 5 (2025) | OPEN ACCESS

https://doi.org/10.3991/ijoe.v21i05.53485

PAPER

Enhanced Intrusion Detection in IoT Smart Homes: Leveraging Binary and Multi-Class Classification Models

Zulhipni Reno Saputra Elsi[1,2], Deris Stiawan[3](✉), Bhakti Yudho Suprapto[2], M. Agus Syamsul Arifin[4], Mohd. Yazid Idris[5], Rahmat Budiarto[6]

[1]Faculty of Engineering, Universitas Muhammadiyah Palembang, Palembang, Indonesia

[2]Faculty of Engineering, Universitas Sriwijaya, Palembang, Indonesia

[3]Faculty of Computer Science, Universitas Sriwijaya, Palembang, Indonesia

[4]Departenment of Computer Science, Universitas Bina Insan, Lubuklinggau, Indonesia

[5]Faculty of Computing, Universiti Teknologi Malaysia, Johor Bahru, Malaysia

[6]College of Computing and Information, AlBaha University, Albaha, Saudi Arabia

deris@unsri.ac.id

ABSTRACT

This study uses the MQTT-IoT-IDS2020 dataset, which contains normal traffic and attack traffic such as scan_A, scan_sU, Sparta, and mqtt_bruteforce attacks. This dataset is statistically extracted based on the unidirectional-based features packet header flow feature and has 19 features. This study used 10 best algorithms, namely ADABOST, eXtreme gradient boosting classifier (XGBC), stochastic gradient descent classifier (SGDC), random forest (RF), Naïve Bayes (NB), multi-layer perceptron classifier (MLPC), decision tree (DT), logistic regression (LR), linear discriminant analysis (LDA), and K-Nearest Neighbor (KNN) using binary class and multi-class. Using this classification algorithm, researchers measure the value of accuracy, precision, recall, F1 score, classification time, and receiver operating characteristic (ROC) curve to obtain the best classification algorithm. Measurement of accuracy value is done by dividing the dataset into 80:20 for training data and testing data, then validating the measurement of accuracy value with k-fold.

KEYWORDS

binary classification, multi-class classification, unidirectional features, intrusion detection system, Internet of Things (IoT) security

1 INTRODUCTION

The Internet of Things (IoT) is an evolving technological paradigm that integrates billions of smart objects [1], [2], enabling smart ecosystems such as smart factories [3], smart healthcare [4], smart transportation [5], smart cities [6], and smart homes [7]. IoT is becoming an integral part of computing and networking paradigms, facilitating human-to-human interconnection and intercommunication on the Internet, allowing communication to occur anytime, anywhere, and across various devices [8].

The advancement of IoT networks has created new opportunities to enhance comfort and efficiency in homes through various smart devices, such as IP cameras [9],

Elsi, Z.R.S., Stiawan, D., Suprapto, B.Y., Arifin, M.A.S., Idris, M.Y., Budiarto, R. (2025). Enhanced Intrusion Detection in IoT Smart Homes: Leveraging Binary and Multi-Class Classification Models. *International Journal of Online and Biomedical Engineering (iJOE)*, 21(5), pp. 63–86. https://doi.org/10.3991/ijoe.v21i05.53485

Article submitted 2024-11-25. Revision uploaded 2025-01-27. Final acceptance 2025-01-29.

smart doors [10], smart lights [11], smart scalars [12], smart wall sockets [13], IR remotes [14], and others. However, IoT-based smart home (ISH) networks are increasingly vulnerable to numerous attacks due to their distributed and heterogeneous nature [15]. These include brute force attacks [16], distributed denial of service (DDoS) attacks [17], and user datagram protocol (UDP) flood attacks [18]. To counter these threats, an intrusion detection system (IDS) is an intelligent mechanism designed to detect and handle network attacks. Many researchers have proposed techniques to enhance the accuracy of IDS in detecting anomalous activities. IDS works by identifying and comparing anomalous patterns with normal patterns in IoT networks [19].

Algorithm-based IDSs can detect malicious activities using classification techniques and statistical features extracted from network protocols [19]. In addition, IDSs can employ metaheuristic algorithms, ranging from simple local search methods to complex learning processes, to analyze and explore network traffic data. This anomaly detection approach improves accuracy while maintaining a high true positive rate and a low false positive rate [20].

Machine learning (ML) has been widely applied in the design of IDS to accurately detect and classify attacks [21], as well as to analyze intrusions targeting electronic devices [22]. ML is a data analysis technique in artificial intelligence, where systems are trained to automate decision-making and pattern recognition with minimal human intervention [23]. ML algorithms can be broadly categorized into supervised, unsupervised, and semi-supervised learning [24]. Researchers have employed ML algorithms for tasks such as feature extraction [25], [26], feature selection [27], classification [28], and clustering [29].

Before implementing ML to analyze IoT attack traffic, a feature extraction process is conducted during the pre-processing stage. The reliability of ML algorithms heavily depends on the data generated by various IoT devices and the features extracted from IoT network traffic [30]. Numerous feature extraction methods can be utilized, including statistical extraction [31], packet extraction [25], principal component analysis (PCA) [32], independent component analysis (ICA) [20], linear discriminant analysis (LDA) [33], and T-Shark analyzer [34].

Feature selection plays a crucial role, particularly when dealing with datasets containing numerous variables and features. It eliminates redundant variables, improving classification accuracy and performance [35]. Although feature selection is less commonly applied in IoT datasets, incorporating it can significantly enhance data analysis [36].

Machine learning algorithms are capable of classifying anomalous events, including various IoT hardware attacks and failures [37]. Algorithms commonly employed include AdaBoost (AB), eXtreme gradient boosting classifier (XGBC), stochastic gradient descent classifier (SGDC), Naive Bayes (NB), LDA, multi-layer perceptron classifier (MLPC), decision tree (DT), logistic regression (LR), K-Nearest Neighbor (KNN), and random forest (RF). Classification tasks are divided into binary-class, which distinguishes between normal and attack traffic, and multi-class, which identifies multiple types of attacks. Through the classification process, metrics such as accuracy, precision, recall, F1 score, classification time, and receiver operating characteristic (ROC) curve are evaluated [38].

The measurement of accuracy often involves splitting the dataset into training and testing data with ratios such as 90:10, 70:30, or 50:50 [39]. To prevent overfitting, k-fold cross-validation is used, where the dataset is divided into k subsets. The model is trained on k-1 subsets and tested on the remaining subset. This process is repeated k times, and the average accuracy is calculated [40], [41].

The main contributions of this study are as follows:

- Utilization of a specialized IoT dataset: This study utilizes the MQTT-IoT-IDS2020 dataset, specifically designed to detect attacks in IoT networks. The dataset

includes various types of attacks, such as Normal, scan_sU, scan_A, sparta, and mqtt_bruteforce, enhancing the relevance of the findings in the IoT context.
- Unidirectional-based feature extraction: The study introduces a method for extracting features based on unidirectional packet headers, resulting in 19 features. This method provides novel insights into network traffic analysis and anomaly detection in IoT networks.
- Comprehensive evaluation of classification algorithms: The performance of 10 leading classification algorithms–AB, XGBC, SGDC, RF, NB, MLPC, DT, LR, LDA, and KNN–is compared in both binary and multi-class scenarios. The evaluation considers metrics such as accuracy, precision, recall, F1 score, classification time, and ROC curve, offering a holistic perspective on their effectiveness.

The structure of this paper is as follows: Section 2 discusses related work, Section 3 introduces the proposed model, Section 4 provides detailed descriptions of the experimental setup, data preprocessing, performance metrics, and results, and Section 5 concludes with suggestions for future research.

2 RELATED WORK

Detection and prevention of cyberattacks remains an important challenge in the cybersecurity domain, especially with the increasing sophistication of these threats. Previous research has explored various methodologies to improve the accuracy and robustness of intrusion detection systems (IDS) as well as other cybersecurity frameworks by utilizing a combination of artificial intelligence, machine learning, and domain-specific techniques. However, increasingly malicious and complex attacks add to the challenge, especially in identifying unknown and disguised malware. Malware authors are now using increasingly sophisticated evasion techniques to hide information and avoid detection by IDSs, exacerbating efforts to ensure effective protection [42].

Khraisat et al. [42] provided a comprehensive taxonomy and review of contemporary IDS, categorizing them into signature-based intrusion detection systems (SIDS) and anomaly-based intrusion detection systems (AIDS). Their work emphasized the need for robust detection mechanisms capable of countering evasion techniques used by attackers. They highlighted the importance of utilizing diverse datasets and identified future research challenges to strengthen IDS effectiveness.

Sarker [43] introduced "CyberLearning," a ML-based approach to cybersecurity modeling. The study presented a binary classification model for anomaly detection and a multi-class model for identifying various types of cyberattacks. Sarker's empirical analysis utilized popular datasets such as UNSW-NB15 and NSL-KDD and demonstrated the effectiveness of multiple machines learning techniques, including RF and artificial neural networks (ANN).

In the context of IoT networks, Dogru and Subasi [44] proposed an intelligent traffic accident detection system using vehicular ad-hoc networks (VANETs). They employed supervised learning algorithms, including RF, support vector machines (SVM), and ANN, to analyze vehicular behavior. Their study demonstrated the superiority of RF in detecting accidents with 91.56% accuracy, outperforming other methods.

Alhafidh et al., [45] addressed prediction accuracy and real-time performance in smart home environments. Their experiments using the MavPad dataset showed that SVMs excelled when analyzing localized sensor data, while RF performed better with distributed sensors across the environment.

The study conducted by O'Connor et al [46] introduced "HomeSnitch," a network-based solution to enhance smart home IoT device transparency and security. By analyzing semantic behavior instead of encrypted payloads, HomeSnitch achieved over 99% accuracy in classifying device behaviors, demonstrating the potential of network-level monitoring in IoT environments.

Buczak and Guven [47] conducted a focused literature survey on ML and data mining methods for intrusion detection. They provided tutorial insights into these methods and discussed the importance of dataset quality in achieving robust cybersecurity analytics.

Sharmila and Nagapadma [48] compared traditional NB algorithms with principal component analysis (PCA-based implementations for IDS. Their experiments with the NSL-KDD dataset indicated improved accuracy with PCA-based models, highlighting the role of dimensionality reduction techniques in enhancing IDS performance.

Liaqat et al. [49] addressed the cybersecurity challenges in the Internet of Medical Things (IoMT) by proposing a hybrid deep learning (DL)-driven framework that integrates convolutional neural networks (CNN) and Cuda deep neural network long short term memory (cuDNNLSTM). Their approach, tested using a state-of-the-art IoMT dataset, demonstrated superior accuracy and efficiency in detecting sophisticated malware attacks. The framework achieved an impressive average accuracy of 99.99%, with a precision of 99.83%, a recall of 99.33%, and an F1 score of 99.33%, highlighting its robust performance in addressing IoMT security threats. Table 1 summarizes the works related to ML-based security models.

Table 1. Summary of ML-based security models for detecting anomaly and IoT attacks

References	Used Techniques	Classification Type	Selection Model
[50]	SVM, Artificial Neural Network (ANN), LR, DT, and RF	Multi-class Classification	Split dataset
[51]	DT, RF, dan NB	Binary Classification and Multi-class Classification	Split dataset
[52]	j48, RF, NB	Multi-class Classification	Split dataset
[53]	DT, NB and ANN	Multi-class Classification	Split dataset
[54]	KNN, DT, SVM, ANN, NB, RF and LR	Binary Classification and Multi-class Classification	Split dataset
[55]	DT	Multi-class Classification	k-Folds
[56]	DT, RF, GBT, SVM, MLP, OneClass SVM	Binary Classification	k-Folds
[57]	LR	Binary Classification	k-Folds
[58]	KNN, XGBoost, and NB	Multi-class Classification	k-Folds

When designing a smart home security system on an IoT network, we utilized a binary classification model to identify anomalies and a multi-class classification model to detect different types of cyber-attacks.

3 METHODOLOGY

This section explains the methods used in data processing and the process to generate an IDS model.

3.1 Raw dataset

The dataset is obtained from the MQTT sensor collection and will be extracted to obtain useful features for intrusion detection. The raw data in the form of files (*. pcap) consists of five files (*.pcap), namely normal, scan_a, scan_su, sparta, and mqtt_brute-force. The characteristics of normal data have 1070577 packets with a data size of 192.5 MB; scan_A data has 113940 packets with a data size of 16.2 MB; scan_sU data has 255058 packets with a size of 41.3 MB; sparta data has 20688940 packets, 3,391.1 MB, and mqtt_bruteforce data has 10049372 packets with a data size of 906.8 MB [59].

3.2 Proposed model

The proposed model is divided into several subtasks as shown in Figure 1.

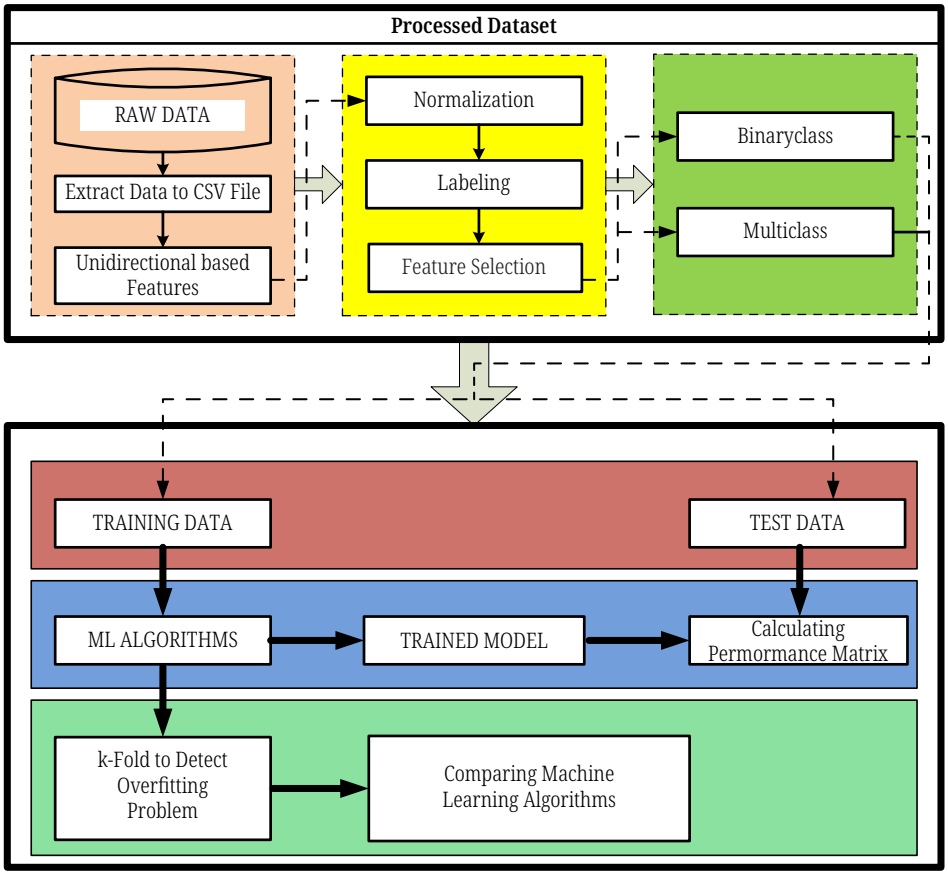

Fig. 1. Proposed process diagram

Figure 1 is a proposed process diagram, containing several steps to be conducted in this study. Firstly, raw data in the form of pcap files will undergo statistical extraction using unidirectional-based features. Secondly, the data, now in CSV format, will be normalized, labeled, and feature selection will be performed. The third dataset was created with binary-class and multi-class classification. The fourth process divided the dataset into training and test data with an 80%:20% composition. The fifth process involves performance measurements, i.e., confusion matrix, accuracy, recall, precision, F1 score, classification time, and ROC curves. Finally, the last step was validation using k-fold to ensure no overfitting occurs.

3.3 Feature extraction

The researchers conducted statistical feature extraction based on packet header flow features, namely unidirectional-based features (UF) [60], [61], and [62]. This dataset extraction resulted in 19 features with different data types, as displayed in Table 2.

Table 2. Feature description of UF

Feature	Data Type	Feature	Data Type
ip_dst	object	mean_pkt_len	float64
ip_src	object	mean_offset	float64
prt_src	int64	num_bytes	int64
prt_dst	int64	num_urg_flags	int64
num_pkts	int64	num_rst_flags	int64
Proto	int64	num_psh_flags	int64
mean_iat	float64	std_pkt_len	float64
std_iat	float64	max_pkt_len	int64
max_iat	float64	min_pkt_len	int64
min_iat	float64	–	–

Out of 19 features, there are two objects, seven floats, and 10 integers. The features ip_src and ip_dst cannot be included in the classification algorithm by the researcher because they are invalid object data types and represent only source and destination IP addresses.

3.4 Classification

The researchers divided the two types of classifications to measure their performance. The first is binary classification, which is divided into two classes: normal class and attack class. The second is multi-class classification, which is divided into several classes, i.e., normal class, brute force class, scan_A class, scan_sU class, and sparta class.

The classification algorithms used are AB, XGBC, SGDC, RF, NB, MLPC, DT, LR, LDA, and KNN. Each of these classification algorithms is evaluated on performance using binary-class and multi-class classification.

4 RESULT AND ANALYSIS

This section examines the performance of the distributed IDS model that was proposed. To conduct the experiments, Python was used, specifically the Scikit-learn library, to implement different ML algorithms. The MQTT-IoT-IDS2020 dataset [62] was utilized to evaluate the model's performance. The experiments took place on a computer with an Intel Core i7-11800H CPU @ 2.30 GHz processor and 16 GB RAM, running the Ubuntu 20.04 operating system.

Researchers assessed the performance of ML classification using 17 features: prt_dst, prt_src, mean_iat, proto, std_iat, num_pkts, min_iat, max_iat, mean_offset, mean_pkt_len, num_bytes, num_psh_flags, std_pkt_len, num_rst_flags, min_pkt_len, and max_pkt_len, num_urg_flags.

We use a confusion matrix to evaluate the performance of the proposed IDS model. Figure 2 explains the results of the confusion matrix with a binary class, and Figure 3 explains the results of the confusion matrix with a multi-class.

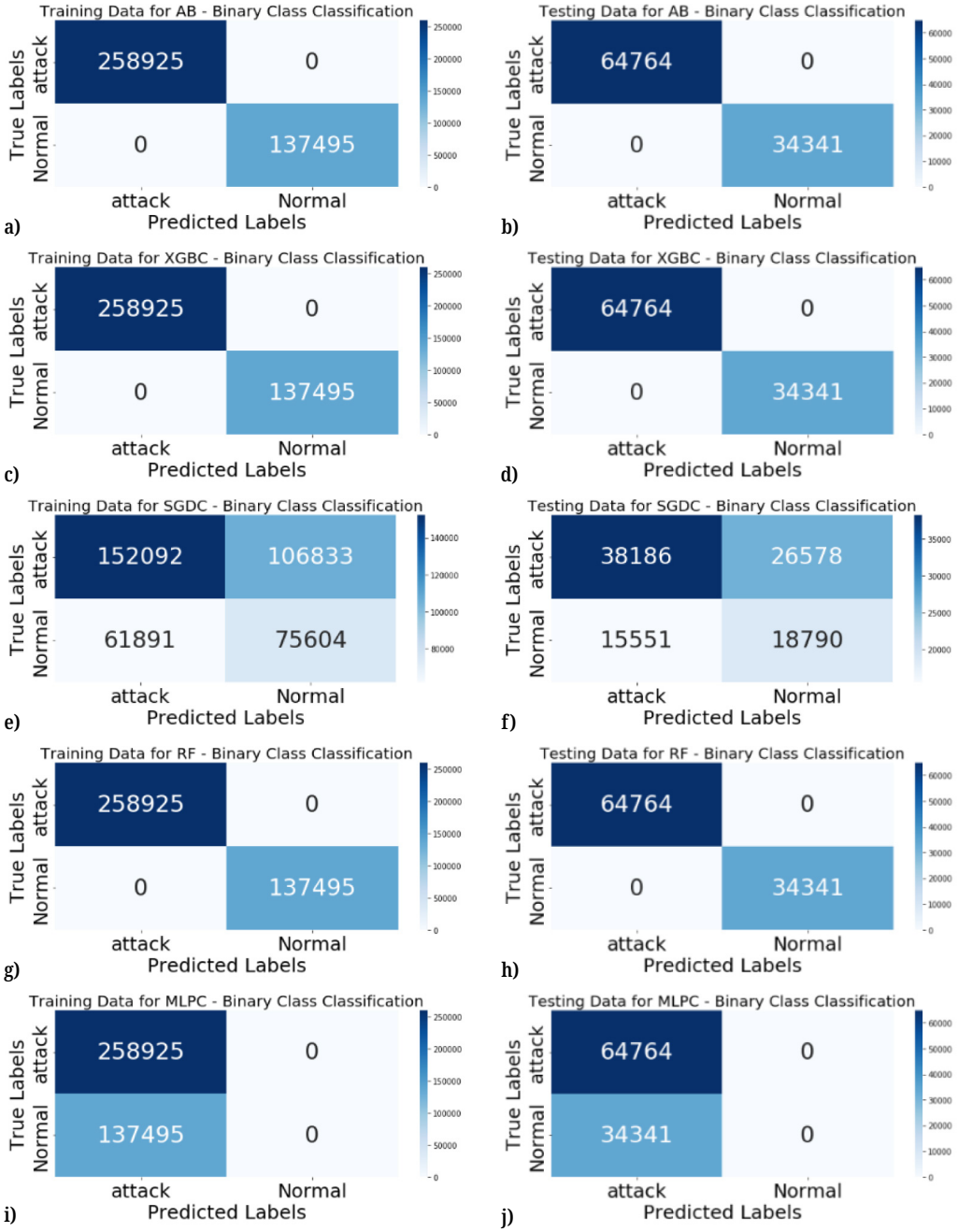

Fig. 2. *(Continued)*

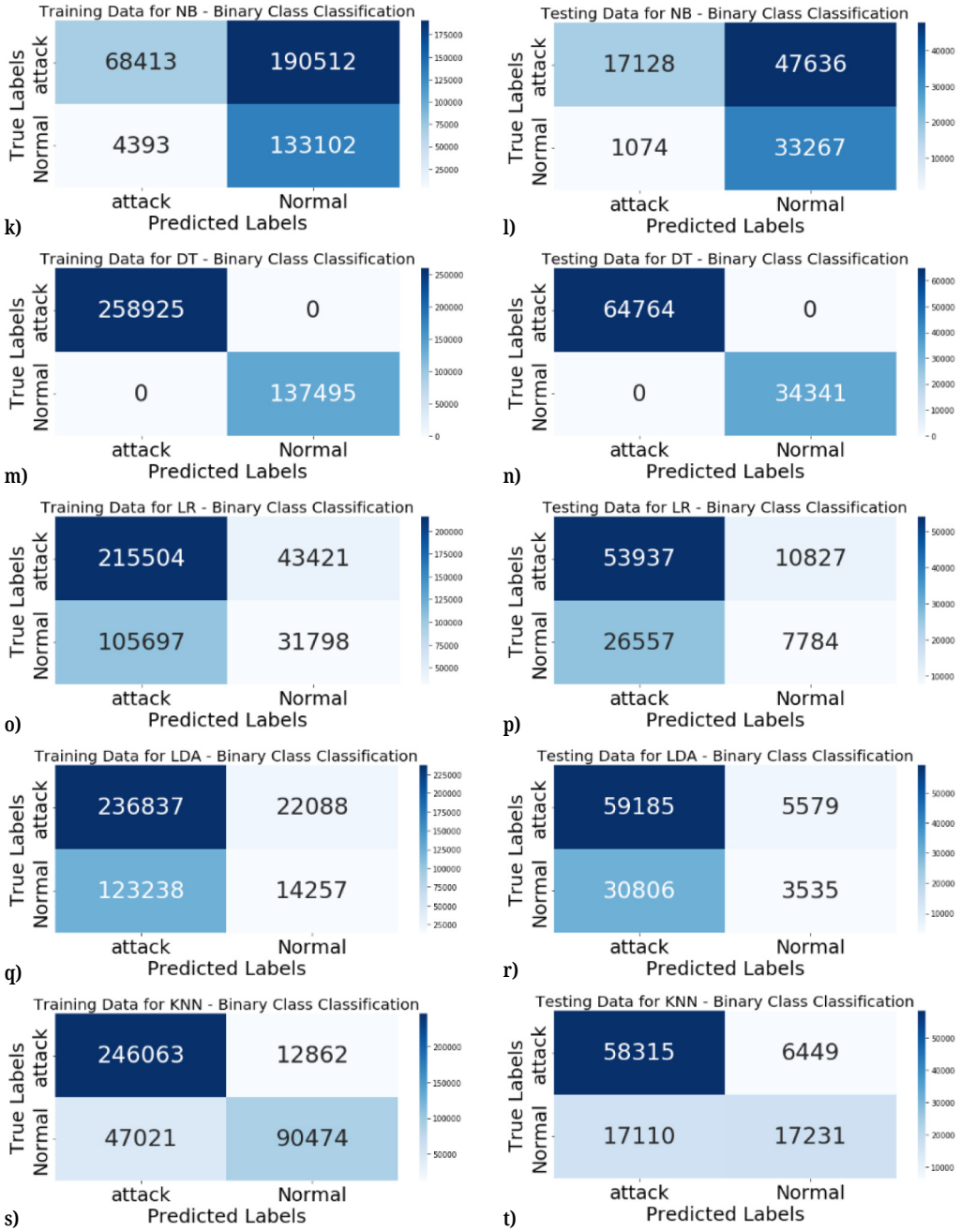

Fig. 2. Confusion matrix for binary classification

In Figure 2, there are 10 binary class matrix confusions, where part a is the matrix confusion of training data AB , part b is matrix confusion of testing data AB, part c is matrix confusion of training data XGBC, part d is matrix confusion of testing data XGBC, part e is matrix confusion of training data SGDC, part f is matrix confusion of testing data SGDC, part g is matrix confusion of training data RF, part h is matrix confusion of testing data RF, part i is matrix confusion of training data MLPC, part j is matrix confusion of testing data MLPC, part k is matrix confusion of training data NB, part l is matrix confusion of testing data NB, part m is matrix confusion of training data DT, part n is matrix confusion of testing data DT, part o is matrix confusion of training data LR, part p is matrix confusion of testing data LR, part q is matrix confusion of training data LDA, part r is matrix confusion of testing data LDA, part s is matrix confusion of training data KNN, part t is matrix confusion of testing data K-Nearest Neighbor.

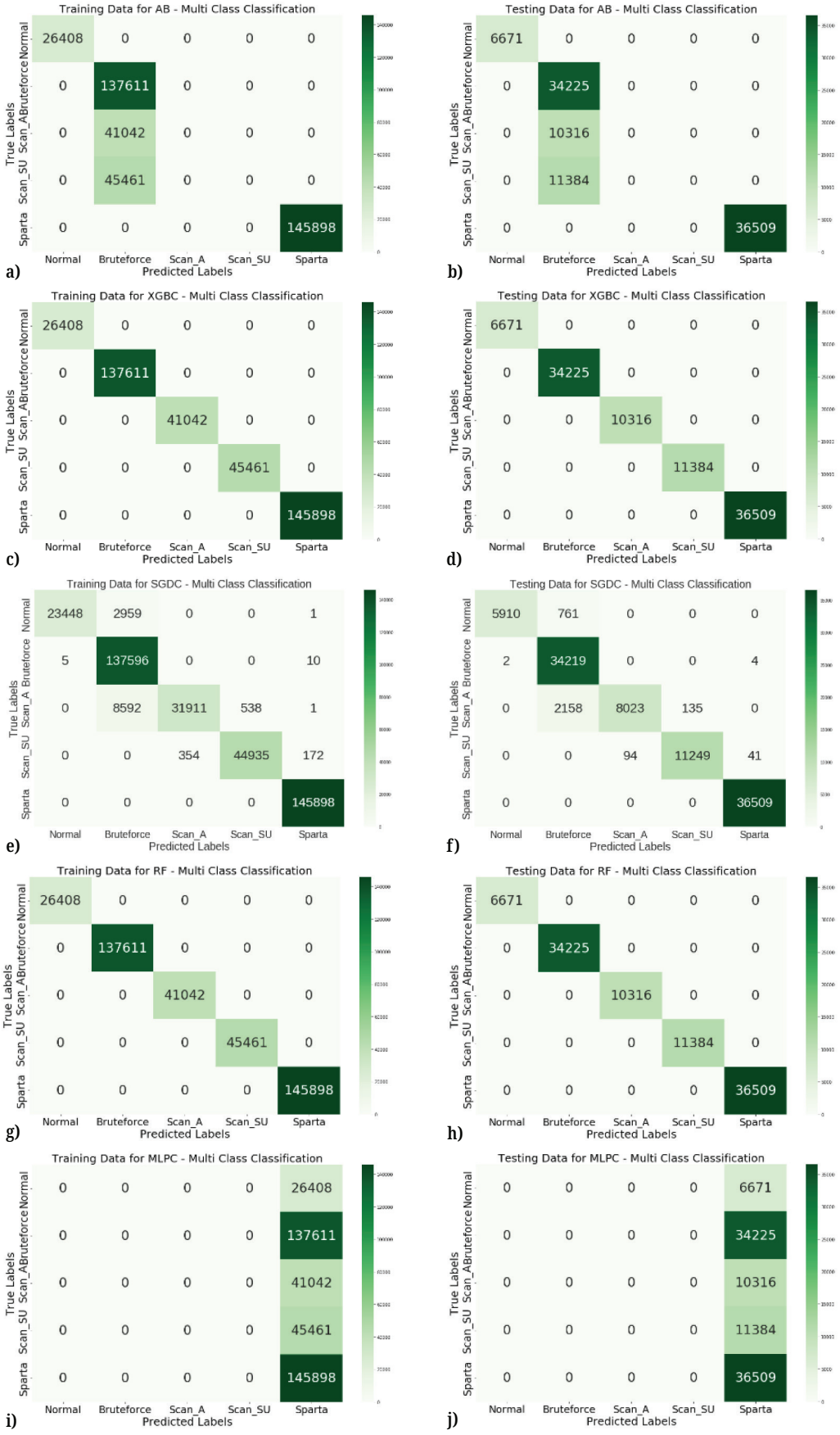

Fig. 3. *(Continued)*

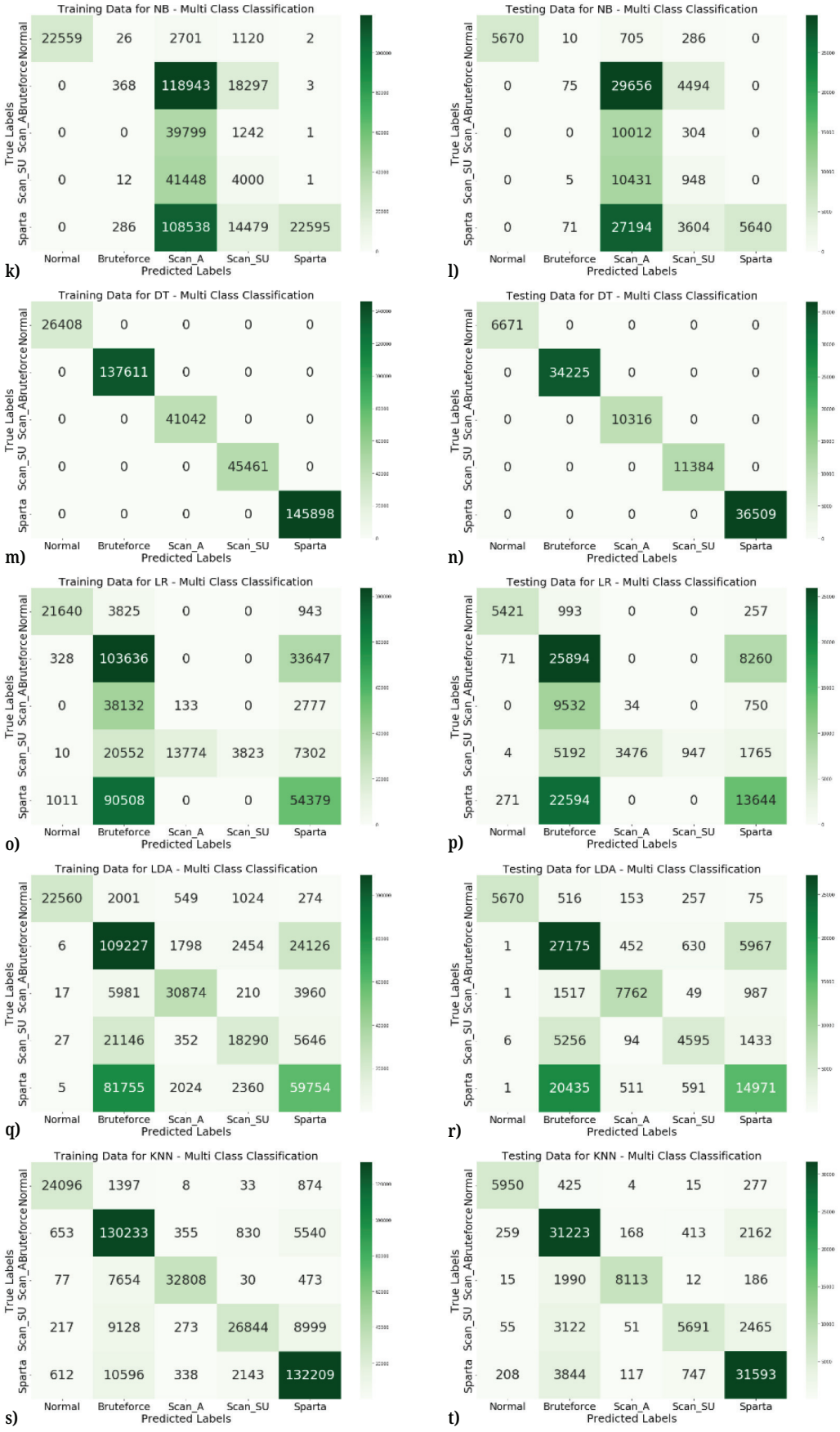

Fig. 3. Confusion multi-class matrix

In Figure 3 there are 10 multi-class matrix confusions, where part a is the matrix confusion of training data AB, part b is matrix confusion of testing data AB, part c is matrix confusion of training data XGBC, part d is matrix confusion of testing data XGBC, part e is matrix confusion of training data SGDC, part f is matrix confusion of testing data SGDC, part g is matrix confusion of training data RF, part h is matrix confusion of testing data RF, part i is matrix confusion of training data MLPC, part j is matrix confusion of testing data MLPC, part k is matrix confusion of training data NB, part l is matrix confusion of testing data NB, part m is matrix confusion of training data DT, part n is matrix confusion of testing data DT, part o is matrix confusion of training data LR, part p is matrix confusion of testing data LR, part q is matrix confusion of training data LDA, part r is matrix confusion of testing data LDA, part s is matrix confusion of training data KNN, part t is matrix confusion of testing data KNN.

According to the confusion matrices in Figure 2 According to the confusion matrices in Figures 2 and 3, the recall, precision, and F1 score values are displayed in Tables 3 and 4, using (1) – (3).

$$\text{Precision} = \frac{TP}{TP + FN} \tag{1}$$

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

$$\text{Recall} = \frac{TP}{TP + FP} \tag{3}$$

Where:

A true positive (TP) is when an accurate prediction correctly identifies an attack on a computer network.

A true negative (TN) is when normal activities are correctly recognized as such.

A false negative (FN) is when attack activities are incorrectly predicted as normal.

A false positive (FP) is when normal activities are incorrectly predicted as attacks.

Table 3. Performance comparison of binary-class classification algorithms

Binary-class Classification	Split Data/Evaluation Metrics					
	Training Data			Testing Data		
	Precision	Recall	F1-Score	Precision	Recall	F1-Score
NB	0.68	0.62	0.49	0.68	0.62	0.50
SGDC	0.58	0.59	0.56	0.58	0.58	0.56
MLPC	0.33	0.50	0.40	0.33	0.50	0.40
LR	0.55	0.53	0.52	0.54	0.53	0.52
LDA	0.53	0.51	0.46	0.52	0.51	0.46
AB	1.00	1.00	1.00	1.00	1.00	1.00
KNN	0.86	0.80	0.82	0.75	0.70	0.71
XGBC	1.00	1.00	1.00	1.00	1.00	1.00
RF	1.00	1.00	1.00	1.00	1.00	1.00
DT	1.00	1.00	1.00	1.00	1.00	1.00

Table 4. Performance comparison of multi-class classification algorithms

Multi-class Classification	Split Data/Evaluation Metrics					
	Training Data			Testing Data		
	Precision	Recall	F1-Score	Precision	Recall	F1-Score
NB	0.55	0.41	0.30	0.54	0.41	0.30
SGDC	0.98	0.94	0.95	0.98	0.94	0.95
MLPC	0.07	0.20	0.11	0.07	0.20	0.11
LR	0.58	0.41	0.40	0.58	0.41	0.40
LDA	0.75	0.64	0.67	0.75	0.64	0.67
AB	0.52	0.60	0.55	0.52	0.60	0.55
KNN	0.90	0.83	0.86	0.87	0.79	0.82
XGBC	1.00	1.00	1.00	1.00	1.00	1.00
RF	1.00	1.00	1.00	1.00	1.00	1.00
DT	1.00	1.00	1.00	1.00	1.00	1.00

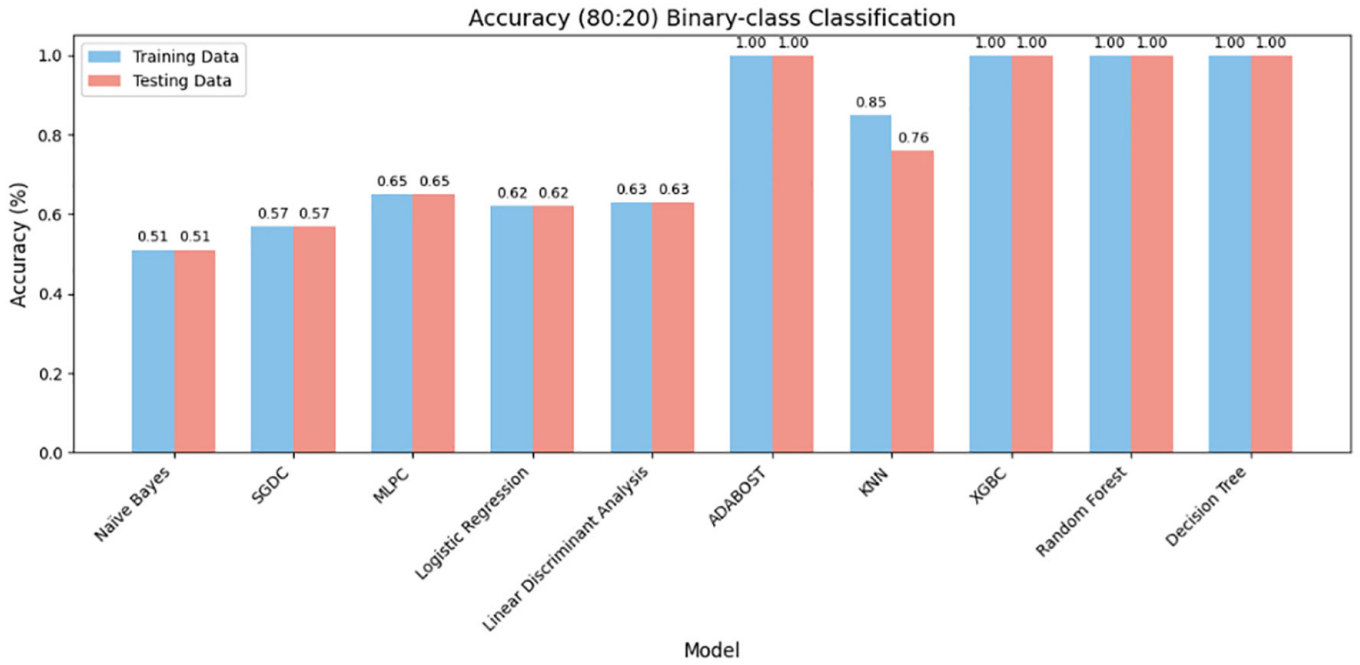

Fig. 4. Binary class accuracy chart with 80:20 split

Figure 4 is a graph of the accuracy value of the binary class algorithm; from this figure, it is clear that the lowest accuracy value is in the NB algorithm, both training data and testing data. And the highest accuracy values for data training and data testing are DT, RF, XGBC, and AB algorithms. From the 10 algorithms, only the KNN algorithm has a different accuracy value between training data and testing data, which are 0.76 and 0.85.

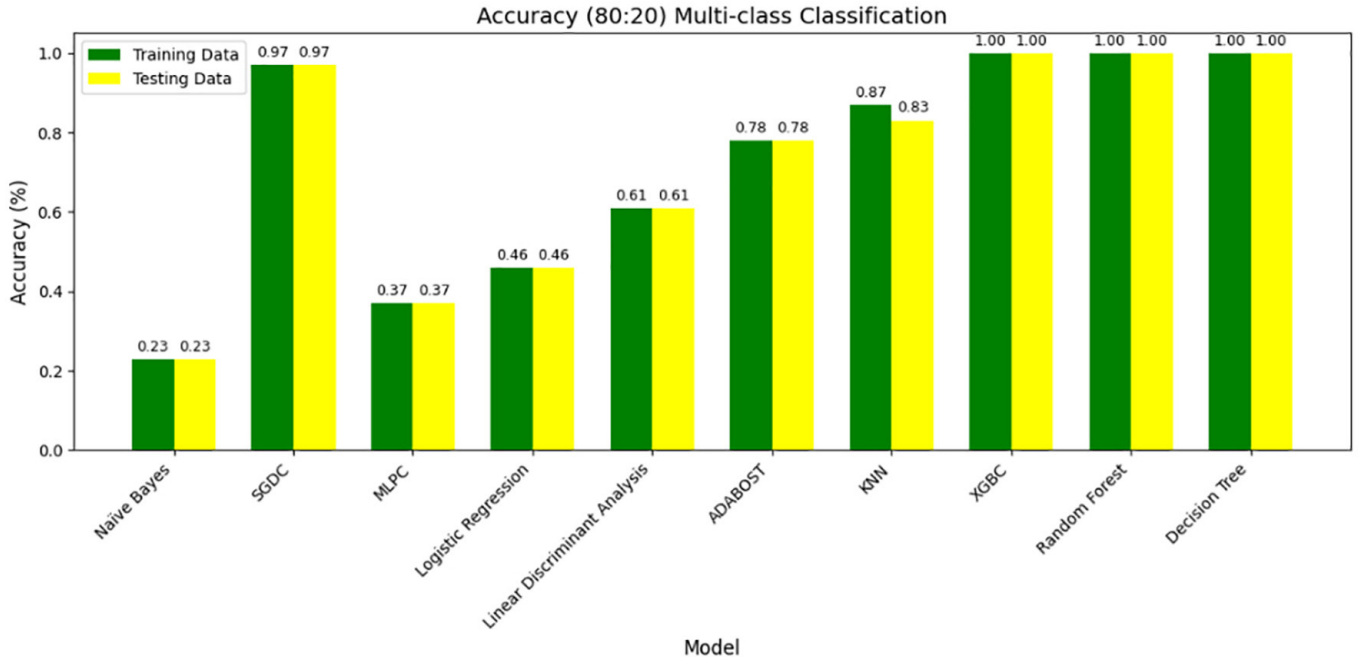

Fig. 5. Multi-class accuracy graph with 80:20 split

Figure 5 is a graph of the accuracy value of a multi-class algorithm. In this picture, only three algorithms have high accuracy values, namely the DT, RF, and XGBC algorithms. And the highest accuracy value is the NB algorithm. Only the KNN algorithm has a different accuracy value between training data and testing data, which are 0.83 and 0.87.

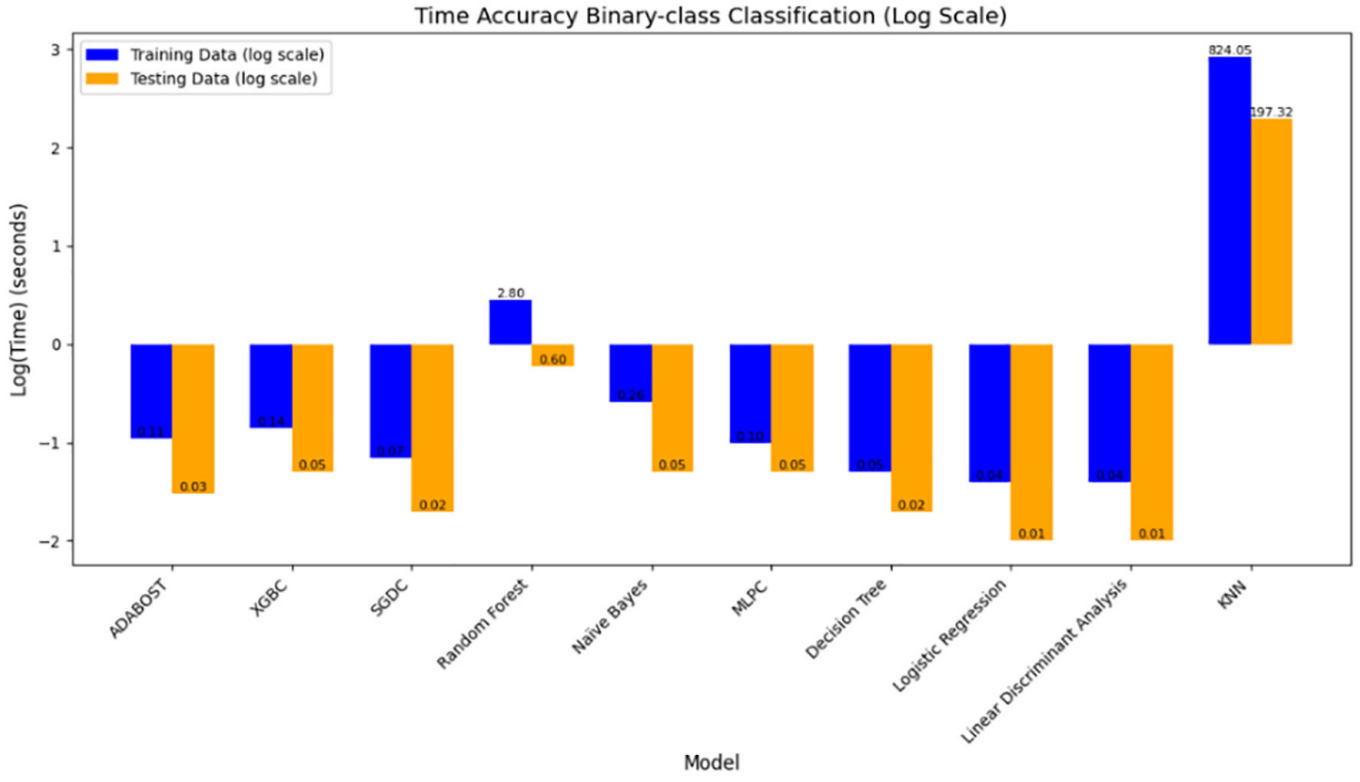

Fig. 6. Binary class accuracy time graph

Figure 6 is a graph using a logarithmic scale so that the comparison between models is more visible, including models with much larger times. The minimum binary class accuracy time is 0.01 seconds for the LR and LDA algorithms for testing data, while the longest time is the KNN algorithm at 824.05 seconds for training data.

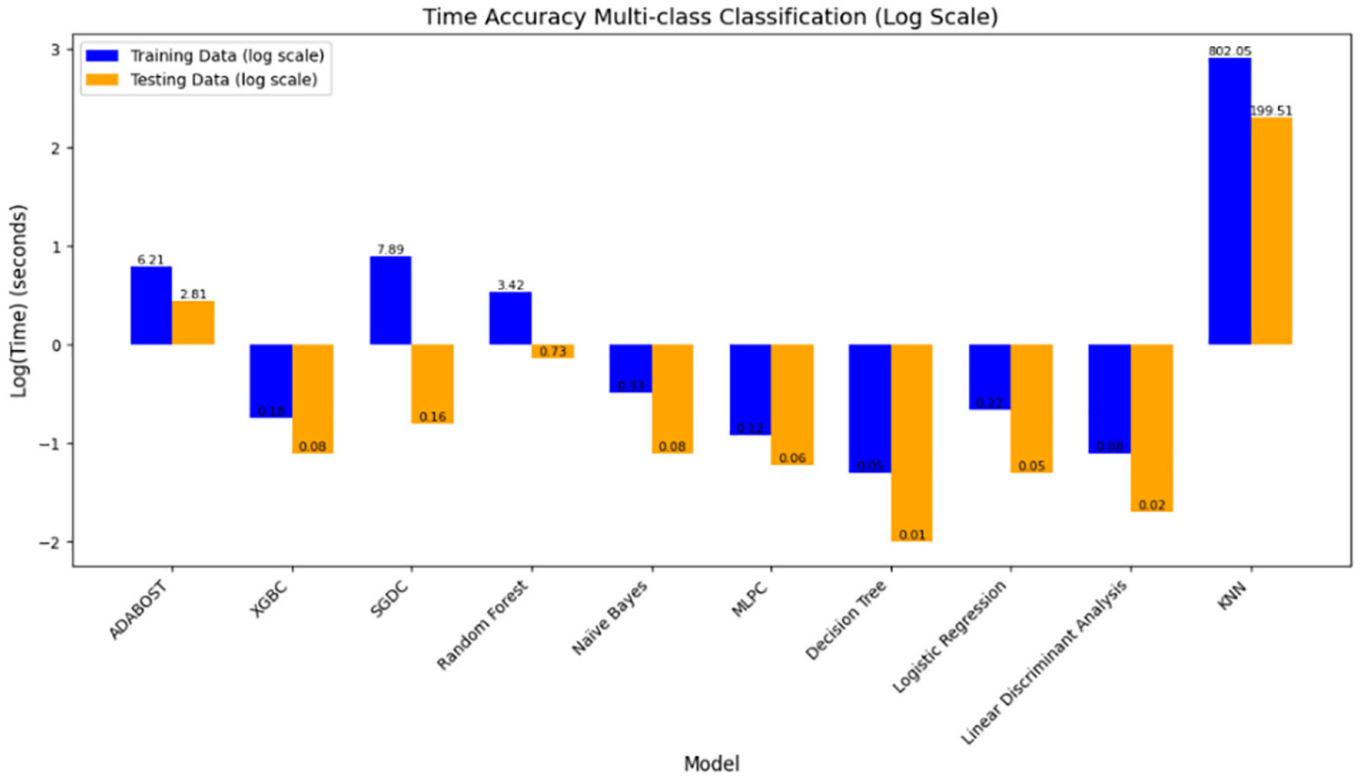

Fig. 7. Multi-class accuracy time graph

Figure 7 is a graph using a logarithmic scale so that the comparison between models is more visible, including models with much larger times. The fastest time on the DT algorithm is 0.01 seconds for testing data, while the longest time is 802.05 seconds for testing data on the KNN algorithm.

Table 5. Validation of k-fold binary-class

k-Fold Validation	Binary-class Classification									
	AB	XGBC	SGDC	RF	NB	MLPC	DT	LR	LDA	KNN
Iteration 1	1.00000	1.00000	0.65310	1.00000	0.50960	0.65320	1.00000	0.62400	0.63130	1.00000
Iteration 2	1.00000	1.00000	0.51330	1.00000	0.50510	0.65320	1.00000	0.62680	0.63460	1.00000
Iteration 3	1.00000	1.00000	0.57920	1.00000	0.50770	0.65320	1.00000	0.62540	0.63270	1.00000
Iteration 4	1.00000	1.00000	0.51720	1.00000	0.50430	0.65320	1.00000	0.62510	0.63020	1.00000
Iteration 5	1.00000	1.00000	0.50990	1.00000	0.50610	0.65320	1.00000	0.62220	0.63170	1.00000
Iteration 6	1.00000	1.00000	0.63580	1.00000	0.50420	0.65320	1.00000	0.62290	0.62980	1.00000
Iteration 7	1.00000	1.00000	0.65250	1.00000	0.50710	0.65320	1.00000	0.62480	0.63150	1.00000
Iteration 8	1.00000	1.00000	0.65310	1.00000	0.50600	0.65320	1.00000	0.62130	0.63060	1.00000
Iteration 9	1.00000	1.00000	0.65230	1.00000	0.50430	0.65320	1.00000	0.62310	0.63290	1.00000
Iteration 10	1.00000	1.00000	0.65320	1.00000	0.46310	0.65320	1.00000	0.62600	0.63070	1.00000

Table 6. Multi-class k-fold validation

k-Fold Validation	Multi-class Classification									
	AB	XGBC	SGDC	RF	NB	MLPC	DT	LR	LDA	KNN
Iteration 1	0.78160	1.00000	0.41010	1.00000	0.22590	0.36810	1.00000	0.49610	0.60680	0.83690
Iteration 2	0.78160	1.00000	0.44790	1.00000	0.22780	0.36810	1.00000	0.51490	0.60830	0.83760
Iteration 3	0.78160	1.00000	0.46410	1.00000	0.22580	0.36810	1.00000	0.51620	0.60970	0.83630
Iteration 4	0.78163	1.00000	0.22220	1.00000	0.22500	0.36810	1.00000	0.49710	0.60900	0.83900
Iteration 5	0.78160	1.00000	0.45600	0.99998	0.26250	0.36810	1.00000	0.46720	0.60660	0.83810
Iteration 6	0.78160	1.00000	0.28920	1.00000	0.22800	0.36810	1.00000	0.43030	0.60820	0.84100
Iteration 7	0.78160	1.00000	0.35330	1.00000	0.22460	0.36810	1.00000	0.41330	0.60790	0.84160
Iteration 8	0.78160	1.00000	0.42770	1.00000	0.22040	0.36810	1.00000	0.47910	0.60870	0.84010
Iteration 9	0.78170	1.00000	0.27710	1.00000	0.22430	0.36810	1.00000	0.51220	0.60600	0.83730
Iteration 10	0.78170	1.00000	0.37100	1.00000	0.23020	0.36810	1.00000	0.51030	0.60800	0.83610

Tables 5 and 6 are accuracy values with 10 iteration k-fold validations. Table 5 has the lowest accuracy value of 0.4631 in the 10th iteration with the NB algorithm; the SGDC algorithm has decreased accuracy in the 2nd, 3rd, 4th, and 5th iterations so that the average accuracy value becomes 0.6020. In Table 6 the NB algorithm has the lowest accuracy value of 0.2204 and the highest in the XGBC, RF, and DT algorithms of 1. In the SGDC algorithm, the accuracy value is unstable, and the RF algorithm has decreased accuracy in the 5th iteration of 0.00002018.

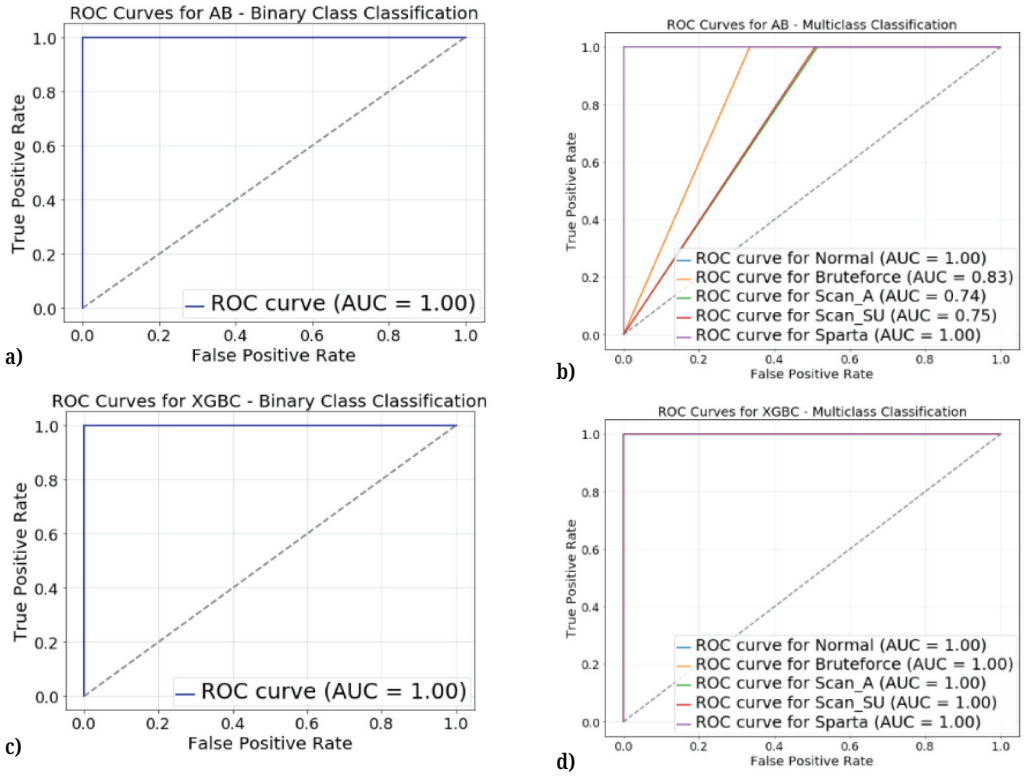

Fig. 8. *(Continued)*

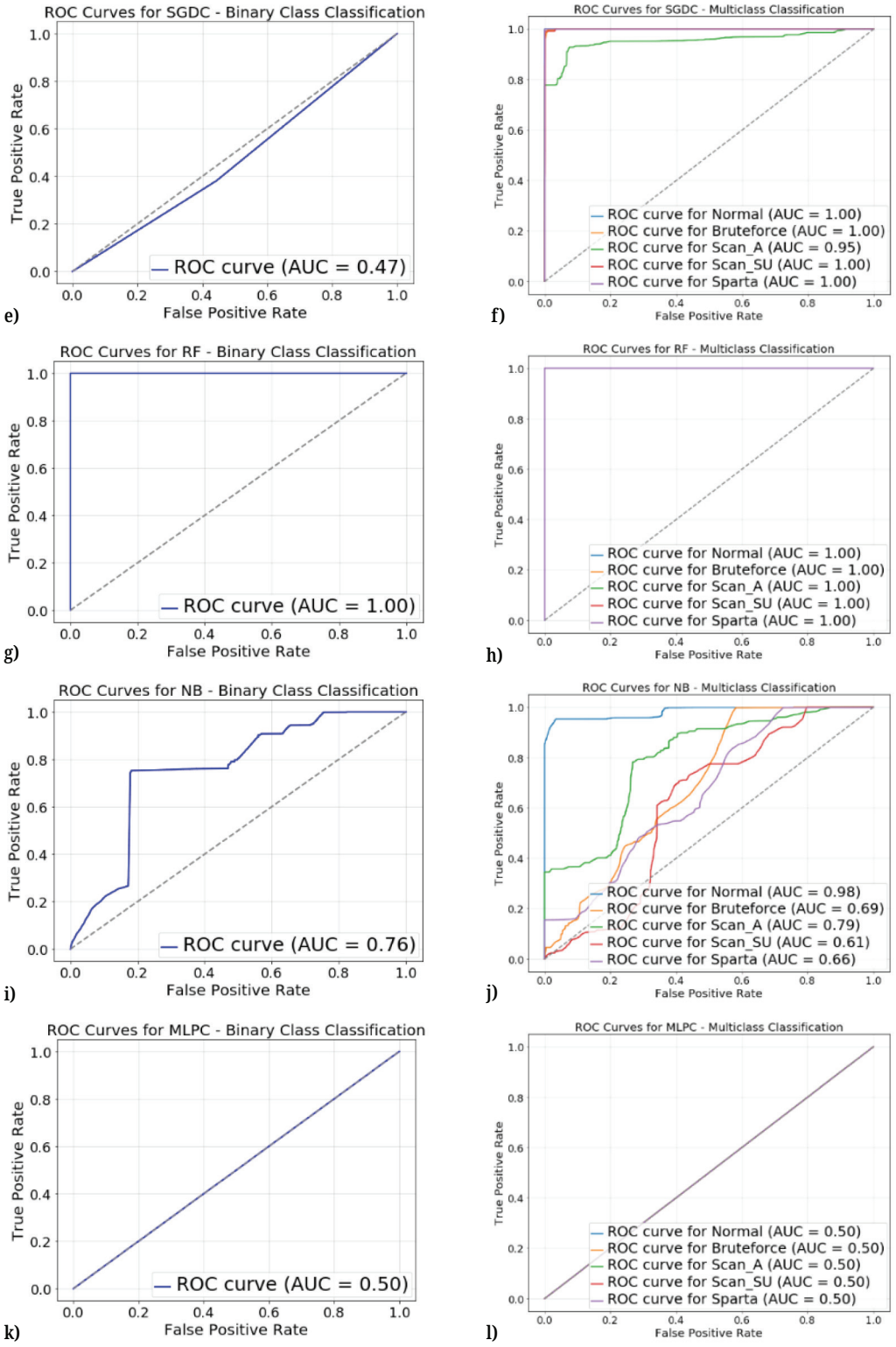

Fig. 8. *(Continued)*

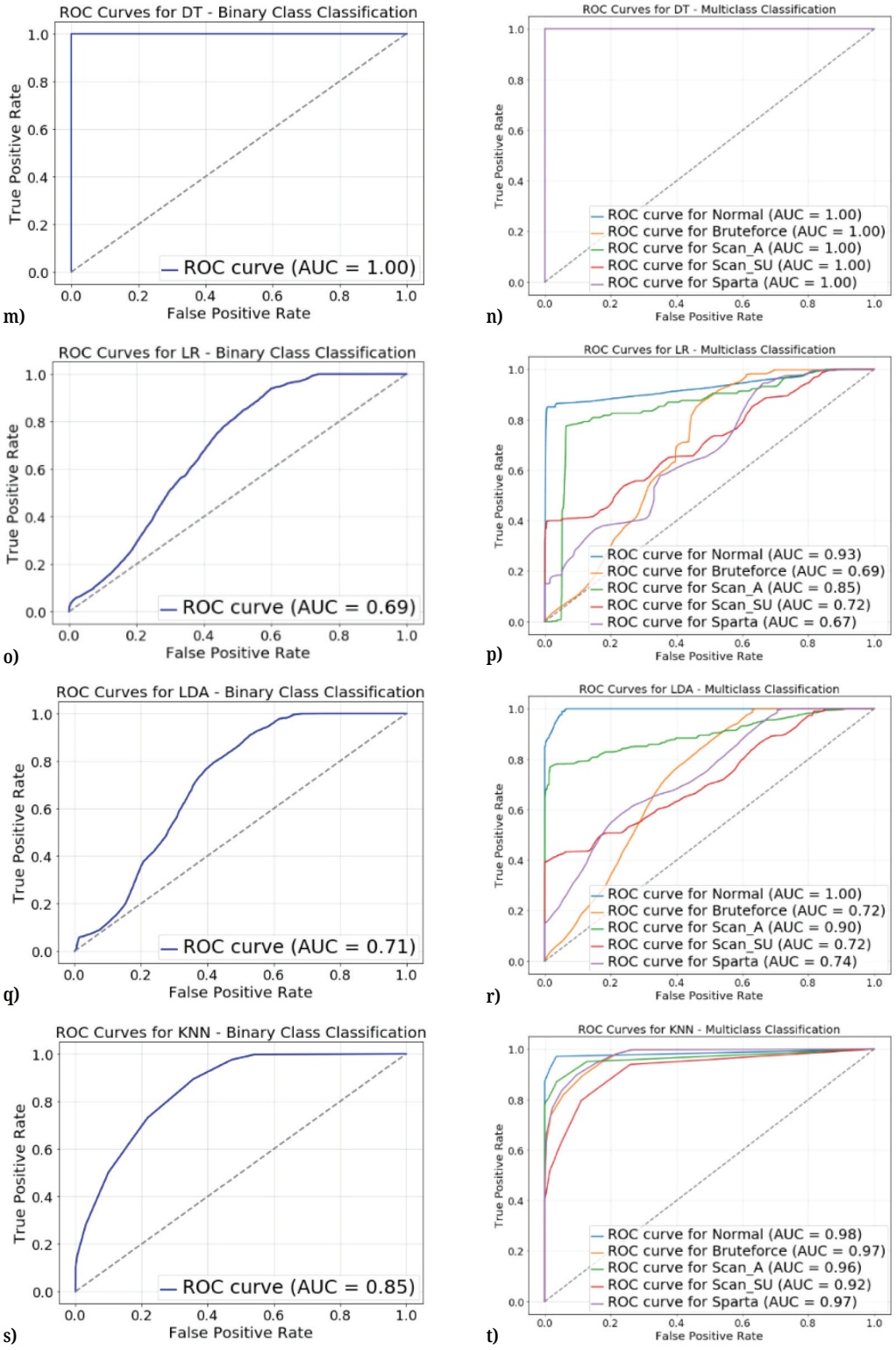

Fig. 8. ROC curve: (a) AB binary class, (b) AB Multi-class, (c) XGBC binary class, (d) XGBC multi-class, (e) SGDC binary class, (f) SGDC multi-class, (g) RF binary class, (h) RF multi-class, (i) NB binary class, (j) NB multi-class, (k) MLPC binary class, (l) MLPC multi-class, (m) DT binary class, (n) DT Multi-class, (o) LR binary class, (p) LR multi-class, (q) LDA binary class, (r) LDA multi-class, (s) KNN binary class, (t) KNN multi-class

Finally, Figure 8 displays the ROC for both binary class and multi-class classification results using various algorithms, including AB, XGBC, SGDC, RF, NB, MLPC, DT, LR, LDA, and KNN. The area under the curve is used to assess accuracy. Specifically, AB binary class, XGBC binary class and multi-class, RF binary class and multi-class, and DT binary class and multi-class consistently demonstrate higher accuracy, as evidenced by the entire area under the curve for each class being roughly equal to one. On the other hand, for SGDC binary class and multi-class, as well as NB multi-class, the curve remains below the diagonal line. As for MLPC binary class and multi-class, the curve falls exactly on the diagonal line.

Smart homes comprise a diverse array of devices such as smart locks, cameras, lighting systems, and thermostats, each with unique communication patterns. The unidirectional feature extraction approach ensures the IDS can generalize to traffic generated by these varied devices. This adaptability is crucial for addressing the dynamic and evolving nature of IoT ecosystems. Energy and computational constraints are often a limitation in IoT networks. The comparative analysis of algorithms highlights options such as DT and RF, which not only achieve high accuracy but also demonstrate efficient computation times. These characteristics make them suitable for deployment on resource-constrained edge devices within smart homes. While the current study validates the proposed IDS on the MQTT-IoT-IDS2020 dataset, its methodology can be extended to other protocols and datasets prevalent in IoT networks, such as CoAP, Zigbee, or LoRaWAN. Future enhancements may include real-time traffic analysis and the incorporation of self-learning mechanisms to adapt to emerging threats, further solidifying the IDS's practical utility.

This study places a strong emphasis on evaluating and strengthening the performance of 10 leading ML algorithms, including DT, RF, XGBC, and AB. The results highlight that DT and RS excel in achieving perfect accuracy for binary classifications, while XGBC shows superior performance in handling multi-class scenarios. These findings underline the adaptability and effectiveness of these algorithms in managing diverse IoT network traffic. The robustness of the proposed models is further enhanced by employing k-fold cross-validation, which ensures the prevention of overfitting and promotes generalizability. By combining high-performance metrics, accuracy, precision, recall, and F1 score with statistical feature extraction and unidirectional traffic analysis, this study provides a well-rounded and scalable IDS solution. The framework's ability to adapt to various IoT device behaviors and traffic patterns underscores its practicality for real-world deployment.

5 CONCLUSION AND FUTURE WORKS

This study concludes that the extraction of statistical features based on the UF packet header flow yields 19 features, but only 17 of these features are used in measuring classification performance. The results indicate that binary-class classification outperforms multi-class classification. Among the 10 algorithms tested, binary-class classification achieved an accuracy value of 1 for 4 algorithms: DT, RF, XGBC, and AB. In contrast, multi-class classification achieved an accuracy value of 1 for only 3 algorithms: DT, RF, and XGBC. The measurements were conducted using an 80:20 ratio data split and validated with k-fold. Notably, the time taken does not significantly impact the performance value. A fast time does not guarantee a high accuracy value, and conversely, a long time does not guarantee a low accuracy value. Binary-class classifications using LR and LDA took 0.01 seconds with accuracy values of 62% and 63%, respectively. On the other hand, the RF algorithm took 3.42 seconds

to achieve an accuracy value of 100% on the training data. On average, binary-class classification required less time compared to multi-class classification for both training and testing.

For future plans, the researchers intend to explore multi-class classification further by incorporating other algorithms such as RF, DT, SVM, and NB. They also plan to create datasets from a more comprehensive smart home network using an IoT network testbed. Additionally, they plan to implement feature selection using mutual information algorithms and Chi Square to improve the scores for both binary-class and multi-class classification.

6 ACKNOWLEDGMENT

Appreciation and thanks to the Directorate General of Higher Education. Research and Technology Ministry of Education. Culture. Research and Technology which has funded Doctoral Dissertation Research activities in 2023 with the title "Digital Forensics on IoT Smart Home Networks with Machine Learning," with contract number: 164/E5/PG.02.00.PL/2023 on date 19 of June 2023. We also thank the Institute of Research and Community Service at Sriwijaya University which has assisted this study activity through the research contract: 0143.11/UN9/SB3.LP2M. PT/2023. 05 of July 2023.

7 REFERENCES

[1] B. Martinez, C. Cano, and X. Vilajosana, "A square peg in a round hole: The complex path for wireless in the manufacturing industry," *IEEE Commun. Mag.*, vol. 57, no. 4, pp. 109–115, 2019. https://doi.org/10.1109/MCOM.2019.1800570

[2] G. Aceto, V. Persico, and A. Pescapé, "A survey on information and communication technologies for industry 4.0: State of the art, taxonomies, perspectives, and challenges," *IEEE Commun. Surv. Tutorials*, vol. 21, no. 4, pp. 3467–3501, 2019. https://doi.org/10.1109/COMST.2019.2938259

[3] Q. Zhang, L. T. Yang, Z. Chen, P. Li, and F. Bu, "An adaptive dropout deep computation model for industrial IoT big data learning with crowdsourcing to cloud computing," *IEEE Trans. Ind. Informatics*, vol. 15, no. 4, pp. 2330–2337, 2019. https://doi.org/10.1109/TII.2018.2791424

[4] A. Aldahiri, B. Alrashed, and W. Hussain, "Trends in using IoT with machine learning in health prediction system," *Forecasting*, vol. 3, no. 1, pp. 181–206, 2021. https://doi.org/10.3390/forecast3010012

[5] F. Zantalis, G. Koulouras, S. Karabetsos, and D. Kandris, "A review of machine learning and IoT in smart transportation," *Futur. Internet*, vol. 11, no. 4, p. 94, 2019. https://doi.org/10.3390/fi11040094

[6] J. Chin, V. Callaghan, and I. Lam, "Understanding and personalising smart city services using machine learning, the Internet-of-Things and big data," in *International Symposium on Industrial Electronics*, 2017, pp. 2050–2055. https://doi.org/10.1109/ISIE.2017.8001570

[7] S. Peter and R. K. Gopal, "Multi-level authentication system for smart home-security analysis and implementation," in *2016 International Conference on Inventive Computation Technologies (ICICT)*, 2016, pp. 1–7. https://doi.org/10.1109/INVENTIVE.2016.7824790

[8] E. M. Zeleke, H. M. Melaku, and F. G. Mengistu, "Efficient intrusion detection system for SDN orchestrated Internet of Things," *J. Comput. Networks Commun.*, vol. 2021, no. 1, p. 5593214, 2021. https://doi.org/10.1155/2021/5593214

[9] V. A. Akpan, J. B. Agbogun, and D. A. Olatunji, "The development of an integrated wireless security surveillance system based on Internet-of-Things technologies," *Int. J. Internet Things*, vol. 10, no. 1, pp. 1–21, 2022.

[10] M. Shanthini, G. Vidya, and R. Arun, "IoT enhanced smart door locking system," in *2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT)*, 2020, pp. 92–96. https://doi.org/10.1109/ICSSIT48917.2020.9214288

[11] T. Malche and P. Maheshwary, "Internet of Things (IoT) for building smart home system," in *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, 2017, pp. 65–70. https://doi.org/10.1109/I-SMAC.2017.8058258

[12] S. P. Makhanya, E. M. Dogo, N. I. Nwulu, and U. Damisa, "A smart switch control system using ESP8266 Wi-Fi module integrated with an android application," in *2019 IEEE 7th International Conference on Smart Energy Grid Engineering (SEGE)*, 2019, pp. 125–128. https://doi.org/10.1109/SEGE.2019.8859904

[13] Y. C. See and S. J. Jing, "Internet of Things (IoT) based smart wall outlet," in *2019 4th International Conference and Workshops on Recent Advances and Innovations in Engineering (ICRAIE)*, 2019, pp. 1–5. https://doi.org/10.1109/ICRAIE47735.2019.9037646

[14] H. Ruser *et al.*, "Evaluating the accuracy and user experience of a gesture-based infrared remote control in smart homes," in *Human-Computer Interaction. Interaction Techniques and Novel Applications*, vol. 12763, 2021, pp. 89–108. https://doi.org/10.1007/978-3-030-78465-2_8

[15] A. A. Diro and N. Chilamkurti, "Distributed attack detection scheme using deep learning approach for Internet of Things," *Futur. Gener. Comput. Syst.*, vol. 82, pp. 761–768, 2018. https://doi.org/10.1016/j.future.2017.08.043

[16] M. K. Kagita, N. Thilakarathne, T. R. Gadekallu, P. K. R. Maddikunta, and S. Singh, "A review on cyber crimes on the Internet of Things," in *Deep Learning for Security and Privacy Preservation in IoT*, 2021, pp. 83–98. https://doi.org/10.1007/978-981-16-6186-0_4

[17] S. Singh, P. K. Sharma, and J. H. Park, "SH-SecNet: An enhanced secure network architecture for the diagnosis of security threats in a smart home," *Sustainability*, vol. 9, no. 4, p. 513, 2017. https://doi.org/10.3390/su9040513

[18] Z. Liu *et al.*, "Using embedded feature selection and CNN for classification on CCD-INID-V1—A new IoT dataset," *Sensors*, vol. 21, no. 14, p. 4834, 2021. https://doi.org/10.3390/s21144834

[19] B. A. Tama and K.-H. Rhee, "Attack classification analysis of IoT network via deep learning approach," *Res. Briefs Inf. Commun. Technol. Evol.*, vol. 3, pp. 150–158, 2017. https://doi.org/10.56801/rebicte.v3i.54

[20] S. Aljawarneh, M. Aldwairi, and M. B. Yassein, "Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model," *J. Comput. Sci.*, vol. 25, pp. 152–160, 2018. https://doi.org/10.1016/j.jocs.2017.03.006

[21] T. Saranya, S. Sridevi, C. Deisy, T. D. Chung, and M. K. A. A. Khan, "Performance analysis of machine learning algorithms in intrusion detection system: A review," *Procedia Comput. Sci.*, vol. 171, pp. 1251–1260, 2020. https://doi.org/10.1016/j.procs.2020.04.133

[22] S. Costantini, G. De Gasperis, and R. Olivieri, "Digital forensics and investigations meet artificial intelligence," *Ann. Math. Artif. Intell.*, vol. 86, pp. 193–229, 2019. https://doi.org/10.1007/s10472-019-09632-y

[23] A. Anish Halimaa and D. K. Sundarakantham, "Machine learning based intrusion detection system," in *Proceedings of the Third International Conference on Trends in Electronics and Informatics (ICOEI)*, 2019, pp. 916–920. https://doi.org/10.1109/ICOEI.2019.8862784

[24] H.-T. Hsu, G.-J. Jong, J.-H. Chen, and C.-G. Jhe, "Improve IoT security system of smart-home by using support vector machine," in *2019 IEEE 4th International Conference on Computer and Communication Systems (ICCCS)*, 2019, pp. 674–677. https://doi.org/10.1109/CCOMS.2019.8821678

[25] I. Cvitic, D. Perakovic, M. Perisa, and B. Gupta, "Ensemble machine learning approach for classifcation of IoT devices in smart home," *Int. J. Mach. Learn. Cybern.*, vol. 12, pp. 3179–3202, 2021. https://doi.org/10.1007/s13042-020-01241-0

[26] M. Shafiq, Z. Tian, Y. Sun, X. Du, and M. Guizani, "Selection of effective machine learning algorithm and Bot-IoT attacks traffic identification for internet of things in smart city," *Futur. Gener. Comput. Syst.*, vol. 107, pp. 433–442, 2020. https://doi.org/10.1016/j.future.2020.02.017

[27] P. Nimbalkar and D. Kshirsagar, "Feature selection for intrusion detection system in Internet-of-Things (IoT)," *ICT Express*, vol. 7, no. 2, pp. 177–181, 2021. https://doi.org/10.1016/j.icte.2021.04.012

[28] M. Al-Akhras, M. Alawairdhi, A. Alkoudari, and S. Atawneh, "Using machine learning to build a classification model for IoT networks to detect attack signatures," *Int. J. Comput. Networks Commun.*, vol. 12, no. 6, 2020. https://doi.org/10.5121/ijcnc.2020.12607

[29] R. Qaddoura, A. M. Al-Zoubi, I. Almomani, and H. Faris, "A multi-stage classification approach for IoT intrusion detection based on clustering with oversampling," *Appl. Sci.*, vol. 11, no. 7, p. 3022, 2021. https://doi.org/10.3390/app11073022

[30] R. Kumar, M. Swarnkar, G. Singal, and N. Kumar, "IoT network traffic classification using machine learning algorithms: An experimental analysis," *IEEE Internet Things Journal*, vol. 9, no. 2, pp. 989–1008, 2022. https://doi.org/10.1109/JIOT.2021.3121517

[31] G. Spanos, K. M. Giannoutakis, K. Votis, and D. Tzovaras, "Combining statistical and machine learning techniques in IoT anomaly detection for smart homes," in *2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*, 2019, pp. 1–6. https://doi.org/10.1109/CAMAD.2019.8858490

[32] P. N. Dawadi, D. J. Cook, M. Schmitter-Edgecombe, and C. Parsey, "Automated assessment of cognitive health using smart home technologies," *Technology Heal. Care*, vol. 21, no. 4, pp. 323–343, 2013. https://doi.org/10.3233/THC-130734

[33] M. S. Reza and J. Ma, "ICA and PCA integrated feature extraction for classification," in *2016 IEEE 13th International Conference on Signal Processing (ICSP)*, 2016, pp. 1083–1088. https://doi.org/10.1109/ICSP.2016.7877996

[34] T. Li, Z. Hong, and L. Yu, "Machine learning-based intrusion detection for IoT devices in smart home," in *2020 IEEE 16th International Conference on Control & Automation (ICCA)*, 2020, pp. 277–282. https://doi.org/10.1109/ICCA51439.2020.9264406

[35] R.-C. Chen, C. Dewi, S.-W. Huang, and R. E. Caraka, "Selecting critical features for data classification based on machine learning methods," *J. Big Data*, vol. 7, 2020. https://doi.org/10.1186/s40537-020-00327-4

[36] M.-O. Pahl and F.-X. Aubet, "All eyes on you: Distributed multi-dimensional IoT microservice anomaly detection," 2018, *14th International Conference on Network and Service Management (CNSM)*, 2018, pp. 72–80. [Online]. Available: https://ieeexplore.ieee.org/document/8584985

[37] G. E. I. Selim, E. E.-D. Hemdan, A. M. Shehata, and N. A. El-Fishawy, "Anomaly events classification and detection system in critical industrial internet of things infrastructure using machine learning algorithms," *Multimed. Tools Appl.*, vol. 80, pp. 12619–12640, 2021. https://doi.org/10.1007/s11042-020-10354-1

[38] A. Abbas, M. A. Khan, S. Latif, M. Ajaz, A. A. Shah, and J. Ahmad, "A new ensemble-based intrusion detection system for Internet of Things," *Arab. J. Sci. Eng.*, vol. 47, pp. 1805–1819, 2022. https://doi.org/10.1007/s13369-021-06086-5

[39] Z. R. S. Elsi *et al.*, "Feature selection using chi square to improve attack detection classification in IoT network: Work in progress," in *2022 9th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI2022)*, 2022, pp. 226–232. https://doi.org/10.23919/EECSI56542.2022.9946621

[40] P. Kumar, G. P. Gupta, and R. Tripathi, "An ensemble learning and fog-cloud architecture-driven cyber-attack detection framework for IoMT networks," *Comput. Commun.*, vol. 166, pp. 110–124, 2021. https://doi.org/10.1016/j.comcom.2020.12.003

[41] J. White and S. D. Power, "k-Fold cross-validation can significantly over-estimate true classification accuracy in common EEG-based passive BCI experimental designs: An empirical investigation," *Sensors*, vol. 23, no. 13, p. 6077, 2023. https://doi.org/10.3390/s23136077

[42] A. Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman, "Survey of intrusion detection systems: Techniques, datasets and challenges," *Cybersecurity*, 2019. https://doi.org/10.1186/s42400-019-0038-7

[43] I. H. Sarke, "CyberLearning: Effectiveness analysis of machine learning security modeling to detect cyber-anomalies and multi-attacks," *Internet of Things*, vol. 14, p. 100393, 2021. https://doi.org/10.1016/j.iot.2021.100393

[44] N. Dogru and A. Subasi, "Traffic accident detection using random forest classifier," in *2018 15th Learning and Technology Conference (L&T)*, 2018, pp. 40–45. https://doi.org/10.1109/LT.2018.8368509

[45] B. M. H. A. Allen, A. I. Daood, and W. H, "Poster abstract: Comparison of classifiers for prediction of human actions in a smart home," in *2018 IEEE/ACM Third International Conference on Internet-of-Things Design and Implementation (IoTDI)*, 2018, pp. 287–288. https://doi.org/10.1109/IoTDI.2018.00043

[46] T. OConnor, R. Mohamed, M. Miettinen, W. Enck, B. Reaves, and A.-R. Sadeghi, "HomeSnitch: Behavior transparency and control for smart home IoT devices," in *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks*, 2019, pp. 128–138. https://doi.org/10.1145/3317549.3323409

[47] A. L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," *IEEE Commun. Surv. Tutorials*, vol. 18, no. 2, pp. 1153–1176, 2016. https://doi.org/10.1109/COMST.2015.2494502

[48] A. Yeboah-Ofori and R. Boachie, "Malware attack predictive analytics in a cyber supply chain context using machine learning," in *2019 International Conference on Cyber Security and Internet of Things (ICSIoT)*, 2019, pp. 66–73. https://doi.org/10.1109/ICSIoT47925.2019.00019

[49] S. Liaqat, A. Akhunzada, F. S. Shaikh, A. Giannetsos, and M. A. Jan, "SDN orchestration to combat evolving cyber threats in Internet of Medical Things (IoMT)," *Comput. Commun.*, vol. 160, pp. 697–705, 2020. https://doi.org/10.1016/j.comcom.2020.07.006

[50] M. Hasan, M. M. Islam, M. I. I. Zarif, and M. M. A. Hashem, "Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches," *Internet of Things*, vol. 7, p. 100059, 2019. https://doi.org/10.1016/j.iot.2019.100059

[51] S. Panda and G. Panda, "Intelligent classification of IoT traffic in healthcare using machine learning techniques," in *2020 6th International Conference on Control*, 2020, pp. 581–585. https://doi.org/10.1109/ICCAR49639.2020.9107979

[52] S. Aljawarneha, M. Aldwairi, and M. B. Yasseina, "Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model," *J. Comput. Sci.*, vol. 25, pp. 152–160, 2018. https://doi.org/10.1016/j.jocs.2017.03.006

[53] N. Moustafa, B. Turnbull, and K.-K. R. Choo, "An ensemble intrusion detection technique based on proposed statistical flow features for protecting network traffic of Internet of Things," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4815–4830, 2019. https://doi.org/10.1109/JIOT.2018.2871719

[54] A. Churcher *et al.*, "An experimental analysis of attack classification using machine learning in IoT networks," *Sensors*, vol. 21, no. 2, p. 446, 2021. https://doi.org/10.3390/s21020446

[55] M. Saharkhizan, A. Azmoodeh, A. Dehghantanha, K.-K. R. Choo, and R. M. Parizi, "An ensemble of deep recurrent neural networks for detecting IoT cyber attacks using network traffic," *Internet Things J.*, vol. 7, no. 9, pp. 8852–8859, 2020. https://doi.org/10.1109/JIOT.2020.2996425

[56] R. Gassais, N. Ezzati-Jivan, J. M. Fernandez, D. Aloise, and M. R. Dagenais, "Multi-level host-based intrusion detection system for Internet of Things," *J. Cloud Comput. Adv. Syst. Appl.*, vol. 9, 2020. https://doi.org/10.1186/s13677-020-00206-6

[57] K. N. Mishra and S. C. Pandey, "Fraud prediction in smart societies using logistic regression and k-fold machine learning techniques," *Wirel. Pers. Commun.*, vol. 119, pp. 1341–1367, 2021. https://doi.org/10.1007/s11277-021-08283-9

[58] P. Kumar, G. P. Gupta, and R. Tripathi, "A distributed ensemble design based intrusion detection system using fog computing to protect the internet of things networks," *J. Ambient Intell. Humaniz. Comput.*, vol. 12, pp. 9555–9572, 2021. https://doi.org/10.1007/s12652-020-02696-3

[59] H. Hindy, E. Bayne, M. Bures, R. Atkinson, C. Tachtatzis, and X. Bellekens, "Machine learning based IoT intrusion detection system: An MQTT case study (MQTT-IoT-IDS2020 Dataset)," in *Selected Papers from the 12th International Networking Conference*, B. Ghita and S. Shiaeles, Eds., Cham: Springer International Publishing, vol. 180, 2021, pp. 73–84. https://doi.org/10.1007/978-3-030-64758-2_6

[60] Z. Cui, R. Ke, Z. Pu, and Y. Wang, "Deep bidirectional and unidirectional LSTM recurrent neural network for network-wide traffic speed prediction," *arXiv preprint arXiv:1801.02143*, 2018. https://doi.org/10.48550/ARXIV.1801.02143

[61] A. Boukhtouta, S. Mokhov, N.-E. Lakhdari, and M. Debbabi, "Network malware classification comparison using DPI and flow packet headers," *J. Comput. Virol. Hacking Tech.*, vol. 12, pp. 69–100, 2015. https://doi.org/10.1007/s11416-015-0247-x

[62] A. Murad and J.-Y. Pyun, "Deep recurrent neural networks for human activity recognition," *Sensors*, vol. 17, no. 11, p. 2556, 2017. https://doi.org/10.3390/s17112556

8 AUTHORS

Zulhipni Reno Saputra Elsi Received a Master's degree in Computer Science from Bina Darma University, Palembang, South Sumatra, Indonesia. Currently he is a PhD candidate at the Faculty of Engineering, Sriwijaya University and serves as a Senior Lecturer at the Faculty of Engineering, Muhammadiyah University, Palembang, Indonesia. His research interests include Internet of Things, computer networks, information security, Intrusion Detection Systems. He can be contacted at email: Zulhipni_renosaputra@um-palembang.ac.id.

Deris Stiawan Received the PhD degree in Computer Engineering from Universiti Teknologi Malaysia, Malaysia. He is currently serving as a Professor at Department of Computer Engineering, Faculty of Computer Science, Universitas Sriwijaya. His research interests include computer network, Intrusion Detection/Prevention System, and heterogeneous network. He can be contacted at email: deris@unsri.ac.id.

Bhakti Yudho Suprapto is an Associate Professor in the Electrical department at the Faculty of Engineering University of Sriwijaya, Indonesia. He obtained a Doctor's Degree in Electrical Engineering from Universitas Indonesia. His professional profile has derived to Robotic and Control, which focused on, fuzzy logic, and neural network. His research interests include control system. He can be contacted at email: bhakti@ft.unsri.ac.id.

M. Agus Syamsul Arifin Received a doctorate degree at the Faculty of Engineering, Sriwijaya University. Currently he serves as a Senior Lecturer at the Computer Faculty of Bina Insan University, Indonesia. His research interests include computer networks, information security, Intrusion Detection Systems. He can be contacted at email: mas.arifin@univbinainsan.ac.id.

Mohd. Yazid Idris An Associate Professor at Faculty of Computing, Universiti Teknologi Malaysia. He obtained his M.Sc and Ph.D. in the area of Software Engineering, and Information Technology (IT) Security in 1998 and 2008 respectively. In software engineering, he focuses on the research of designing and development of mobile and telecommunication software. His main research activity in IT security is in the area of Intrusion Prevention and Detection (IPD). He can be contacted at email: yazid@utm.my.

Rahmat Budiarto Received B.Sc. degree from Bandung Institute of Technology in 1986, M.Eng. and Dr.Eng. in Computer Science from Nagoya Institute of Technology in 1995 and 1998, respectively. Currently, he is a full Professor at College of Computer Science and IT, Albaha University, Saudi Arabia. His research interests include intelligent systems, brain modeling, IPv6, network security, Wireless sensor networks, and MANETs. He can be contacted at email: rahmat@bu.edu.sa.