Machine learning classification-based portscan attacks detection using decision table

Mahdi Nsaif Jasim, Ali Munther Abdul Rahman, Muthanna Jabbar Abdulredhi
College of Business Informatics, University of Information Technology and Communications, Baghdad, Iraq

Article Info

Article history:

Received Oct 2, 2022
Revised Oct 29, 2022
Accepted Nov 2, 2022

Keywords:

CICIDS2017
Data mining
Decision table
Feature selection
Machine learning
Network security
OneR

ABSTRACT

Port scanner attackers are typically used to identify weak points or vulnerabilities in an organization's network. When attackers send a detective message to a port number, the response tells them whether the port is open and assists them in identifying potential vulnerabilities. However, machine-learning approaches are the most effective techniques for detecting and identifying port scanner attacks. This attack is regarded as one of the most dangerous internet threats. This research aims to strengthen the detection accuracy and reduce the detection time. Tagged network traffic data sets are used to train the classification machine learning techniques. On the other hand, network traffic analysis is used by unsupervised method to detect attacks. This study modifies the decision table and OneR classification algorithms as a supervised technique for portscan detection. The proposed algorithm uses the CICIDS2017 dataset for both training and testing. The proposed hybrid feature selection methods use and apply multiple training and testing through a sequence of experiments, the proposed method is capable of detecting the portscan attack with 99.8% accuracy, which is competitive in addition to the proposed combination's fast response.

Corresponding Author:

Mahdi Nsaif Jasim
College of Business Informatics, University of Information Technology and Communications
Baghdad, Iraq
Email: mahdinsaif@uoitc.edu.iq

1. INTRODUCTION

Cyber security can be defined as the safeguarding, resisting, and releasing of all resources that consume the target machine's power. Cyber-attacks are malicious attempts to destroy and infiltrate organizational or personal secret data [1], [2]. This attack cripples the targeted machines function by overloading their resources and let them out of service. One method used by attackers to accomplish this is to flood the network with bogus requests. Scanning attacks are carried out using the communication protocols such as user datagram protocol (UDP), transmission control protocol (TCP), internet control message protocol (ICMP), stream control transmission protocol (SCTP), and file transfer protocol (FTP), among others. Attackers use faults in these protocols to learn about endpoint issues. To determine which ports are attractive to vulnerabilities, port scanners often send large packets with a specific set of flags to a large number of ports on the victim machine. Basic threshold approaches, such as the secondary heuristic analysis for defensive online warfare (SHADOW) IDS, can identify such scans [3].

Data mining has been used to create advanced intrusion detection systems since the 1990s. In general, both data mining and machine learning techniques are usually implemented in the next four processes Preprocessing, mining, transformation, and interpretation) which are the main steps in the learning process [4], [5]. These three crucial procedures are the most difficult of all the methods for detecting intrusions via data mining.

Machine learning-based portscan recognition algorithms in use. Supervised machine learning (SML) techniques that construct the detection model from generated and labeled network traffic datasets. The supervised approaches must cope with two major issues. To begin, creating labeled datasets of network traffic takes a significant amount of time and computational capacity. SML approaches cannot anticipate novel activities that are both safe and dangerous without regular model upgrades. Semi-supervised ML classifiers perform poorly when there is a high volume of anomalous data flow of any network under consideration. In contrast to the first category, the second category does not require a labeled dataset to create the detection process. The fundamental issue with unsupervised approaches is that they produce a large number of false positives (FP). The multidimensionality challenge complexity [6] makes it not easy for supervised approaches to find portscan accurately [7]. SML ideas use supervised techniques since they can work on labeled class datasets. Machine learning is one of the most important approaches available today for employing a soft computing approach to identify optimal solutions to a wide range of real-world problems. Cyber security is no exception, and academics are using a number of machine learning-based techniques to solve the challenges of cyber threats and develop intrusion detection solutions.

In briefly, there are two main types of machine learning: supervised and unsupervised learnings. Supervised machine learning algorithms are used when there is labeled data target values used to find responses for the new data with unknown output. two main components of supervised learning are classification/ prediction and optimization. The first is categorization which is used for discrete output and the second is the forecast which is used for continuous output. The latter category includes machine learning algorithms that lead to evolutionary computing for final outputs or other supporting solutions like feature selection [8].

Several approaches for detecting portscan attacks have been proposed, including [9]–[11]. Machine learning techniques are the ones that the most published papers that forming a research trend in the current days. Table 1 gives a quick overview of some current portscan detection research and developments.

Table 1. Recent related works

No	Authors	Results Discussion
1	[12]	Network administrators are increasingly in need of information that will assist them in detecting future assaults. In this work, the authors employed logistic regression to detect Port Scan assaults and used data balancing strategies to achieve better results.
2	[13]	This study proposes a novel comprehensive discovery scheme for identifying port scan attacks that compares five supervised machine learning classifiers: LogisticRegression, DecisionTrees, linear/quadratic discriminant, NaiveBayes, and Ensemble BoostedTrees. The authors studied the detection accuracy of various techniques for port scanning attacks using a current dataset (PSA-2017).
3	[14]	The goal of this research is to identify and stop DDoS attacks. For the purpose of detecting DDoS attacks, a variety of data mining techniques, including Jrip, J48, and k-NN, have been used. For each method, a thorough evaluation of its performance in this area is conducted before implementation. Utilizing the most recent dataset CICIDS2017, the provided work has been assessed.
4	[15]	This study suggests using a photonic neuromorphic lookaside accelerator to perform real-time traffic inspection. This will allow us to identify port-scanning attacks, which are a sign of DDoS attacks.
5	[16]	In this research, A deep learning (DL) based model trained on CICIDS2017 dataset employing a convolutional neural network (CNN) to classify Port scan attempts. For selecting the best features, DL models have been combined with feature selection methods including recursive feature elimination (RFE) and Fisher score. To investigate the impact of dimensionality reduction, experiments are conducted with various values for the ideal number of features.
6	[17]	Introduced a detection solution for internet of thing (IoT) device scanning and reconnaissance attacks in this paper that is based on deep neural networks. The suggested approach was put into use and demonstrated extremely high accuracy, topping 98%. Additionally, experiments revealed a 1.9% false-positive rate and a false-negative rate less than 0.02%.
7	[18]	This paper proposes a network traffic flow-based approach for mobile malware detection in which each HTTP flow is treated as a document and HTTP flow requests are analyzed using natural language processing string analysis. The N-Gram line generation, feature selection approach, and SVM algorithm are used to develop an effective malware detection model.
8	[19]	The features of Packet-In messages transmitted from the OpenFlow (OF) switch to the controller are taken into account when a port scan detection approach is proposed in this paper. In comparison to traditional polling methods, this enables rapid detection and with minimal overhead. Real and simulated traffic data were used in the evaluation. The suggested method can detect port scans with less overhead than the current methods, according to the results.
9	[20]	The authors demonstrate how to detect distributed denial of service (DDoS) attacks using the entropy value of the destination IP address. The proposed solution is implemented using the OpenFlow protocol's (OFP) flexibility and an OpenFlow controller (POX).
#	Our Proposed	1- CICIDS2017 dataset for training and testing. 2- Hybrid feature selection approaches proposed 3- Create a suitable model using the decision table and OneR algorithms. 4- Evaluation.

One of the most popular cyber-attacks is the port scanning attack in which an attacker sends inspection packets with different port numbers to scan available server to find open ports on a network. As a result, numerous detection/prevention strategies have been developed to counteract such cyber-attacks. So, the fundamental purpose of this work is to find an appropriate strategy for detecting portscan assaults using SML and a worldwide attack dataset. In addition to identifying the best influential classifier model for use in offensive classification. Some of the advantages of the proposed approach over previous detection systems based on SML methods are as follows:

a) Labelled datasets are required to train detection models using the SML algorithms.
b) A hybrid feature selection method is proposed that employs both low variance filtering and information gain rationing strategies.
c) The present model can be classified as portscan and regular to aid in their online implementation for traffic classification.

The remaining sections of this work are summarized below. The limits of related efforts in portscan attack detection are discussed. Section 2 presents our detection model, which is based on a supervised classification method. Following a discussion of the significance of the experiments' results and analysis, the report finishes with recommendations for out several.

2. PROPOSED METHOD

Description of the used dataset is done at the beginning. Figure 1 shows the main processes of the proposed system. The proposed system exposes a new technique for intrusion detection of portscan attack based on the classification algorithms OneR and decision table. Finally, the findings are examined, performance of the proposed algorithms are evaluated.

2.1. The dataset description

The CICIDS2017 dataset has been used by so many researchers for analysis and development of novel models and algorithms since its inception. The CICIDS2017 dataset was made up of eight different files that each contained five days of normal and assault traffic data. Researchers in [21] propose the CICIDS2017 to circumvent the lack of IDS datasets that fulfill real-world network traffic characteristics [22]. CICIDS2017 [23], the largest and most often used dataset [24], is the valid dataset. The dataset consists of 84 features represent both regular and malicious traffic as class. The Canadian Institute of Cyber Security's CICIDS2017 dataset was made up of eight different files covering five days of normal and attack traffic data.

2.2. The decision table classification algorithm

Decision table is an ordered set of If-Then rules that has the potential to be more compact and hence more intelligible than decision trees and is an accurate method for numeric prediction from decision trees. The decision-table-based approach was chosen because it is a simpler, less computationally costly algorithm than the decision-tree-based approach [25]. It analyses feature subsets using best-first search and can do cross-validation. Based on the same set of features, an option determines the class for each instance that is not covered by a decision table entry using the nearest-neighbor approach rather than the table's global majority.

2.3. The OneR classification algorithm

The OneR based classifier (OneR) is known as the "One Rule" rule learner algorithm. It is a straightforward categorization technique that generates a one-level decision tree. From a group of cases, OneR may deduce simple and valid classification rules. OneR can also handle missing values and numeric attributes, demonstrating flexibility despite its simplicity. For each attribute in the training data, the OneR algorithm generates one rule. It chooses the rule with the lowest mistake rate [26].

2.4. The techniques of feature selection

In order for a model to predict the target variable, feature selection methods aim to reduce the number of input variables to those that are thought to be most useful. When few features are used, that may lead to poor detection accuracy, but when there are many features may result in good detection accuracy at more time complexity and more resources overhead. The current research used dual appealing feature selection strategies; Figure 1 depicts the primary sketch of the proposed system.

2.4.1. The variance approach

The variance approach [27] is frequently used because of the nature of the attributes were integers, the variance was used to choose the features used in this work. The features with low variance are omitted because they are not discriminant features. Each feature variance (V) is calculated using (1).

$$\mathrm{V}\ (\sigma^2) = \frac{\sum_{i=1}^{n}(X_i-\mu)^2}{N} \tag{1}$$

While N is the whole numbers of the trials. While μ is all values average that are related to the feature. The feature values, denoted by X_i, are computed using a group of samples.

2.4.2. The information gain (IGR)

The researchers frequently utilize the features selection technique to determine the limits of an attribute's importance. By deducting the entropy value before separation from the entropy value after separation, the IGR [28]value is determined. Depending on this value, properties are either used or removed. For categorization, only the attributes that satisfy the weighting criteria will be considered. In this work, the information gain is utilized in cooperation with variance to precisely select the important features (2).

$$IGR(Y, A_j) = \frac{H(Y)-H(Y|A_j)}{H(A_j)} \tag{2}$$

Where Y refers to the class and A_j the *jth* feature. Entropy formula, *H (.)*, is denoted according to (3).

$$H(X) = -\sum_{i=1}^{n} p(x_i)\log p(x_i) \tag{3}$$

For example, taking the input, *P(.)* is the probability and *i* is an index of the probabilities.

2.5. The proposed portscan attack classification

Decision tables are one of the simplest hypothesis spaces and are usually simple to understand. Decision table creates a majority classifier for decision tables. This paper's proposed method employs supervised decision table to generate binary classifier incoming packets as either benign or attacks. Using the CICIDS2017 dataset as a starting point, we employ the decision table algorithm to detect the port scan attack. The proposed strategy comprises using labeled data to train the model and testing it on the same dataset using a 75:25 training and testing ratio. Figure 1 depicts the proposed system's block diagram

The main steps in the proposed method can be listed as follow:

a) The features selected utilizing hybrid feature selection techniques. The variance approach and information gain were utilized in this work to find the ideal set of characteristics. By using variance scores to neglect characteristics with low variance values less than 2.9. Furthermore, 13 selected features are produced by deleting the minimum the information gain weight features, which are less than 0.6, as demonstrated and stated in Table 2.

b) Create a suitable classifier model using the decision table and OneR algorithms. The suggested technique was trained using 75% of the CICIDS2017 dataset, while 25% of the dataset is utilized to assess the suggested method.

c) Make comparison of the proposed models' performance and the choose the best.

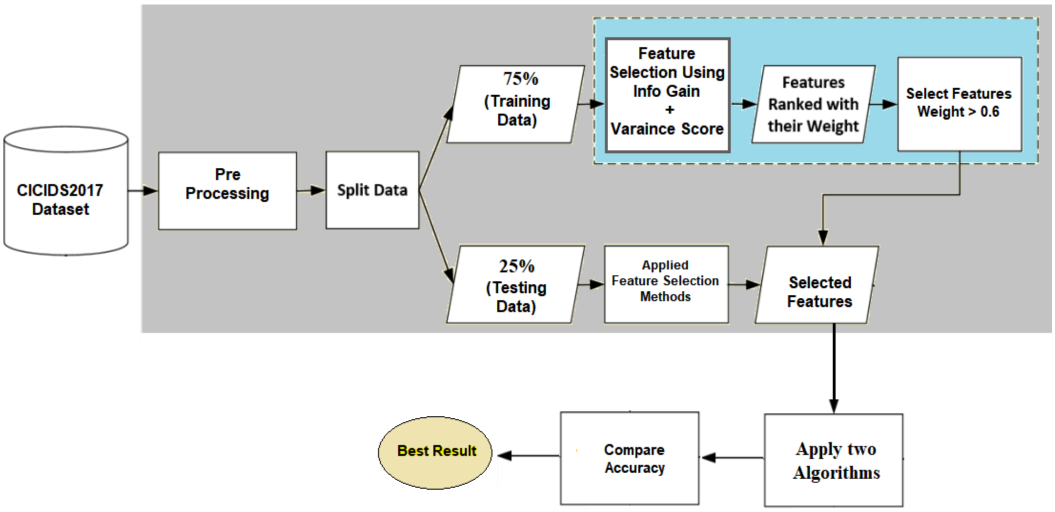
CICIDS2017 Dataset
Pre Processing
Split Data
75% (Training Data)
25% (Testing Data)
Feature Selection Using Info Gain + Varaince Score
Features Ranked with their Weight
Select Features Weight > 0.6
Applied Feature Selection Methods
Selected Features
Apply two Algorithms
Compare Accuracy
Best Result

Figure 1. The proposed framework

Table 2. The scores of features by IGR

No.	FeatureName	FeatureScore
1	TotalLengthofBwdPackets	0.939343
2	BwdPacketLengthMax	0.939343
3	BwdPacketLengthMin	0.80995
4	BwdPacketLengthMean	0.782456
5	MaxPacketLength	0.782456
6	PacketLengthMean	0.781841
7	PSHFlagCount	0.781841
8	AveragePacketSize	0.778016
9	AvgBwdSegmentSize	0.77582
10	SubflowBwdBytes	0.760317
11	Init_Win_bytes_backward	0.708411
12	act_data_pkt_fwd	0.706064
13	min_seg_size_forward	0.706064

3. RESULTS AND EVALUATION

In this experiment, the detection performance of the proposed methods was evaluated. WEKA's categorization and feature selection performance as measured by information gain. The accuracy of proposed algorithm represents a measure to its ability of detect the attacks. The accuracy of the algorithm can be calculated by using (4).

$$\text{Accuracy } \frac{TP+TN}{TP+TN+FP+FN} \tag{4}$$

The accuracy is used as measure of the proposed system performance. The algorithm's accuracy indicates its ability to estimate the traffic based on trained model. In other words, an algorithm's ability to precisely classify of the packets traffic into normal and portscan attack. The results of comparing the criteria measures of decision table and OneR are shown in Figure 2 and Table 3. As demonstrated in Table 3, the results of both algorithms are practically identical because both are capable of classifying traffic as normal or portscan attack.

Table 3. The results of comparing the criteria measures of both decision table and OneR

Algorithm	Accuracy	Recall	Precision	F-Measure
Decision table	99.82%	99.70%	99.90%	99.80%
OneR	99.57%	99.40%	99.60%	99.50%

The algorithms with the chosen features produce the best overall classifier performance, according to an analysis of the four-performance metrics the two classifiers obtained for the 13 features. The CICIDS2017 dataset's chosen attributes and use in this work are sufficient for recognizing portscan assaults by DesisionTable and OneR algorithms, according to experimental results as shown in Table 3. The proposed DesisionTable is better than the OneR algorithm, which achieved 99.60% of accuracy.

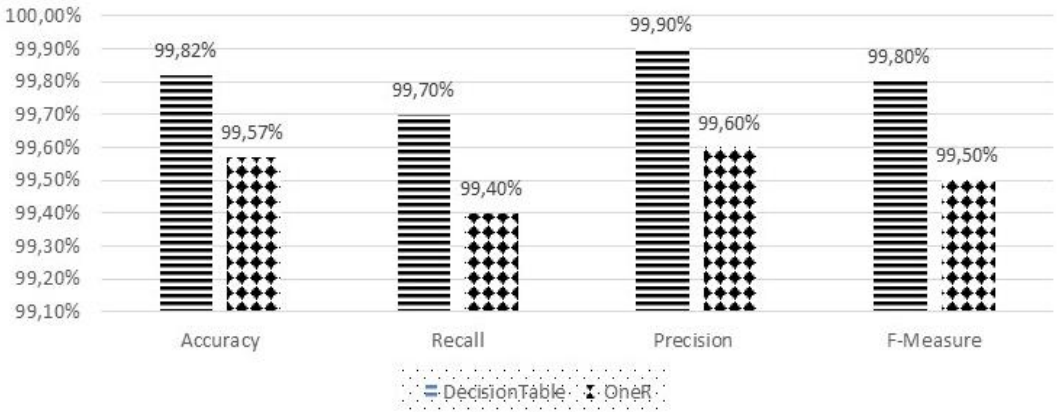

Figure 2. The performance of the proposed classifier

4. CONCLUSION AND FUTURE WORK

In this research, we use SML to identify traffic as normal or malicious. It begins with labeled traffic statistics extracted from the dataset. In the proposed framework, hybrid feature selection strategies are provided to reduce 84 features to 13 of the features that are used for the final classify of traffic packets. The decision table classification method can classify the traffic into normal and portscan attack after the successful training the algorithm on a labelled dataset. Both the ML models were trained and tested using the well-known dataset "CICIDS2017" which is famous as the current benchmark labelled datasets. As a suggestion the future work, its recommended to apply the proposed method in real environment usch software defined networking (SDN) or IoT. In addition, training and testing the proposed model on more recent dataset such as CICDDoS2019.

REFERENCES

[1] L. Li, W. He, L. Xu, I. Ash, M. Anwar, and X. Yuan, “Investigating the impact of cybersecurity policy awareness on employees’ cybersecurity behavior,” *Int. J. Inf. Manage.*, vol. 45, pp. 13–24, 2019, doi: 10.1016/j.ijinfomgt.2018.10.017.

[2] C. Douligeris and A. Mitrokotsa, “DDoS attacks and defense mechanisms: a classification,” in *Proceedings of the 3rd IEEE International Symposium on Signal Processing and Information Technology (IEEE Cat. No. 03EX795)*, 2003, pp. 190–193.

[3] “What is a distributed denial-of-service (DDoS) attack? | Cloudflare.” https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/ (accessed Jun. 18, 2022).

[4] K. Kalegele, K. Sasai, H. Takahashi, G. Kitagata, and T. Kinoshita, “Four decades of data mining in network and systems management,” *IEEE Trans. Knowl. Data Eng.*, vol. 27, no. 10, pp. 2700–2716, 2015, doi: 10.1109/TKDE.2015.2426713.

[5] W. I. D. Mining, “Data mining: Concepts and techniques,” *Morgan Kaufinann*, vol. 10, pp. 559–569, 2006.

[6] “Curse of Dimensionality - A ‘Curse’ to Machine Learning by Shashmi Karanam Towards Data Science.” https://towardsdatascience.com/curse-of-dimensionality-a-curse-to-machine-learning-c122ee33bfeb (accessed Jun. 19, 2022).

[7] P. Berkhin, “A survey of clustering data mining techniques,” in *Grouping multidimensional data*, Springer, pp. 25–71, 2006, doi: 10.1007/3-540-28349-8_2.

[8] M. Aamir, S. S. H. Rizvi, M. A. Hashmani, M. Zubair, and J. Ahmad, “Machine learning classification of port scanning and DDoS attacks: A comparative analysis,” *Mehran Univ. Res. J. Eng. Technol.*, vol. 40, no. 1, pp. 215–229, 2021, doi: 10.22581/muet1982.2101.19.

[9] M. I. Kareem and M. N. Jasim, “DDOS attack detection using lightweight partial decision tree algorithm,” in 2022 *International Conference on Computer Science and Software Engineering (CSASE)*, 2022, pp. 362–367, doi: 10.1109/CSASE51777.2022.9759824.

[10] M. I. Kareem and M. N. Jasim, “Fast and accurate classifying model for denial-of-service attacks by using machine learning,” *Bull. Electr. Eng. Informatics*, vol. 11, no. 3, pp. 1742–1751, 2022, doi: 10.11591/eei.v11i3.3688.

[11] M. I. Kareem and M. N. Jasim, “The current trends of DDoS detection in SDN environment,” in *2021 2nd Information Technology To Enhance e-learning and Other Application (IT-ELA)*, 2021, pp. 29–34, doi: 10.1109/IT-ELA52201.2021.9773744.

[12] C. A. C. Tojeiro, C. D. J. Reis, K. A. P. D. Costa, and T. J. Lucas, “Port scan identification through regression applying logistic testing methods to balanced data,” 2022, doi: 10.21203/rs.3.rs-1554916/v1.

[13] Q. A. Al-Haija, E. Saleh, and M. Alnabhan, “Detecting port scan attacks using logistic regression,” *2021 4th Int. Symp. Adv. Electr. Commun. Technol. ISAECT 2021*, 2021, doi: 10.1109/ISAECT53699.2021.9668562.

[14] S. D. Kebede, B. Tiwari, V. Tiwari, and K. Chandravanshi, “Predictive machine learning-based integrated approach for DDoS detection and prevention,” *Multimed. Tools Appl.*, vol. 81, no. 3, pp. 4185–4211, 2022, doi: 10.1007/s11042-021-11740-z.

[15] M. Kirtas *et al.*, “Early detection of DDoS attacks using photonic neural networks,” in *2022 IEEE 14th Image, Video, and Multidimensional Signal Processing Workshop (IVMSP)*, 2022, pp. 1–5, doi: 10.1109/IVMSP54334.2022.9816178.

[16] K. Singh, A. Mahajan, and V. Mansotra, “Using recursive feature elimination and fisher score with convolutional neural network for identifying port scan attempts,” in *Smart Trends in Computing and Communications*, Springer, 2022, pp. 551–560, doi: 10.1007/978-981-16-4016-2_52.

[17] M. M. Alani, “Detection of reconnaissance attacks on IoT devices using deep neural networks,” in *Advances in Nature-Inspired Cyber Security and Resilience*, Springer, 2022, pp. 9–27, doi: 10.1007/978-3-030-90708-2_2.

[18] S. R. Akula, “Semi supervised machine learning approach for DDOS detection,” *Int. J. Innov. Res. Educ.*, vol. 8, no. 1, pp. 27–35, 2021, doi: 10.18844/ijire.v8i1.6445.

[19] D. Ono, L. Guillen, S. Izumi, T. Abe, and T. Suganuma, “A proposal of port scan detection method based on packet-in messages in openflow networks and its evaluation,” *Int. J. Netw. Manag.*, vol. 31, no. 6, p. e2174, 2021, doi: 10.1002/nem.2174.

[20] M. I. Kareem and M. N. Jasim, “Entropy-based distributed denial of service attack detection in software-defined networking,” *Indones. J. Electr. Eng. Comput. Sci.*, vol. 27, no. 3, pp. 1542–1549, 2022, doi: 10.11591/ijeecs.v27.i3.pp1542-1549.

[21] I. Sharafaldin, A. Gharib, A. H. Lashkari, and A. A. Ghorbani, “Towards a reliable intrusion detection benchmark dataset,” *Softw. Netw.*, vol. 2018, no. 1, pp. 177–200, 2018, doi: 10.13052/jsn2445-9739.2017.009.

[22] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, “Toward generating a new intrusion detection dataset and intrusion traffic characterization,” *ICISSp*, vol. 1, pp. 108–116, 2018, doi: 10.5220/0006639801080116.

[23] “IDS 2017, Datasets, Research, Canadian Institute for Cybersecurity, UNB.” https://www.unb.ca/cic/datasets/ids-2017.html (accessed Jun. 16, 2022).

[24] A. Ahmim, L. Maglaras, M. A. Ferrag, M. Derdour, and H. Janicke, “A novel hierarchical intrusion detection system based on decision tree and rules-based models,” in *International Conference on Distributed Computing in Sensor Systems*, 2019, pp. 228–233.

[25] S. R. Kalmegh, “Comparative analysis of the WEKA classifiers rules conjunctiverule & decision table on indian news dataset by using different test mode,” 2018, Accessed: Oct. 02, 2022. [Online]. Available: www.ijesi.org.

[26] D. P. Gaikwad, “Intrusion detection system using ensemble of rule learners and first search algorithm as feature selectors,” *Int. J. Comput. Netw. Inf. Secur.*, vol. 13, no. 4, 2021, doi: 10.5815/ijcnis.2021.04.03.

[27] M. N. Jasim and M. T. Gaata, “K-Means clustering-based semi-supervised for DDoS attacks classification,” *Bull. Electr. Eng. Informatics*, vol. 11, no. 6, pp. 3570–3576, 2022, doi: 10.11591/eei.v11i6.4353.

[28] N. Purnamasari, M. A. Fauzi, L. S. D. Indriati, and L. S. Dewi, “Cyberbullying identification in twitter using support vector machine and information gain based feature selection,” *Indones. J. Electr. Eng. Comput. Sci.*, vol. 18, no. 3, pp. 1494–1500, 2020, doi: 10.11591/ijeecs.v18.i3.pp1494-1500.

BIOGRAPHIES OF AUTHORS

Mahdi Nsaif Jasim iD 8 SC ⟳ is Assist. Prof. Dr. Mahdi Nsaif Jasim, University of Information Technology and Communications, College of Business Informatics Dept. of Management Information Systems. Born in Babylon, Iraq, lives in Baghdad. Interest: information systems, data and information security, mining in vector data, GIS, database systems. The researcher has interest in SDN data acquisition and data processing. He also Supervised a number of PhD and MSc. Students in different Iraqi universities. Dr. Mahdi has been supervised 10 MSc students and 5 PhD students. He taught number OS BSc. and MSc. courses a number of Iraqi universities. He can be contacted at email: mahdimnsaif@uoitc.edu.iq.

Muthanna Jabbar Abdulredhi iD 8 SC ⟳ has been supervised 6 BSc. Students. He taught a number of BSc. Students' courses at several Iraqi universities Like Al-Nahrain University/collage of Engineering and Information Engineering collage and the University of Information Technology and Communications Muthanna has more than 15 years of installing, Administering, and managing several networks in different Iraqi Ministries trends from 2002 till now. He can be contacted at email: muthanna.jabbar@uoitc.edu.iq.

Ali Munther AbdulRahman iD 8 SC ⟳ is a member of teaching staff in the University of Information Technology and Communications, College of Business Informatics Dept. of Information Systems Management, Born in Baghdad/Iraq, lives in Baghdad. Interest: Information Systems, Data and Information Security, Machine Learning, Database Systems. The researcher has interest in SDN data acquisition and data processing. He also Supervised 4 BSc Students in different Iraqi universities. Mr. Ali has more than 15 years of software systems development in different trends starting from 2002, till now. The Experience in development of Business and management systems, engineering and scientific systems, and around 5 years giving training in the fields of e-government, web designs, and software engineering. He can be contacted at email: alneemyali@uoitc.edu.iq.