Machine Learning for Securing Traffic in Computer Networks

Ahmed BaniMustafa[1], Mahmoud Baklizi[2], Khalaf Khatatneh[3]
(Senior Member, IEEE)-Data Science and Artificial Intelligence Department, Isra University, Amman, Jordan[1]
Computer Science Department, Isra University, Amman, Jordan[2, 3]

***Abstract*—Computer network attacks are among the most significant and common threats against computer-wired and wireless communications. Intrusion detection technology is used to secure computer networks by monitoring network traffic and identifying attacks. In this paper, we investigate and evaluate the application of four machine learning classification algorithms for identifying attacks that target computer networks: DDoS, Brute Force Web, and SQL Injection attacks, in addition to Benign Traffic. A public dataset of 80 features was used to build four machine learning models using Random Forest, Logistic Regression, CN2, and Neural Networks. The constructed models were evaluated based on 10-fold cross-validation using Classification Accuracy (CA), Area under the Curve (AUC), F1, Recall, Specificity, and Sensitivity metrics in addition to Confusion Matrix, Calibration, Lift, and ROC plots. The Random Forest model achieved 98% in the CA score and 99% in the AUC score, while the Logistic regression achieved 90% in the CA score and 98% in the AUC score.**

***Keywords*—Machine learning; data mining, cyber security; computer networks; intrusion detection**

I. Introduction

Computer networks are pivotal in today's world. They connect people, machines, and systems on various scales. Cisco has estimated that 29 billion devices will be connected through computer networks by 2023 [1].

However, network communication security is subject to being hampered by several novel attacks, which necessitate more effective monitoring, detection, identification, and prevention of network attacks which remains an unsolved challenge in the cyber world. This is due to the variety, complexity, and ever-growing sophistication of the technology utilized in these attacks.

Machine learning has successfully solved similar problems in various domains and applications [2, 3] using several supervised and unsupervised learning algorithms [4-6]. This success can be inspired to solve problems in network security by detecting and identifying various types of intrusion attacks that enable monitoring and prevention of such attacks.

This work investigates and evaluates the use of machine learning technology for detecting and identifying four types of network traffic: DDoS attacks, SQL Injection, Brute Force Web attacks, and Benign Traffic. Four machine learning techniques were applied in this study. These include Random Forest (RF), Logistic Regression (LR), CN2 Rules Inducer, and Neural Networks (NN). The constructed models were then evaluated based on Classification Accuracy (CA), Area Under the Curve (AUC) [7], Precision, Recall, and F1 metrics [8]. A confusion matrix was also created for each constructed model [9]. The Calibration, Lift, and Receiver Operating Characteristic (ROC) curves were used to compare and confirm the validity and robustness of the created models [10].

The dataset in this work was sampled from a publicly simulated big dataset which was created by the Communications Security Establishment (CSE) and the Canadian Institute of Cybersecurity (CIC) for Intrusion Detection Systems (IDS). The dataset was published under the name CSE-CIC-IDS2018 [11, 12]. The original dataset comprises 16 million samples described using 80 features related to the traffic flow on the network [13, 14]. The dataset was acquired using the Amazon Amazon Web Services (AWS) Command Line Tool (CLI) [12] and underwent intensive processing involving intensive filtering, sampling, integration, and randomization procedures. It was then explored to examine its quality, distribution, and potential. The sampled data covers three types of attacks: (1) Distributed Denial of Service (DDoS) Low Orbit Ion Cannon (LOIC) Datagram Protocol (UDP), which is referred to as DDOS LOIC-UDP attacks; (2) Structured Query Language (SQL) Injection attacks; (3) Brute-Force Web attacks in addition to Benign Traffic.

Research Problem: Network attacks are difficult to detect and identify using normal network hardware and software tools. Differentiating normal Traffic from network attacks is a complex task that might create threats to network security and interrupt services.

Research Question: Can machine learning classification algorithms detect and identify network attacks based on the numerous characteristics of network traffic flow?

Research Objectives: Investigate and evaluate the use of four machine learning algorithms for detecting and identifying common types of network attacks. The resulting models can be embedded in the network firewall, proxies, routers, and other security tools, suites, and solutions.

Research Contribution:

1) Creating successful machine learning models that can be used for detecting and identifying types of network attacks.

2) Identifying significant traffic features can be used as predictors for identifying and detecting network attacks.

Section II provides a theoretical framework for the conducted research, while Section III reviews the related work. Section IV describes the dataset, while Section V describes the research methodology applied in the study. Section VI describes the research results, Section VII discusses the obtained results, and Section VIII draws a conclusion and comments on the limitation and the future work which can extend this study.

II. Related Work

This section reviews five of the most relevant works on intrusion detection using machine learning.

A study was reported in [15] which aimed at investigating the use of A Convolutional Neural Network (CNN) and Recurrent Neural Networks for detecting denial service (DoS) attacks using the CSE-CIC-IDS2018 and Knowledge Discovery in Databases (KDD) Cup 1999 data. The Convolutional Neural Network (CNN) model detected the Denial of Service (DoS) attacks using the CSE-CIC-IDS2018 dataset with a CA score of 91.5% and 99% using the KDD Cup 99 dataset. On the other hand, the Recurrent Neural Network (RNN) model could classify the CSE-CIC-IDS2018 with a CA score of 65% and a CA score of 93% based on the KDD Cup 99 dataset.

In [16], Andercut reported applying the K-Nearest Neighbor (KNN) algorithm in identifying attacks from benign Traffic with a CA score of 99% using 9/10 of the files in the CSE-CIC-IDS2018 dataset. However, the model scored a CA score of 72% using one of the files in the dataset.

The Iterative Dichotomiser 3 (ID3) and Naïve Bayes algorithms were used in [17] to detect four attack classes and a normal traffic class using the KDD Cup 99 dataset. The study reported a CA score between 97% and 99% in classifying Probe, DoSm R2L, and Normal classes and 94% in predicting attacks that belong to the U2R class.

A study reported using K-Nearest Neighbor Classifier (KNN), Naïve Bayes, Adaboost with Decision Tree, Support Vector Machine, and Random Forest using CSE-CIC-IDS2018 in identifying portrayal botnet attacks with a reported accuracy of 99% [18].

A study in [30] reported using KNN, Random Forest, and Logistic Regression to identify botnet and infiltration attacks using the CSE-CIC-IDS2018 dataset. The applied algorithms identified the attacks with a CA score of 90%.

The related work analysis shows that most of the surveyed studies were conducted to identify a subset of the attacks in the CSE-CIC-IDS2018 and KDD Cup 99 datasets with a CA score ranging from 65% to 99%. However, most studies that reported high CA scores aimed at identifying only one or two types of attacks.

Furthermore, the performance of the applied machine learning techniques scored better when they were applied to the KDD Cup 99 dataset, which contains much fewer samples and much fewer features than the CSE-CIC-IDS2018 dataset. On the other hand, most of the reported studies used the CA metric to evaluate the performance of their reported models, while some used other metrics only to confirm the CA score.

III. Theoretical Framework

Here we provide a brief overview of the concepts related to network intrusion attacks and the machine learning techniques applied in this study.

A. Network Attacks

Network attacks are ″a set of malicious activities that disrupt, deny, degrade, or destroy information and services in a computer network.″ The attacks are usually carried out by sending streams of data that intrudes to affect the availability, integrity, privacy, and secrecy of the services and data communicated through the targeted network [19]. Four types of computer network traffic are investigated in this work: Benign, DDos-LOIC-UDP, Brute-Force-Web, and SQL Injection attacks.

- Brute-Force Web: attacks that aim at cracking vulnerable computer networks that depend on weak user credentials, which consist of weak usernames and passwords [11, 20, 21].
- Distributed Denial of Service (DDoS): attacks designed to target network or web servers with limited bandwidth by overwhelming them with requests from tens or hundreds of distributed URL addresses [11, 22, 23]. DDOS LOIC-UDP stands for Distributed Denial of Service (DDoS) Low Orbit Ion Cannon (LOIC) Datagram Protocol (UDP).
- SQL Injection: stands for Structured Query Language (SQL) attacks. It works by injecting code into databases to gain unauthorized access to data by executing unsolicited queries or damaging the integrity of your database [11, 24-27].
- Benign Traffic: generated to realistically simulate the normal and usual behavior of human users in a typical and normal computer network [11, 16, 19].

B. Machine Learning

- Machine learning is an artificial intelligence field that aims to mimic the human learning process by creating algorithms fed with data [28]. Machine learning techniques are divided into two categories: supervised and unsupervised. While supervised learning aims to find patterns in pre-labeled data, unsupervised learning depends on finding patterns based on data self-labeling [2, 3, 5].
- Random Forest: An ensembled supervised learning technique for regression, classification, and feature ranking. The Random Forest algorithm builds multiple trees created based on a recursive partitioning approach that divides the feature space into several regions that encapsulate a set observation with relative values of responses. The random-forest algorithm is applied to many variables with hard-to-analyze relationships

[29-31]. Random Forest were applied by recent studies in detecting intrusion attacks [32-35].

- Logistic Regression: A supervised learning algorithm that works by assuming a non-linear relationship between features using a logit function that is used to predict the probability of data belonging to a predefined class which is assigned a value between 0 and 1 and then labeled with the closest value (0 or 1). Unlike linear regression, Logistic Regression can be applied to numerical and nominal data [36]. Examples of recent studies that reported the successful use of Logistic Regression in intrusion detection are available in [6, 34, 37].
- CN2: A rules induction algorithm that aims at inducing simple and understandable rules in the form of (if-then-statements). The CN2 algorithm is used for solving classification problems and is known for its ability to handle noise in data [38]. A recent comparative study reported using CN2 in network security [39].
- Neural Networks: A supervised machine learning technique that simulates thinking in the brain. It consists of interconnected neurons organized into a set of layers that input, output, and one or more hidden layers. The algorithm can achieve learning by example by adjusting the triggering weights assigned to the neurons using a sigmoid function and then adjusting through backpropagation. Neural Networks can solve regression and classification problems [40, 41]. Several example studies reported that the neural networks technique was successful in detecting network intrusion attacks [18, 42, 43].

IV. Dataset

The original dataset in this research is a simulated public dataset published by the Communications Security Establishment (CSE) and the Canadian Institute of Cybersecurity (CIC) for Intrusion Detection Systems (IDS) under the name CSE-CIC-IDS2018 dataset. The dataset was collected over a sixteen-day period which extends between 14/02/2018 and 20/03/2018.

The data was labeled with the date of its recording and then stored in a Comma Separated Values (CSV) file corresponding to that date. The dataset can be described as big data as it consists of 16 million records distributed over 80 features which cover: attack type, time stamp, protocols, and number, in addition to 76 other features which are related to the typical flow and Traffic of data in a computer communication network such as flow duration, packet number, bytes number, size of the packet, etc. More details about the original dataset can be found in [13, 14].

The dataset was sampled as a representative sample of the original data. The sampled dataset consists of 1,359 records. It covers three types of network attacks: (1) DDOS LOIC-UDP attacks; (2) SQL Injection attacks; (3) Brute-Force Web attacks in addition to Benign Traffic.

V. Methodology

The method applied in this study consists of five stages that correspond to the typical phases of popular data mining process models [2, 44], which cover: (1) Data acquisition, (2) Data preprocessing, (3) Data exploration, (4) Model construction; and (5) Model evaluation. Fig. 1 illustrates the applied research method and its involved five stages.

A. Data Acquisition

The data acquisition procedures involve obtaining the dataset by accessing, downloading, and storing it in the proper file format. The dataset is stored on Amazon AWS and was obtained using the AWS CLI tool [12].

B. Data Preprocessing

Due to the vast number of records in the dataset, which consists of 16 million records, the dataset must be treated as big data. The data needs intensive preprocessing procedures, which involve data filtering, randomization, sampling, and combining to construct a representative and informative dataset which can be used to construct useful models that can achieve excellent performance while avoiding both under-fitting and over-fitting through achieving balance in class distribution [5].

C. Data Exploration

Data exploration aims at prospecting the dataset and examining its quality, distribution, and potential toward achieving the desired machined learning objectives.

The data exploration procedures involve investigating and visualizing the dataset distribution to confirm the sufficiency of the dataset in each predicted class and to ensure the balance of samples in each class.

The relationship between variables is also visualized and examined using projection plots to uncover relationships between the data set features. The data exploration also involves assessing the importance of dataset features and their contribution toward enhancing the power of the classifier's prediction. Applied variable importance algorithms include the popular information gain (IG) and Gini algorithms.

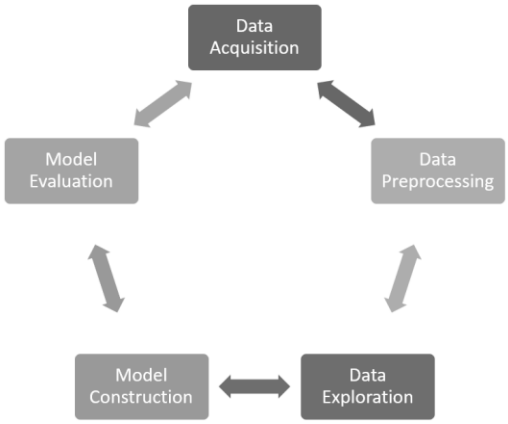

Fig. 1. The five stages of the applied research method.

D. Model Construction

The model construction phase will involve building four prediction models using four classification algorithms which include (1) Random Forest; (2) Logistic Regression; (3) CN2; and (4) Neural Networks.

E. Model Evaluation

The model evaluation phase involves scoring the performance of all the constructed classification models using Classification Accuracy (CA), Area Under the Curve (AUC), and F1 metrics [7, 45]. The equation for calculating the classification accuracy (CA), Precision, Recall, and F1 are described by Equations 1, 2, 3, and 4.

$$\text{Classification Accuracy (CA)} = TP+TN/N \quad (1)$$

$$\text{Precision} = TP/(TP+FP) \quad (2)$$

$$\text{Recall} = TP/(TP+FN) \quad (3)$$

$$F1 = 2TP/2TP+FP+FN \quad (4)$$

Where TP represents the number of samples classified as belonging to the assigned class, TN represents the number of samples classified as not belonging to the assigned class. N is the total number of samples.

In addition to constructing a confusion matrix [9] for each successful model, the performance of all models is visualized and confirmed using the Lift, Calibration, and ROC curves [10].

VI. Results

A. Data Acquisition Results

The CSE-CIC-IDS2018 dataset [13] was downloaded using the AWS CLI tool from the Amazon AWS website [12]. The dataset is managed by the Canadian Institute of Cybersecurity (CIC) [14]. The data was exported and stored in 10 CSV files. Each file was labeled with a name that represents the data acquisition date.

B. Data Preprocessing Results

The data processing procedures involved combining the dataset into one file and then filtering the dataset to contain the dataset records that correspond only to the three classes of attacks considered in this study in addition to a benign class: and excluding all other records.

The resulting dataset was filtered once again and then spitted into four datasets, each representing only one attack classification to the benign class. Each of the four datasets was stored in a separate CSV file which was then loaded and sampled using a stratified random method that involved dividing the dataset into several homogeneous groups. The size of each sample size is a maximum number of 400 records. This number was set to tackle the dataset's size complexity due to the Computer's limited power in this experiment.

The four resulting datasets were then randomized and then combined in a single dataset that was stored again in another CSV file which contains a total of 1359 records, where 400 records represent each of the DDOS LOIC-UDP, Brute Force Web, and Benign classes, and 159 records represent the entire dataset recorded for the SQL Injection attack class.

C. Data Exploration Results

The data exploration involved examining the dataset quality, its trends and distribution, and finding the correlation and association between the dataset features.

The sampled dataset consists of 1,359 samples distributed over four classes. Each class contains 400 samples, except the SQL Injection, which contains only 159 classes, representing 100% of the samples recorded in the original dataset. The sampled dataset has n and use and no significant outliers. Fig. 2 illustrates the distribution of the dataset over the four assigned classes.

The dataset trends were analyzed using the data projection method, which involves projecting the data samples over four selected dimensions. The projection results show a considerable influence on the time feature and the packet lengths, as shown in Fig. 3. This result was consistent with the variable importance calculated based on the Information Gain and Gini.

The variables were also ranked using Gini and Information Gain (IG) algorithms. Both algorithms agreed on ranking the top four important features, including Fwd Pkt Len Max, Tot Len Fwd Pkts, Subflow Fwd Byts, and Fwd Header Len.

The Gini algorithm ranked the Timestamp feature as number nine, while information ranked it as a number. On the other hand, while Gini ranked the number of the forwarded bytes sent in the initial window as number seven, the Information Gain algorithm ranked it as number nine. Analyzing the variable's importance ranking results was useful in prospecting the dataset's potential in predicting the attack classes. Table I ranks the top-ten features based on Gini and Information Gain variable importance ranking algorithms.

TABLE I. Top-Ten Variable Importance Ranking

#	GINI Ranked Feature	Score	Information Gain Ranked Feature	Score
1	Fwd Pkt Len Max	0.796	Fwd Pkt Len Max	1.56
2	TotLen Fwd Pkts	0.72	TotLen Fwd Pkts	1.43
3	Subflow Fwd Byts	0.72	Subflow Fwd Byts	1.43
4	Fwd Header Len	0.72	Fwd Header Len	1.36
5	**Fwd Pkt Len Mean**	0.70	*Timestamp*	1.33
6	Fwd Seg Size Avg	0.70	**Fwd Pkt Len Mean**	1.30
7	***Fwd Win Byts***	0.68	Fwd Seg Size Avg	1.30
8	Pkt Len Max	0.68	Pkt Len Max	1.29
9	*Timestamp*	0.66	***Fwd Win Byts***	1.26
10	Tot Fwd Pkts	0.62	Tot Fwd Pkts	1.22

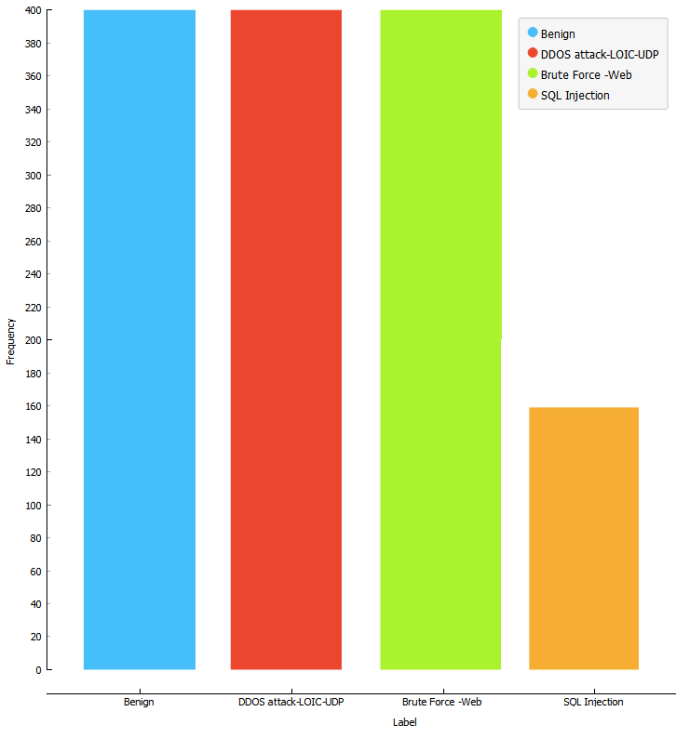

Fig. 2. Distribution of dataset records over the selected four classes.

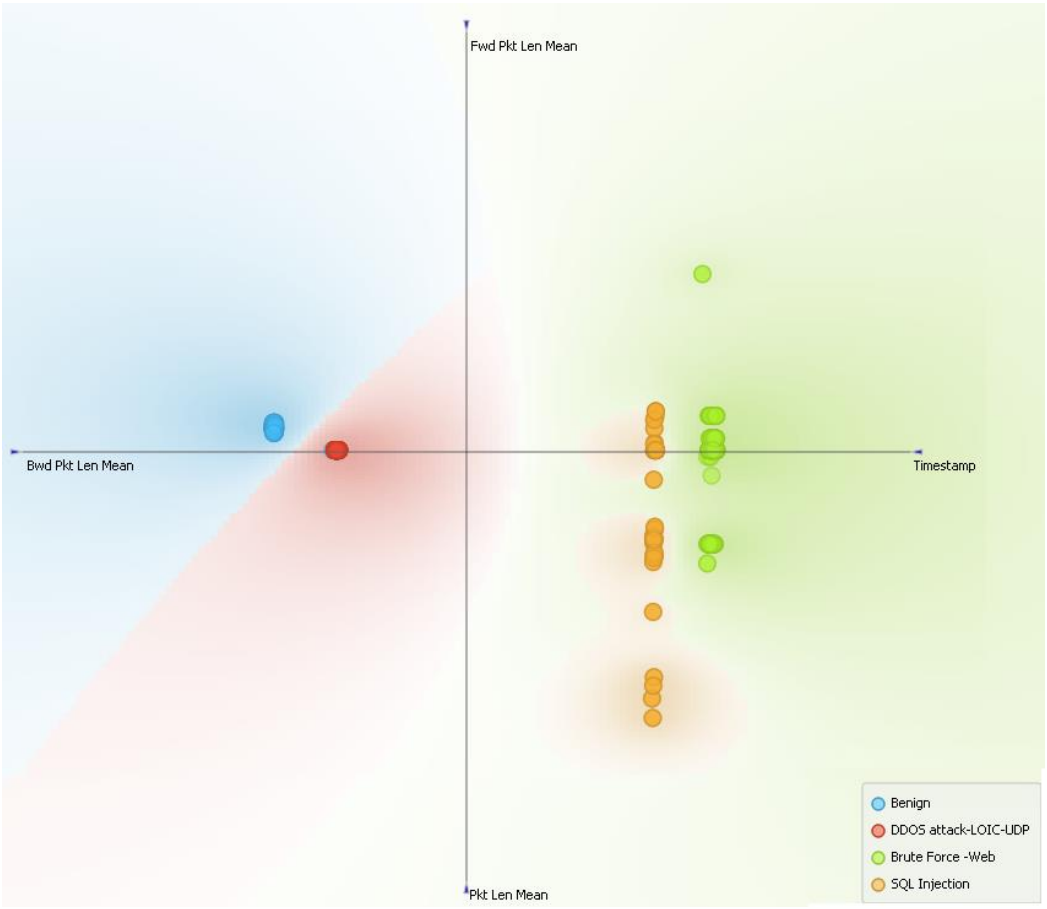

Fig. 3. An example of samples projection over an asset of four features.

D. Model Construction Results

Four models have been constructed in this study using four classification algorithms which include: Neural Networks, CN2, Logistic Regression, and Random Forest. The constructions of the Logistic Regression and Random Forest were the fastest, while the construction of the neural networks was the slowest, and the CN2 model was the second slowest.

E. Model Evaluation Results

The four created models were evaluated using three performance metrics: Classification Accuracy (CA), Area under the Curve (AUC), and F1.

The Random Forest model performed best with a CA score of 98%, an AUC score of 99%, and an F1 score of 98%. The Logistic Regression model scored the second-best performance, scoring 90% in the CA metrics, 98% in the AUC metrics, and 91% in the F1 metrics.

The CN2 achieved satisfactory results with a CA performance of 70%, an AUC performance of 94%, and an F1 performance of 63%, while the neural network model failed to achieve satisfactory results. Table II shows a comparison between the performances of the four constructed models.

The confusion matrices of the three successful models confirm the validity of the models for predicting the classification of all classes except the CN2 model, which failed to predict the Benign class. At the same time, it performed excellently in predicting the three other classes.

The confusion matrix of the CN2 model is illustrated in Table III. It shows that it performed well in predicting all attacks but poorly in predicting benign Traffic. On the other hand, its confusion matrix is illustrated in Table IV; despite the excellent performance of the Logistic Regression model in predicting Benign Traffic, Brute-Force Web, SQL Injection, and DDOS attacks. Shows its inferior performance in predicting Brute-Force Web attacks. The confusion matrix of the Random Forest model shown in Table V was the best, as the model performed excellently in predicting all classes.

TABLE II. CLASSIFICATION MODELS PERFORMANCE

Model	AUC	CA	Precision	Recall	F1
Random Forest	0.99	0.98	0.98	0.98	0.98
Logistic Regression	0.98	0.90	0.94	0.90	0.91
CN2 Rule Inducer	0.94	0.70	0.82	0.71	0.63
Neural Network	0.50	0.27	0.27	0.28	0.27

TABLE III. CN2 MODEL CONFUSION MATRIX

		Predicted				
		Benign	**DDOS attack-LOIC-UDP**	**Brute Force -Web**	**SQL Injection**	**Sum**
Actual	**Benign**	**4**	1	**49**	346	**400**
	DDOS attack-LOIC-UDP	1	**399**	0	0	**400**
	Brute Force -Web	0	0	**298**	2	**400**
	SQL Injection	0	0	4	**159**	**159**
	Sum	**5**	**400**	**447**	**507**	**1359**

TABLE IV. LOGISTIC REGRESSION CONFUSION MATRIX

		Predicted				
		Benign	**DDOS attack-LOIC-UDP**	**Brute Force -Web**	**SQL Injection**	**Sum**
Actual	**Benign**	**399**	0	1	0	**400**
	DDOS attack-LOIC-UDP	0	**399**	0	0	**400**
	Brute Force -Web	0	0	**275**	125	**400**
	SQL Injection	0	0	4	**155**	**159**
	Sum	**399**	**399**	**281**	**280**	**1359**

TABLE V. RANDOM FOREST CONFUSION MATRIX

		Predicted				
		Benign	**DDOS attack-LOIC-UDP**	**Brute Force -Web**	**SQL Injection**	**Sum**
Actual	**Benign**	**398**	0	1	0	**400**
	DDOS attack-LOIC-UDP	0	**400**	1	0	**400**
	Brute Force -Web	0	0	**385**	15	**400**
	SQL Injection	0	0	3	**156**	**159**
	Sum	**399**	**399**	**281**	**280**	**1359**

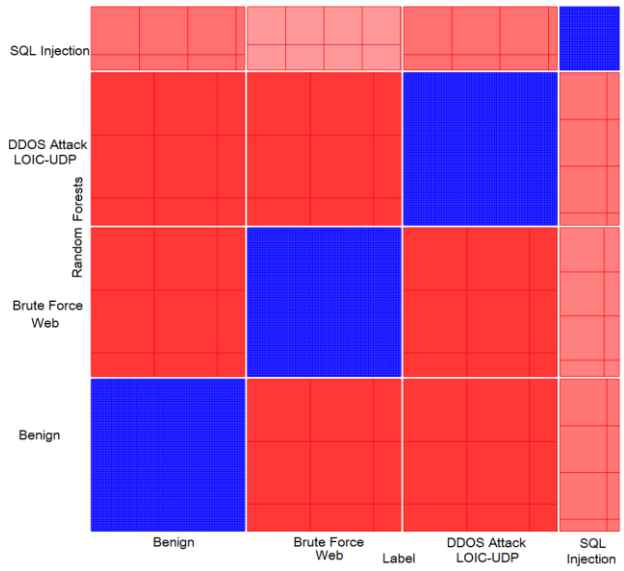

Fig. 4. An example sieve plot that shows the performance of the random.

A sieve plot was constructed for the Random Forest model to visualize the model performance, shown in Fig. 4. The correctly classified samples are represented by blue rectangles. In contrast, the wrongly classified samples are shown in red colors. The size of the rectangles corresponds to the size of the classified samples.

The Calibration curve, shown in Fig. 5 also confirms the validity and robustness of the constructed models. The closest the curve to the logistic function curve is, the better. While the Random Forest and Logistic Regression both show excellent performance, the performance of the CN2 model is relatively modest. In contrast, the performance of the Neural Network model was inferior as it appears as a straight flat line in the plot.

The Lift curve shows the relation between the predicted positive samples and those positive. The Lift curve in Fig. 6 confirms the validity of the Random Forest and Logistic Regression models. They both have excellent curves, and while the CN2 model shows a fluctuating curve, the neural network model performance was poor. This is demonstrated by their excellent lift curves showing the relationship between the predicted positive samples and those that are positive. While the CN2 model shows a fluctuating curve, the neural network model performance was inferior.

The ROC curve in Fig. 7 confirms the robustness and consistency of the performance of the constructed models, where the Random Forest model achieves the best performance. The region under its curve covers a large portion of the chart, followed by the Logistic Regression and CN2 model. However, the performance of the neural networks model was poor as its ROC curves pass through the baseline of the middle region, which indicates that its performance matches the performance achieved by a random model.

The region under the curve of the Random Forest model is the largest in the ROC chart, followed by the Logistic Regression and the CN2 models, respectively. The curve of the neural networks model was found to be poor as its performance curve passes through the baseline of the ROC, which matches the performance of a random stochastic model.

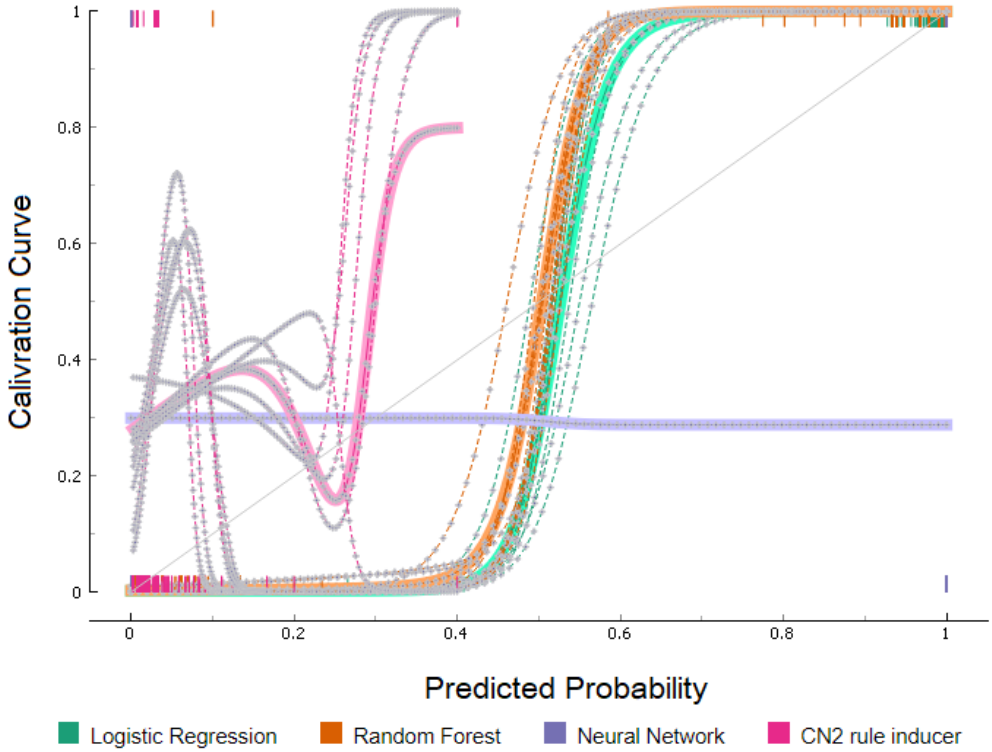

Fig. 5. Calibration curve shows the performance of the four constructed classification models.

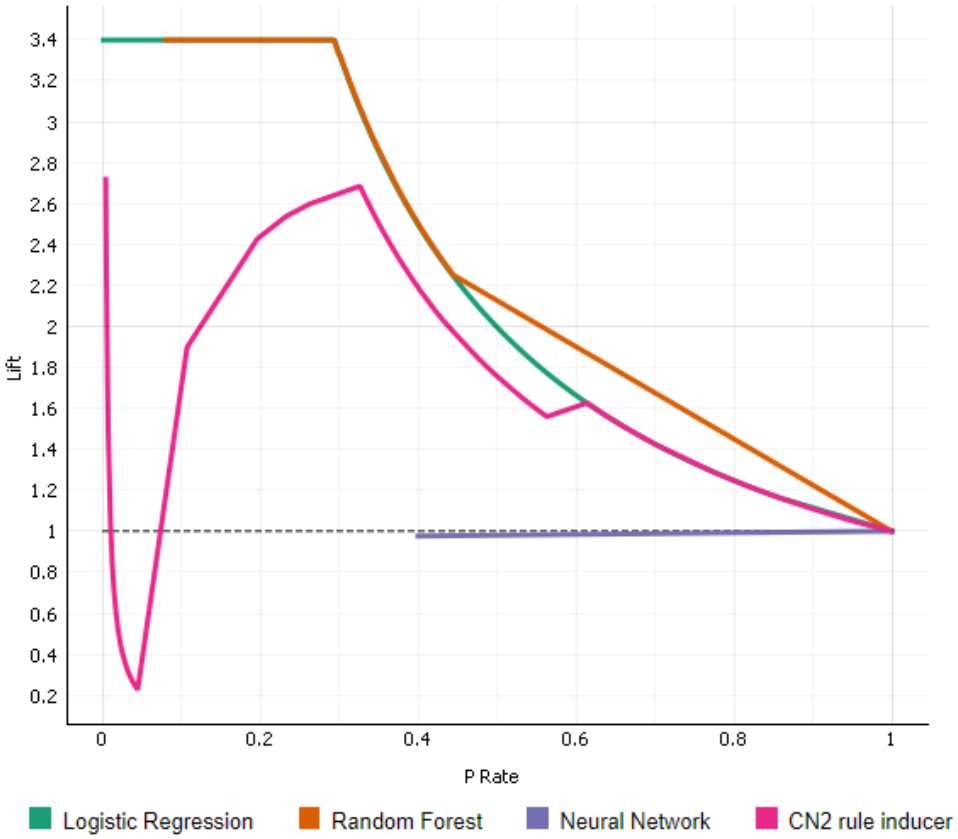

Fig. 6. A lift curve that shows the performance of the four constructed classification models.

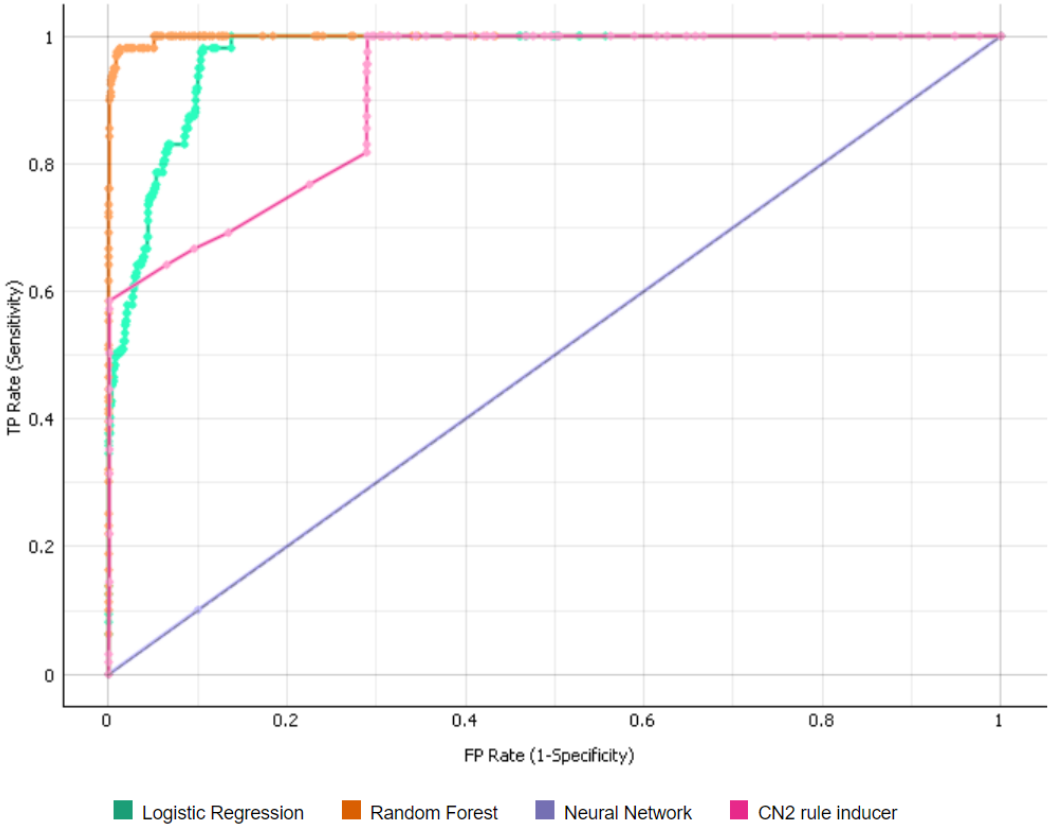

Fig. 7. The ROC curve of the constructed models.

VII. Discussion

The results of this study confirmed the validity of the applied machine learning algorithms for detecting and identifying three classes of network attacks and a benign class depending on several features related to computer traffic.

Furthermore, the variable importance ranking results conducted using GINI and Information Gain successfully identified Fwd Pkt Len Max, Tot Len Fwd Pkts, Subflow Fwd Byts, and Fwd Header Len. As the most prominent features for identifying network attacks. This result is consistent with the data exploration stage findings and the network security domain knowledge discussed in the literature [18, 46].

The Random Forest classifiers scored a CA score of 98%, while the Logistic Regression model scored a CA score of 90%. The Random Forest model achieved an AUC of 99%, while the Logistic Regression model achieved 98%. On the other hand, the CN2 model scored a modest CA performance of 70%, while the Neural Network model failed with a CA score of only 27%. The robustness of the Random Forest and Logistic Regression algorithms in creating the two most successful models was confirmed by the excellent performance shown in the confusion matrix for the two models and the results of the Lift and Calibration curves.

When comparing the results of this study with the results of other studies reported in the literature, in this respect, the results reported in this study outperformed all the excellent results reported in the surveyed literature. While most of the surveyed studies which achieved high CA Scores focused on identifying one or two types of network attacks. For example, the surveyed study reported in [15] aimed at detecting denial of service (DoS) attacks, while the study reported in [16] aimed at distinguishing benign Traffic from network attacks. The study reported in [30] aimed to distinguish botnets from infiltration attacks, while the study reported in [18] aimed to identify portrayal from botnet attacks. In comparison, the Random Forest model that was created in this work was successful in identifying four classes of network traffic: (1) Brute-Force Attacks; (2) Distributed Denial of Service Attacks (DDoS); (3) SQL Injection Attacks; and (4) Benign Traffic with an excellent 99% CA accuracy and 98 AUC.

In addition, the result of this study is quite significant when considering the type of dataset used in this study. This study was applied using a sample of the CSE-CIC-IDS2018 dataset, which is more challenging than the KDD Cup 99 that was used in some of the studies as reported in [15, 17] since CSE-CIC-IDS2018 is larger and it also has more features when compared to the KDD Cup 99 dataset.

However, the limitations of this study come from its dependence on using simulated data rather than real-world ones. In addition, the other important constraint in this study was the limited computational power of the standard PCs, which caused some issues related to the long execution time while experimenting.

VIII. Conclusion

This work has successfully investigated and evaluated the use of four machine learning algorithms: Random Forest, Logistic Regression, CN2, and Neural Networks for detecting and identifying three types of network traffic attacks: DDoS, Brute-Force Web, and SQL Injection, in addition to Benign Traffic.

The study provided a positive answer to the research question and successfully achieved the research objectives. Four machine learning algorithms were applied to a randomized sample of the CSE-CIC-IDS2018 dataset: Random Forest, Logistic Regression, CN2, and Neural Networks. Random Forest scored a CA score of 98%, while Logistic Regression scored 90%. Random Forest scored 99% in the AUC metric, while Logistic Regression scored 98%.

The results obtained in this study contribute towards solving some of the most important problems in computer network traffic and cyber security. These contributions can be summarized as (1) Creating successful machine learning models that can be deployed to detect and identify three types of network attacks based on network traffic data; (2) Identifying significant network traffic features that can be used as predictors for providing fast, accurate and reliable detection and identification of network attacks. These contributions can contribute towards developing solutions that help for preventing, monitor, and mitigate harmful computer network attacks, which affect the reliability, efficiency, and availability of the services provided by computer networks.

The practical use of the successful results that are reported in this study implies deploying the two most successful models reported in this study: Random and Logistic Regression, by embedding them in a network router, security suit, proxy, or firewall system in order to detect, identify or filter network traffic that creates a potential threat to the network.

Future work could be conducted to cover more machine learning techniques and more types of network attacks. In addition, a more real-world dataset can also be used rather than depending only on a simulated one. In addition, more powerful computers can also be used to conduct the same or a comprehensive study on the entire dataset rather than on a sample of it.

References

[1] U. Cisco, "Cisco annual internet report (2018–2023) white paper," CISCO Public, vol. 10, 2020.

[2] A. Banimustafa and N. Hardy, "A Scientific Knowledge Discovery and Data Mining Process Model for Metabolomics," IEEE Access, vol. 8, pp. 209964-210005, 2020.

[3] A. BaniMustafa, "Predicting Software Effort Estimation Using Machine Learning Techniques," in 2018 8th International Conference on Computer Science and Information Technology (CSIT), Amman, 2018, pp. 249-256: IEEE.

[4] A. H. BaniMustafa and N. W. Hardy, "A strategy for selecting data mining techniques in metabolomics," in Plant Metabolomics, N. Hardy and R. Hall, Eds.: Springer, 2011, pp. 317-333.

[5] A. BaniMustafa, "Enhancing learning from imbalanced classes via data preprocessing: A data-driven application in metabolomics data mining," ISeCure, vol. 11, no. 3, pp. 79-89, 2019.

[6] E. Y. Güven, S. Gülgün, C. Manav, B. Bakır, and Z. G. J. E. Aydın, "Multiple Classification of Cyber Attacks Using Machine Learning," vol. 22, no. 2, pp. 313-320, 2022.

[7] C. X. Ling, J. Huang, and H. Zhang, "AUC: A Better Measure than Accuracy in Comparing Learning Algorithms," in Advances in Artificial Intelligence, Berlin, Heidelberg, 2003, pp. 329-341: Springer Berlin Heidelberg.

[8] M. J. Zaki, W. Meira Jr, and W. Meira, Data mining and analysis: fundamental concepts and algorithms. Cambridge University Press, 2014.

[9] R. Susmaga, "Confusion Matrix Visualization," in Intelligent Information Processing and Web Mining, Berlin, Heidelberg, 2004, pp. 107-116: Springer Berlin Heidelberg.

[10] M. Vuk and T. Curk, "ROC Curve, Lift Chart and Calibration Plot," Metodolo ški zvezki, vol. 3, no. 1, pp. 89-108, 2006.

[11] A. Ferriyan, A. H. Thamrin, K. Takeda, and J. Murai, "Generating Network Intrusion Detection Dataset Based on Real and Encrypted Synthetic Attack Traffic," Applied Sciences, vol. 11, no. 17, 2021.

[12] T. C. I. f. C. (CIC). (2018, 15/10/2022). A Realistic Cyber Defense Dataset (CSE-CIC-IDS2018). Available: https://registry.opendata.aws/cse-cic-ids2018.

[13] C. I. f. C. (CIC). (2018, 15/10/2022). CSE-CIC-IDS2018 on AWS: A collaborative project between the Communications Security Establishment (CSE) & the Canadian Institute for Cybersecurity (CIC). Available: https://www.unb.ca/cic/datasets/ids-2018.html.

[14] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "Toward generating a new intrusion detection dataset and intrusion traffic characterization," presented at The International Conference on Information Systems Security and Privacy (ICISSp), Funchal, Madeira, Portugal, 2018.

[15] CNN-based network intrusion detection against denial-of-service attacks, 9, 2020.

[16] M. Andrecut, "Attack vs Benign Network Intrusion Traffic Classification," arXiv preprint arXiv:.07323, 2022.

[17] D. M. Farid, J. Darmont, N. Harbi, H. H. Nguyen, and M. Z. Rahman, "Adaptive network intrusion detection learning: attribute selection and classification," in International Conference on computer systems Engineering (ICCSE 2009), Bangkok, Thailand, 2009, p. TH60000: World Academy of Science, Engineering and Technology (WASET).

[18] V. Kanimozhi and T. P. Jacob, "Artificial Intelligence outflanks all other machine learning classifiers in Network Intrusion Detection System on the realistic cyber dataset CSE-CIC-IDS2018 using cloud computing," ICT Express, vol. 7, no. 3, pp. 366-370, 2021/09/01/ 2021.

[19] A. A. Ghorbani, W. Lu, and M. Tavallaee, Network intrusion detection and prevention: concepts and techniques. Springer Science & Business Media, 2009.

[20] R. Hofstede, M. Jonker, A. Sperotto, A. Pras, and s. management, "Flow-based web application brute-force attack and compromise detection," Journal of network, vol. 25, no. 4, pp. 735-758, 2017.

[21] C. Adams, G.-V. Jourdan, J.-P. Levac, and F. Prevost, "Lightweight protection against brute force login attacks on web applications," in 2010 Eighth International Conference on Privacy, Security and Trust, 2010, pp. 181-188: IEEE.

[22] C. Douligeris and A. Mitrokotsa, "DDoS attacks and defense mechanisms: classification and state-of-the-art," Computer networks, vol. 44, no. 5, pp. 643-666, 2004.

[23] A. Chadd, "DDoS attacks: past, present and future," Network Security, vol. 2018, no. 7, pp. 13-15, 2018.

[24] L. K. Shar and H. B. K. Tan, "Defeating SQL Injection," Computer, vol. 46, no. 3, pp. 69-77, 2013.

[25] W. G. Halfond, J. Viegas, and A. Orso, "A classification of SQL-injection attacks and countermeasures," in Proceedings of the IEEE international symposium on secure software engineering, 2006, vol. 1, pp. 13-15: IEEE.

[26] M. Baklizi et al., "A Technical Review of SQL Injection Tools and Methods: A Case Study of SQLMap," vol. 10, no. 3, pp. 75-85, 2022.

[27] A. Almomani et al., "An enhanced online phishing e-mail detection framework based on evolving connectionist system," vol. 9, no. 3, pp. 169-175, 2013.

[28] A. L. Samuel, "Some Studies in Machine Learning Using the Game of Checkers," IBM Journal of Research and Development, vol. 3, no. 3, pp. 210-229, 1959.

[29] L. Breiman, "Random forests," Machine learning, vol. 45, no. 1, pp. 5-32, 2001.

[30] A. Cutler, D. R. Cutler, and J. R. Stevens, "Random forests," in Ensemble machine learning: Springer, 2012, pp. 157-175.

[31] L. Breiman, "Random Forests," Mach. Learn., vol. 45, no. 1, pp. 5-32, 2001.

[32] M. Choubisa, R. Doshi, N. Khatri, and K. K. Hiran, "A Simple and Robust Approach of Random Forest for Intrusion Detection System in Cyber Security," in 2022 International Conference on IoT and Blockchain Technology (ICIBT), 2022, pp. 1-5: IEEE.

[33] T. Wu, H. Fan, H. Zhu, C. You, H. Zhou, and X. J. E. J. o. A. i. S. P. Huang, "Intrusion detection system combined enhanced random forest with SMOTE algorithm," vol. 2022, no. 1, pp. 1-20, 2022.

[34] N. S. Bhati and M. Khari, "An Ensemble Model for Network Intrusion Detection Using AdaBoost, Random Forest and Logistic Regression," in Applications of Artificial Intelligence and Machine Learning: Springer, 2022, pp. 777-789.

[35] B. Yogesh, G. S. J. T. J. o. C. Reddy, and M. Education, "Intrusion Detection System using Random Forest Approach," vol. 13, no. 2, pp. 725-733, 2022.

[36] R. E. Wright, "Logistic regression," in Reading and understanding multivariate statistics.Washington, DC, US: American Psychological Association, 1995, pp. 217-244.

[37] P. Kanimozhi, T. J. C. Aruldoss Albert Victoire, C. Practice, and Experience, "Oppositional tunicate fuzzy C-means algorithm and logistic regression for intrusion detection on cloud," vol. 34, no. 4, p. e6624, 2022.

[38] P. Clark and T. Niblett, "The CN2 induction algorithm," Machine learning, vol. 3, no. 4, pp. 261-283, 1989.

[39] N. Kumar, U. Kumar, and Applications, "Comparative analysis of CN2 rule induction with other classification algorithms for network security," Multimedia Tools, vol. 81, no. 26, pp. 37119-37135, 2022.

[40] J. A. Anderson, An introduction to neural networks. MIT press, 1995.

[41] C. M. Bishop, "Neural networks and their applications," Review of scientific instruments, vol. 65, no. 6, pp. 1803-1832, 1994.

[42] J. Wei, Y. Chen, Y. Lai, Y. Wang, and Z. J. I. C. L. Zhang, "Domain adversarial neural network-based intrusion detection system for in-vehicle network variant attacks," vol. 26, no. 11, pp. 2547-2551, 2022.

[43] A. Rosay, K. Riou, F. Carlier, and P. J. A. o. T. Leroux, "Multi-layer perceptron for network intrusion detection," vol. 77, no. 5, pp. 371-394, 2022.

[44] A. BaniMustafa, "A Knowledge Discovery and Data Mining Process Model for Metabolomics," PhD, Computer Science Dept., University of Wales, Aberystwyth Aberystwyth, 2012.

[45] J. Novakovic et al., "Evaluation of Classification Models in Machine Learning," vol. 7, pp. 39-46, 2017.

[46] A. Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman, "Survey of intrusion detection systems: techniques, datasets, and challenges," Cybersecurity, vol. 2, no. 1, 2019.