

# Machine learning-based PortScan attacks detection using OneR classifier

Mohammed Ibrahim Kareem<sup>1</sup>, Mohammad Jawad Kadhim Abood<sup>2</sup>, Karrar Ibrahim<sup>3</sup>

<sup>1</sup>Department of Information Security, University of Babylon, Hillah, Iraq

<sup>2</sup>Department of Software, University of Babylon, Hillah, Iraq

<sup>3</sup>Department of English, College of Education, Al-Zahraa University for Women, Karbala, Iraq

## Article Info

### Article history:

Received May 28, 2022

Revised Jul 14, 2022

Accepted Feb 3, 2023

### Keywords:

CICIDS2017

Feature selection

JRip

Machine learning

Network security

PortScan attack

## ABSTRACT

PortScan attacks are a common security threat in computer networks, where an attacker systematically scans a range of network ports on a target system to identify potential vulnerabilities. Detecting such attacks in a timely and accurate manner is crucial to ensure network security. Attackers can determine whether a port is open by sending a detective message to it, which helps them find potential vulnerabilities. However, the best methods for spotting and identifying port scanner attacks are those that use machine learning. One of the most dangerous online threats is PortScan attack, according to experts. The research is work on detection while improving detection accuracy. Dataset containing tags from network traffic is used to train machine learning techniques for classification. The JRip algorithm is trained and tested using the CICIDS2017 dataset. As a consequence, the best performance results for JRip-based detection schemes were 99.84%, 99.80%, 99.80%, and 0.09 ms for accuracy, precision, recall, F-score, and detection overhead, respectively. Finally, the comparison with current models demonstrated our model's proficiency and advantage with increased attack discovery speed.

*This is an open access article under the [CC BY-SA](#) license.*



## Corresponding Author:

Mohammed Ibrahim Kareem

Department of Information Security, University of Babylon

Hillah, Iraq

Email: Mohamed.ibrahim@uobabylon.edu.iq

## 1. INTRODUCTION

The first step in launching a network attack is to identify vulnerable hosts and prospective victims. Port scanning is a common method used by attackers to determine the level of vulnerability in their targets. This is a reconnaissance attack that allows the attacker to collect information about receiving hosts' port numbers, network configurations, server implementations, operating systems, and potential service vulnerabilities. Sending a probe packet to a specific host port on the network and analyzing the answer from an open port is what port scanning entails [1]. Port scanning is typically performed on transmission control protocol (TCP), user datagram protocol (UDP), and internet control message protocol (ICMP) channels.

In order to find out which network ports are open and which services are currently using them on a computing endpoint, port scanning is the act of making attempts to connect to multiple network ports on the device. In order to find holes in a system or network, hackers frequently utilize this technique. An attacker can discover the services and apps running on a device and potentially exploit any known vulnerabilities in those services by determining which ports are exposed. Port scanning is frequently the first stage of a cyber-attack, making it crucial to recognize it. Security experts can take proactive steps to secure the systems and networks by spotting port scanning attempts before an attacker has an opportunity to take advantage of any flaws [2].

Scientists have spent a lot of time and energy creating reliable methods for detecting port scanning operations over the past ten years, including machine learning. Machine learning makes use of the capacity to learn from examples or data patterns in order to carry out tasks and gradually improve its performance. Machine learning makes it feasible to distinguish between previously unexpected attacks, regular, and well-known attack patterns in network traffic. The identification and selection of the most important input features needed to create an efficient model for a particular classification problem, based on the training data available, represents a key issue in machine learning [3].

Machine learning approaches are typically employed in the four primary steps in the learning process (preprocessing, mining, transformation, and interpretation) [4], [5]. The multidimensional challenge's [6] complexity makes it difficult for classification techniques to accurately find PortScan attack [7]. Because they can work on named classes, the behind ideas employ supervised procedures. Various machine learning techniques are being employed to address the challenges posed by cyber threats and develop intrusion detection systems. Machine learning techniques that result in evolutionary computing as a final output or additional supporting solutions such as feature selection [8].

One of the most common penetration testing techniques that attackers use to carry out malicious objectives is port scanning assaults. The problem of efficiently and quickly detecting open ports persists due to the more sophisticated nature of cybercriminals, modern technology, and the failure of traditional network intrusion detection solutions. Therefore, many recent research has sought to fix and address the issue of upgrading this intrusion detection technology, particularly those that used machine learning approaches, but suffer from several performance challenges necessitating additional exploration. The relevant component was successfully resolved using principal component analysis and the findings were improved utilizing seven machine learning classifiers which were used in this paper to detect port scanning assaults. The following are some benefits of the suggested strategy over earlier detection systems based on JRip algorithm: i) to train detection models utilizing JRip and one rule (OneR) algorithms, classified datasets are necessary, ii) an information acquisition ratio and variance filtering-based feature selection approach is suggested, and iii) to implement it online for traffic classification, the existing model may be categorized as port scanning and routine.

Various papers, such as [9]–[11], have presented a variety of methods for detecting cyberattacks utilizing statistical techniques or machine learning advancements. A current research area is being shaped by articles on machine learning techniques, which are among the most widely published. Table 1 (in Appendix) [12]–[20] gives a brief summary of some recent breakthroughs and research in PortScan attack detection.

The remainder of this work is summarized here. PortScan attack detection discusses the limitations of related approaches. Our disclosure model, which is based on a supervised classification algorithm, is presented in section 2. Section 3 present the result and discussion and finally section 4 present conclusions and future works. The study concludes with recommendations for several trials after discussing and analyzing the significance of the trial outcomes.

## 2. METHOD

This section first describes the data set that was used, then demonstrates the algorithms that were used to create the model, and then covers the suggested methods for a hybrid type of feature selection. The primary functions of the suggested system are depicted in Figure 1. The proposed system introduces a novel method of PortScan attack detection for intrusion detection. It makes use of supervisory methods, particularly JRip and OneR. In order to determine how effective these algorithms are, the study analyzes the data and reviews the results.

### 2.1. The CICIDS2017 description

CICIDS2017, contains both benign and malicious activity [21]. It includes the outcomes of a study of network traffic using labelled flows based on timestamps, IP addresses with ports for source and destination, protocols, and attacks. The five-day data collection session lasted from Monday, July 3<sup>rd</sup>, 2017 to Friday, July 7<sup>th</sup>, 2017. In this dataset, the assaults include PortScan Heartbleed, DoS, infiltration, brute-force SSH and FTP attacks, distributed denial of service (DDoS), web attack, and Botnet. Other IDS datasets split the training dataset from the testing dataset, but CICIDS2017 compiled all attack logs into a single CSV file [22]. There are 85 networks flow characteristics in this dataset. CICIDS2017 [23], the most extensive and frequently used dataset [24], is the valid dataset.

### 2.2. The JRip classification model

JRip is a machine learning classification algorithm. It is a rule-based classifier that combines decision trees with rule induction approaches. JRip excels at dealing with categorical data and generating interpretable rules. The JRip algorithm generates a collection of rules that humans can easily understand and

interpret. These rules can provide insights into the classifier's decision-making process, making it valuable in sectors where interpretability is essential, such as healthcare or finance.

### 2.3. The OneR classification algorithm

OneR is a well-known rule-based classifier that is easy to understand and apply in machine learning. The objective is to identify a single attribute (feature) with the greatest ability to distinguish between different classes of instances. Because it builds a single rule depending on the chosen property. Even though the OneR approach is straightforward, it can function effectively in situations where a single property strongly predicts the class labels. However, it might be unable to recognize subtle correlations between qualities, which would restrict its effectiveness in increasingly challenging categorization tasks. As a result, it is frequently used as a starting point or in conjunction with other classifiers to shed light on the significance of specific traits [25].

### 2.4. The feature selection methods

Choosing a subset of relevant features from a broader collection of available information is an important stage in machine learning. The goal is to optimize computing efficiency while improving model performance, reducing overfitting, and improving interpretability. It's important to note that each feature selection method has its own set of advantages and disadvantages. The approach chosen is determined by the unique problem, the nature of the data, the computational resources available, the desired trade-offs between performance, interpretability, and efficiency. Experimentation and careful examination are frequently required to discover the best effective feature selection strategy for a specific assignment. Figure 1 displays the suggested system's preliminary schematic.

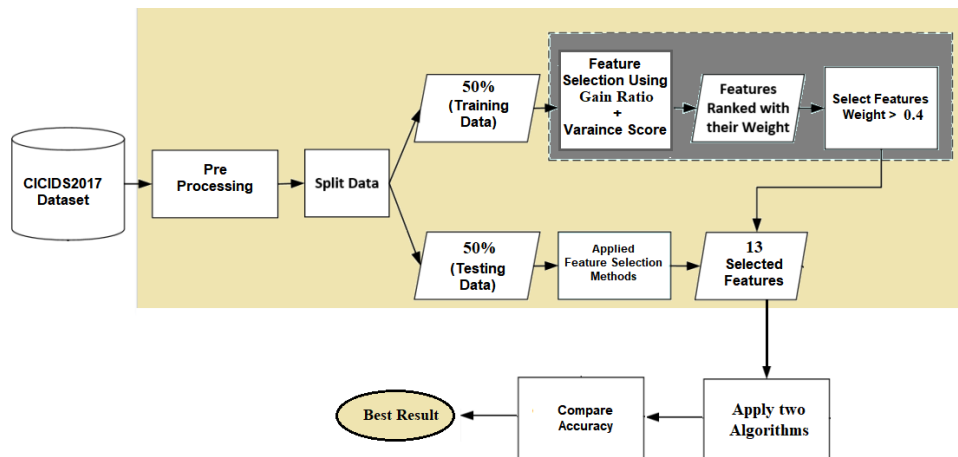


Figure 1. Block diagram of the proposed system

#### 2.4.1. The variance features filtering

The features with low variance can be found and excluded from further analysis or modeling by computing the variance for each feature and comparing it to the threshold. Reduced dimensionality and features that might not have strong discriminatory power for the classification task are achieved through this filtering process. In (1) is used to calculate the variance (V) of each characteristic [14]:

$$V(\sigma^2) = \frac{\sum_{i=1}^n (X_i - \mu)^2}{Z} \quad (1)$$

Where Z is the total number of trials,  $\mu$  is the mean (average) value of the feature. Values of the features, represented by  $X_i$ , are calculated from a set of samples.

#### 2.4.2. The information gain ratio

A statistic used in feature selection to assess the applicability of a feature for classification is the information gain ratio (IGR) [26]. It is determined by deducting the entropy value before to feature-based data separation from the entropy value following feature-based data separation. The IGR aids in determining

whether or not to include a feature in the classification process. Only qualities that match the weighting criteria will be considered for classification. Information gathering in conjunction with variance is utilized in this work to accurately identify features of interest using (2):

$$IGR(M, A_j) = \frac{H(M) - H(M|A_j)}{H(A_j)} \quad (2)$$

where  $M$  denotes the class and  $A_j$  denotes the  $j$ th feature. The formula for entropy,  $H(\cdot)$ , is indicated by (3):

$$H(E) = -\sum_{i=1}^n p(e_i) \log p(e_i) \quad (3)$$

Taking the input as an example,  $p(i)$  represents the probability of occurrence of class  $i$  within the dataset  $S$ .

## 2.5. The proposed PortScan attack detection

Machine learning-based detection and response tools can better comprehend typical scanning activity on specific networks and offer high-fidelity detection even when attackers try to hide their footprints. The strategy put out in this research uses supervised JRip to produce binary classifiers that categorize incoming packets as either hostile or benign. We use the JRip technique to identify the PortScan attack starting with the CICIDS2017 dataset. The suggested approach calls for training the model on labeled data with a 50:50 training to testing split. The block diagram of the suggested system is shown in Figure 1. The following are the key steps in the suggested process:

- Features chosen with the aid of hybrid feature selection methods. The best possible combination of attributes was discovered in this study using variation and IGR methods. Ignoring properties with low contrast values under 3.4 by using contrast scores. In addition, as indicated in Table 2, 13 features are generated by removing the minimal IGR of features that are smaller than 0.4.
- Using the JRip and OneR algorithms, construct a suitable classifier model.
- Compare the effectiveness of the suggested models and select the top one.

Table 2. The features degree by IGR

No.	Feature name	Feature score
1	PSH flag count	0.615
2	Avg Bwd segment size	0.5396
3	Bwd packet length mean	0.5396
4	Bwd packet length min	0.529
5	Init_Win_bytes_backward	0.5138
6	Subflow Bwd bytes	0.452
7	Total length of Bwd packets	0.452
8	min_seg_size_forward	0.4449
9	Bwd packet length max	0.444
10	Packet length mean	0.4344
11	Average packet size	0.431
12	act_data_pkt_fwd	0.4059
13	Max packet length	0.4043

## 3. RESULTS AND EVALUATION

The method was tested in this experiment, and the effectiveness of the suggested methods' detection was assessed in light of the findings. Without a doubt, the suggested algorithm's accuracy serves as a barometer for how well it can identify assaults. In the case of the current work, distinguish between regular and port scan data. In (4) allows for the calculation of the algorithm's accuracy:

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad (4)$$

Accuracy was employed as a metric to determine how well the suggested system performed. The algorithm's accuracy is measured by how well it can predict traffic using a trained model. The algorithm's capability to distinguish between a regular attack and a port scan assault with accuracy. Figure 2 and Table 3 display the findings of the comparison of the JRip and OneR benchmarks. Because both methods can distinguish between normal traffic and PortScan attacks, as explained in Table 3, the outputs of the two techniques are almost identical.

An evaluation of the performance measures obtained from the two supervisor algorithms using the 13 selected features reveals that these features significantly enhance the classifier's overall performance in

detecting PortScan attacks. Based on the experimental results and the analysis, both the JRip and OneR algorithms effectively recognize PortScan attacks using the chosen features from the CICIDS2017 dataset (refer to Table 3). However, the proposed JRip model outperforms the OneR algorithm with an accuracy of 99.84%.

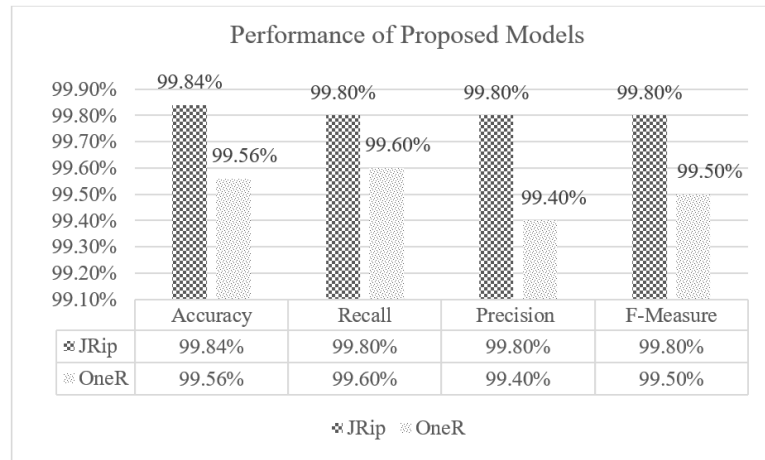


Figure 2. The efficiency of the recommended approaches

Table 3. The outcomes of comparing JRip with OneR criterion measurements

Algorithm name	Accuracy (%)	Recall (%)	Precision (%)	F-Measure (%)
JRip	99.84	99.80	99.80	99.80
OneR	99.56	99.60	99.40	99.50

#### 4. CONCLUSION

Machine learning-based detection and response tools can better comprehend typical scanning activity on certain networks and offer high-accuracy detection even when attackers try to cover their tracks. This study uses machine learning to distinguish between legitimate and malicious port scan traffic. In order to train the model, one of the databases was chosen. The outcomes demonstrated the excellent accuracy of the suggested strategy. To reduce 84 attributes to the final 13 features that are required to classify traffic packets, the proposed system offers hybrid feature selection algorithms. Once the algorithm has been properly trained on a classified data set, the JRip and OneR are the proposal classification approaches may categorize traffic into a conventional attack and a PortScan attack. Future work should include applying the suggested technique in a practical setting, such as software-defined networking (SDN) or the IoT. Additionally, use a more recent dataset, such as CICDDoS2019, to train and test the suggested model.

#### APPENDIX

Table 1. Related works

No	Ref.	Findings discussion
1	[12]	Present a detection technique for slow PortScan attacks using the fluid reasoning index (FRI) method. For the purposes of this research, a controlled test-bed environment was also designed and implemented. Various observations were used to try and evaluate the proposed detection method. Experimenting on a real test-bed environment yields helpful information about the effectiveness of the proposed detection method.
2	[13]	Build a traffic feature set based on protocol features and port scan connection patterns that can not only detect specific scan types but also remain effective for the sampled traffic. They also customize a data format called scan detection sketch (SDS) for feature extraction. Experiment findings with publicly available datasets indicate that our method can detect slow port scans in 10 Gbps high-speed network with excellent accuracy and low memory consumption.
3	[14]	For the classification of DDoS, a semi-supervised approach based on the K-means clustering algorithm was created. The proposed algorithm was tested and trained using the CICIDS2017 dataset. DDoS and regular activities were chosen as the ideal two centroids by using hybrid feature selection techniques, multiple training, and testing iterations. These centroids were used to precisely sort and categorize DDoS traffic through a series of well-planned experiments. Centroids that are produced can be used to categorize network activity.
4	[15]	Seven machine learning classifiers to identify PortScan attacks after successfully resolving the relevant component and improving the results using principal component analysis.

Table 1. Related works (continue)

No	Ref.	Findings discussion
5	[16]	Logistic regression to detect PortScan attacks and tested data balancing methods to achieve better results.
6	[17]	Suggest a method for identifying internal and external network scanning attacks on business networks. An inline SDS is used in the method to monitor the ingress and egress flows of a corporate network subnet and identify scanning probes by correlating the flows with previous domain name system (DNS) queries, replies, and shortening DNS resource records' TTL values (RR).
7	[18]	The UNSW-NB15 dataset, which contains 49 features for nine distinct attack samples, has been used to test the proposed models. Comparing the accuracy of the decision tree classifier to the ensemble models of random forest (98.96%), Adaboost (97.87%), and XGBoost (98.08%), it gave the best results 99.5%. With K=7 and an accuracy of 95.58%, the K-nearest neighbor (KNN) classifier performed best when taught for different values of K.
8	[19]	Employs a strobe to identify open ports. Super optimized TCP port surveyor (strobe) is a tool used to perform port scanning or probe service tasks in secure networks and systems running on the UNIX platform.
9	[20]	An empirical study to assess Snort's efficacy against network attacks, probing, brute force, and DoS, along with four supervised machine learning classifiers: KNN, decision tree, Bayesian net, and naïve bayes. Using the weka tool, one can evaluate the snort metric, true alarm rate, F-measure, precision, and accuracy and compare them to the same metrics obtained from the use of machine learning algorithms. For the majority of algorithms, machine learning classifiers exhibit improved performance with over 99% of properly classified instances.





## REFERENCES

- [1] A. Upadhyay, "A Survey on Different Port Scanning Methods and the Tools used to perform them," *International Journal for Research in Applied Science and Engineering Technology*, vol. 8, no. 5, pp. 3018–3024, May 2020, doi: 10.22214/ijraset.2020.5505.
- [2] J. M. Pittman, "Machine Learning and Port Scans: A Systematic Review," *Arxiv-Computer Science*, vol. 1, pp. 1–8, 2023, doi: 10.48550/arXiv.2301.13581.
- [3] S. S. Panwar, Y. P. Raiwani, and L. S. Panwar, "Evaluation of Network Intrusion Detection with Features Selection and Machine Learning Algorithms on CICIDS-2017 Dataset," in *International Conference on Advances in Engineering Science Management & Technology (ICAESMT)*, 2019, pp. 1–10. doi: 10.2139/ssrn.3394103.
- [4] K. Kalegele, K. Sasai, H. Takahashi, G. Kitagata, and T. Kinoshita, "Four Decades of Data Mining in Network and Systems Management," in *IEEE Transactions on Knowledge and Data Engineering*, vol. 27, no. 10, pp. 2700–2716, Oct. 2015, doi: 10.1109/tkde.2015.2426713.
- [5] J. Han, J. Pei, and M. Kamber, *Data Mining: Concepts and Techniques*. USA: Elsevier-Morgan Kaufmann, 2011.
- [6] S. Karanam, "Curse of Dimensionality—A 'Curse' to Machine Learning," *Towards Data Science*, [Online]. Available: <https://towardsdatascience.com/curse-of-dimensionality-a-curse-to-machine-learning-c122ee33bfeb>. Access date: Jun. 19, 2022.
- [7] P. Berkhin, "A Survey of Clustering Data Mining Techniques," in *Grouping Multidimensional Data*, Springer: Verlag, pp. 25–71, doi: 10.1007/3-540-28349-8\_2.
- [8] M. Aamir, S. S. H. Rizvi, M. A. Hashmani, M. Zubair, and J. A. Usman, "Machine Learning Classification of Port Scanning and DDoS Attacks: A Comparative Analysis," *Mehran University Research Journal of Engineering and Technology*, vol. 40, no. 1, pp. 215–229, Jan. 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)*, IEEE, Duhok, Iraq, 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," *Bulletin of Electrical Engineering and Informatics*, vol. 11, no. 3, pp. 1742–1751, Jun. 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)*, IEEE, Dec. 2021, pp. 29–34, doi: 10.1109/it-ela52201.2021.9773744.
- [12] M. Almseidin, M. Al-Kasassbeh, and S. Kovacs, "Detecting Slow Port Scan Using Fuzzy Rule Interpolation," in *2019 2nd International Conference on new Trends in Computing Sciences (ICTCS)*, IEEE, Oct. 2019, pp. 1–6, doi: 10.1109/ictcs.2019.8923028.
- [13] H. Wu, Z. Shao, G. Cheng, X. Hu, J. Ren and W. Wang, "Detecting Slow Port Scans of Long Duration in High-Speed Networks," *GLOBECOM 2022 - 2022 IEEE Global Communications Conference*, Rio de Janeiro, Brazil, 2022, pp. 3405–3410, doi: 10.1109/GLOBECOM48099.2022.10001708.
- [14] M. N. Jasim and M. T. Gaata, "K-Means clustering-based semi-supervised for DDoS attacks classification," *Bulletin of Electrical Engineering and Informatics*, vol. 11, no. 6, pp. 3570–3576, Dec. 2022, doi: 10.11591/eei.v11i6.4353.
- [15] E. K. Baah et al., "Enhancing Port Scans Attack Detection Using Principal Component Analysis and Machine Learning Algorithms," in *Communications in Computer and Information Science*, Springer Nature Singapore, 2022, pp. 119–133, doi: 10.1007/978-981-19-8445-7\_8.
- [16] 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," *Research Square*, pp. 1–10, May 2022, doi: 10.21203/rs.3.rs-1554916/v1.
- [17] J. H. Jafarian, M. Abolfathi, and M. Rahimian, "Detecting Network Scanning through Monitoring and Manipulation of DNS Traffic," *IEEE Access*, vol. 11, pp. 20267–20283, 2023, doi: 10.1109/access.2023.3250106.
- [18] K. A. Dhanya, S. Vajipayajula, K. Srinivasan, A. Tibrewal, T. S. Kumar, and T. G. Kumar, "Detection of Network Attacks using Machine Learning and Deep Learning Models," *Procedia Computer Science*, vol. 218, pp. 57–66, 2023, doi: 10.1016/j.procs.2022.12.401.
- [19] A. Zikri, D. M. Alfira, L. Ahmadi, M. J. Alfuruqi, N. Agung, and Y. Pangestu, "Port scanning identification on wireless networks using the strobe method," *JComce-Journal of Computer Science*, vol. 2, no. 2, 2023.
- [20] S. Abdulrezak and F. Sabir, "An Empirical Investigation on Snort NIDS versus Supervised Machine Learning Classifiers," *Journal of Engineering*, vol. 29, no. 2, pp. 164–178, Feb. 2023, doi: 10.31026/j.eng.2023.02.11.
- [21] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "A Detailed Analysis of the CICIDS2017 Data Set," in *Communications in Computer and Information Science*, Springer International Publishing, 2019, pp. 172–188, doi: 10.1007/978-3-030-25109-3\_9.





- [22] Y. Zhou, G. Cheng, S. Jiang, and M. Dai, "Building an efficient intrusion detection system based on feature selection and ensemble classifier," *Computer Networks*, vol. 174, pp. 1–17, Jun. 2020, doi: 10.1016/j.comnet.2020.107247.
- [23] "Intrusion Detection Evaluation Dataset (CIC-IDS2017)," Canadian Institute for Cybersecurity, 2017. [Online]. Available: <https://www.unb.ca/cic/datasets/ids-2017.html>. Access date: 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 *2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS)*, IEEE, May 2019, pp. 228–233, doi: 10.1109/dccoss.2019.00059.
- [25] D. P. Gaikwad, "Intrusion Detection System Using Ensemble of Rule Learners and First Search Algorithm as Feature Selectors," *International Journal of Computer Network and Information Security*, no. 4, pp. 26–34, Aug. 2021, doi: 10.5815/ijcnis.2021.04.03.
- [26] N. M. G. D. Purnamasari, M. A. Fauzi, I. Indriati, and L. S. Dewi, "Cyberbullying identification in twitter using support vector machine and information gain based feature selection," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 18, no. 3, pp. 1494–1500, Jun. 2020, doi: 10.11591/ijeecs.v18.i3.pp1494-1500.

## BIOGRAPHIES OF AUTHORS







**Mohammed Ibrahim Kareem**     received bachelor's degree in Information Technology from the University of Babylon, Iraq, in 2013, and his Master's degree in Data Mining from the University of Babylon, Iraq, in 2019. He currently holds a Ph.D. Information Security student at Babylon University, Iraq. Worked for several years as a software engineer at OMNNEA Telecom from 2014 to 2020. His research interests include computer networking, network security, and data mining. He can be contacted at email: mohamed.ibrahim@uobabylon.edu.iq.



**Mohammad Jawad Kadhim Abood**     is a Ph.D. student at the University of Babylon, College of Information Technology, Department of Networks, Iraq. He received a bachelor's degree in Computer Science from the University of Babylon, Iraq, and a master's degree in Information Technology from SHUATS, India. His current field is dynamic allocation in the virtual environment and network security in NGN. He is one of the CISCO instructors in the Iraq region, holding MCSE, MCSA, and is certified as an IT admin by TUBerlin. He can be contacted at email: mu4su@uobabylon.edu.iq.



**Karrar Ibrahim**     received Bachelor's degree in Computer Technology Engineering from Al-Mansour University College, Iraq, in 2015, and his Master's degree in Network Technology from UTeM, Malaysia, in 2018. He is currently a Ph.D. in Information Technology student at Babylon University, Iraq. Worked for several years as an IT engineer at Al Liwa International Company from 2015 to 2017 and also at Al-Zahraa university for women as an IT manager from 2020 to present. His research interests include computer networking, communication, and machine learning. He can be contacted at email: karrar.ibrahim@alzahraa.edu.iq.