

# An observational mechanism for detection of distributed denial-of-service attacks

Norliza Katuk<sup>1</sup>, Mohamad Sabri Sinal<sup>1</sup>, Mohammed Gamal Ahmed Al-Samman<sup>1</sup>, Ijaz Ahmad<sup>2</sup>

<sup>1</sup>School of Computing, Universiti Utara Malaysia, Kedah, Malaysia

<sup>2</sup>Faculty of Information Technology, Majan College in Muscat, Muscat, Oman

## Article Info

### Article history:

Received Nov 12, 2022

Revised Mar 4, 2023

Accepted Apr 17, 2023

### Keywords:

Attacks

Intrusion detection system

Machine learning

Network security

Security

## ABSTRACT

This study proposes a continuous mechanism for detecting distributed denial of service (DDoS) attacks from network traffic data. The mechanism aims to systematically organise traffic data and prepare them for DDoS attack detection using convolutional deep-learning neural networks. The proposed mechanism contains ten phases covering activities, including data preprocessing, feature selection, data labelling, model building, model evaluation, DDoS detection, attack pattern identification, alert creation, notification delivery, and periodical data sampling. The evaluation results suggested that the detection model built based on convolutional deep-learning neural networks and relevant network traffic features provided 97.2% detection accuracy. The study designed a holistic mechanism that considers the systematic network traffic data management for continuous monitoring and good performance of DDoS attack detection. The proposed mechanism could provide a solution for network traffic data management and enhance the existing methods for DDoS attack detection. In addition, it generally contributes to the cybersecurity body of knowledge.

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



## Corresponding Author:

Norliza Katuk

School of Computing, Universiti Utara Malaysia

06010 UUM Sintok, Kedah, Malaysia

Email: k.norliza@uum.edu.my

## 1. INTRODUCTION

Network traffic data are generated daily from various computer devices and applications connected to the internet. For example, traffic data could be contributed by users' web browsing activities, e-mails, chats, streams, file transfers, voice-over internet protocol (IP), and peer-to-peer applications [1]. These data can be captured and analysed using network or packet analysis tools. They provide information about network consumption, such as application protocols, users, traffic volume, and profiles [2]. In addition, these data also contained network-related properties of packet information such as port numbers, flags, IP addresses, and time stamps, to name a few [3]. Thus, network traffic data contains features of big data, which plays an essential role in network management and security [4]. Network managers can access and observe network traffic data in any part of the network segment. However, the biggest challenge is analysing the data to determine whether the traffic data represent normal or abnormal user activities [3]. Abnormal activities in the context of this study refer to the traffic data that could be classified as distributed denial of service (DDoS) attacks. Thus, understanding the data and its patterns is crucial to protecting the computing infrastructure from DDoS attacks. However, identifying the attacks becomes more difficult due to the complex nature of network traffic data [5].

Researchers have proposed various methods to analyse network traffic data previously. For example, Miao *et al.* [4] performed feature selection during pre-processing of traffic data that reduced their dimensions and removed irrelevant information to classify them better. On the other hand, Ji *et al.* [5] proposed using data

visualisation techniques that include data filtration and transformation in analysing a large volume of network traffic data to detect abnormal activities in the network. However, although many studies have been conducted to address the issue, the best method for detecting network attacks cannot be obtained because network traffic patterns are constantly changing [5]. Therefore, analysis of the data remains an unsolved issue.

Nevertheless, researchers agreed that a periodical analysis of network traffic data is critical as an input to a functional and responsive intrusion detection system (IDS) [6]. Furthermore, by having a consistent analysis interval, any pattern change in the data would be determined quickly, and the pattern could be recorded in the database. Therefore, extensive network traffic data can be processed within a reasonable period to detect DDoS, and subsequently, the system can respond to such attacks more quickly [7]. IDS is a framework that monitors the traffic data in the internet system to prevent activities or events that pose threats or attacks to the network [8]. It provides an extra layer to securing the network components [9]. The central role of IDS is to observe and recognise abnormal activities in a device or computer network and notify the administrators of such activities [10], [11]. Depending on the system's defence architecture, the system can be located inside or outside the network's perimeter and on the host. Figure 1 illustrates the possible locality of IDS [12]. No matter where the IDS is placed, its primary purpose is to detect all attacks, including DDoS, which is the scope of the study reported in this article [11].

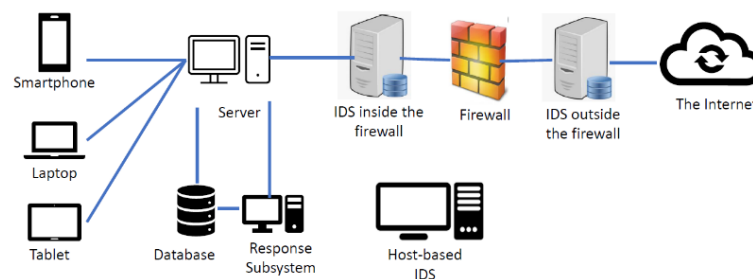


Figure 1. The possible locality of IDS [12]

The detection mechanism in IDS can be divided into two, namely, signature or anomaly detection. The signature mechanism analyses network traffic data and compares it to rules based on a predefined pattern to detect attacks, while the anomaly approach detects strange and unusual traffic patterns [9]. Nevertheless, the major challenge for any IDS is to classify the incoming pattern to determine if it is normal, with the highest accuracy and lowest false-positive possible [10]. Studies on determining the pattern and classifying traffic data have long since begun. Furthermore, various network protocols have also encouraged current research covering aspects of intrusion detection, such as dataset pre-processing methods, optimisation of detection models, and detection technologies in different network environments [13]. On the other hand, the advent of various artificial intelligence methods can achieve good detection results through hybrid feature selection technology and optimisation of detection models. Therefore, the potential of artificial intelligence methods is very beneficial and helps provide more accurate classification results and, in turn, create IDS that can function more efficiently.

Many methods have been proposed to detect DDoS; nevertheless, they cannot provide effective detection as attackers enhance their strategy and use more sophisticated methods in launching the attacks. Consequently, many DDoS detection methods suffer from low detection accuracy and high false-positive alarms. One possible reason for this situation is that the methods have not considered representative features of traffic data related to DDoS attacks [14]. Recent development shows that researchers began to apply machine learning approaches to detect DDoS, providing promising outcomes and leading to efficient IDS implementation. However, research on DDoS detection methods will never stop because a method becomes ineffective when attackers change to new strategies or use other approaches to launch the attack. Therefore, trying all possible methods and technologies to deal with this problem is worthwhile.

The use of machine learning for intrusion detection, including DDoS attacks, has long since begun. The classifiers' success depends on the dataset's relevant features and the accuracy of classification results [15]. The machine learning model is divided into two groups: the classical and deep learning models. Recently, studies have demonstrated that deep learning methods provide better results in several domains, such as picture classification, speech recognition, and machine translation. In the domain of intrusion detection, both classical machine learning and deep learning models have been used with promising results [16]. However, it is also

known that machine learning has no concept of one size fits all. In other words, no model is perfect and suitable for all situations.

Therefore, machine and deep learning studies to detect intrusions and attacks will keep growing to address the sophistication of the launched attacks [17]. Deep learning or deep neural network is a subset of machine learning techniques [18] that uses various levels of representation [19] in layers which allows a higher level of abstraction and prediction of the data [18]. It makes computer systems learn from experience and understand the world through hierarchical concepts [20]. In traditional machine learning, data contain many features, and only relevant features are extracted for the classification process to produce the prediction.

Neural networks, such as deep feed-forward neural networks, convolutional neural networks, deep belief networks, autoencoders, and long short-term memory networks, are used in deep learning for classifying data [21]. Further, many deep learning frameworks and libraries have been developed like Caffe, Microsoft Cognitive Toolkit, Gluon, Keras, MXNet, TensorFlow, Theano, Torch, PyTorch, Chainer, and Deeplearning4J [22]. The development and introduction of various libraries allow extensive studies in deep learning to solve various problems, particularly in cyber defence, particularly intrusion detection. For example, Gamage and Samarabandu [16] presented the deep learning approach more systematically in the context of intrusion detection, as depicted in Figure 2. They categorised deep learning models for intrusion detection into four categories: supervised instance learning, supervised sequence learning, semi-supervised instance learning, and other learning paradigms.

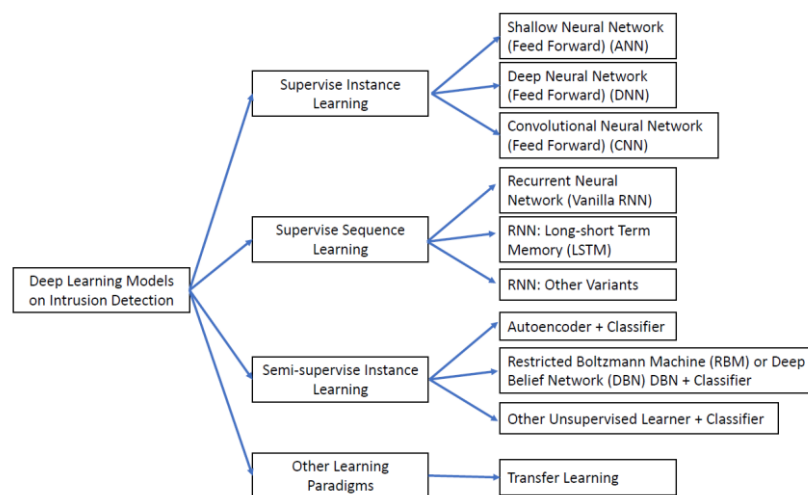


Figure 2. Deep learning taxonomy for IDS [16]

Deep learning for intrusion detection has been a growing interest among researchers recently. For example, Gamage and Samarabandu [16] evaluated different deep learning models, namely feed-forward neural network, autoencoder, deep belief network, and long short-term memory network, to classify intrusions. In addition, Ojugo and Yoro [23] used a deep-learning neural network for classifying normal and DDoS attacks. The model was able to classify the data with over 80% accuracy. Thus, researchers have started studying deep learning for intrusion detection. However, those studies applied deep learning to older datasets [16], which might not accurately represent current DDoS attacks.

## 2. THE PROPOSED OBSERVATIONAL MECHANISM FOR DDOS ATTACK DETECTION AND RESPONSE

This section describes the proposed observational mechanism for detecting DDoS attacks and how to respond to them. The mechanism comprises ten phases: i) data pre-processing, ii) feature selection, iii) data labelling, iv) model building, v) model evaluation, vi) DDoS detection, vii) attack patterns identification, viii) alert creation, ix) notification delivery, and x) periodical data sampling. The phases in this mechanism run in a cycle and iterate over time. The primary input to the mechanism is the network traffic data, and the final output is a notification received by the network managers. Other outputs are also generated within the mechanism, including a deep learning model, a DDoS detector module, detection results, alert traces, and attack patterns stored in a database. Finally, periodical data sampling on the network traffic would generate a network traffic

sample for consistent and systematic monitoring of the user activities for detecting DDoS attacks. Figure 3 illustrates the overall flow of the mechanism.

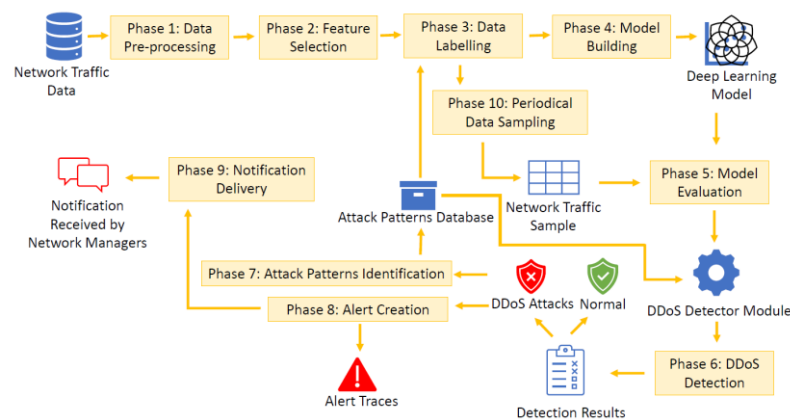


Figure 3. The proposed observational mechanism for DDoS attack detection and response

Phase 1: data pre-processing—the mechanism receives input from network traffic data. The data can be captured using network packets analysing tools like Wireshark, TCPdump, and WinDump, to name a few. These data are considered raw and comprise a dataset with information on the packet's time, source, destination, protocol, length, and user data. Hence, they require data pre-processing, an essential step in a data-driven system. The raw network traffic data may be incomplete or inappropriate for use by software to perform data mining and machine learning processes. For example, data may contain missing values or unnecessary features. The data may also contain noise that can affect the model's performance for DDoS detection. Therefore, it is crucial to ensure that the data is in a form that is ready for use by software [24]. Further, data pre-processing is also necessary to ensure accurate detection [25]. This phase mainly focuses on checking the dataset for missing values. First, the dataset is sorted to detect missing values, then data lines with missing content are discarded.

Phase 2: feature selection—this phase has three processes covering selecting relevant network traffic properties, data transformation, and data normalisation. First, the pre-processed network traffic dataset obtained in phase 1 still contains raw data, which does not ready for further analysis. Second, it also contained unnecessary features that are not relevant for detecting DDoS; therefore, there is a need for selecting relevant network traffic properties that characterise DDoS attacks. Finally, the chosen features are further used for data transformation. It is a branch of data mining and machine learning research aiming to improve the classification process's performance [26]. Past studies suggested that the dataset's selected features highly influence intrusion detection mechanisms [27]. Feature selection significantly reduces the number of features that can distinguish between normal and attack data [28]. Therefore, reducing data dimensions in IDS can improve system performance by eliminating unnecessary features. For example, Shiravani *et al.* [29] proposed a feature selection method using a fuzzy triangular number parameter and genetic algorithm optimisation, which reduces false alarm rates and increases efficiency.

Hence, feature selection (called attribute selection) is a crucial process which it involves selecting a subset of relevant features (i.e., attributes) for constructing the model [30]–[32] and producing good classification results. New traffic features like total packets in the forward direction, total packets in the backward direction, the total size of packets in the forward direction, and the total size of the packet in the backward direction are calculated and added to the dataset. This process is known as data transformation. Finally, min-max data normalisation is performed based on (1) [33] to deal with inconsistencies in the range of the data. The data normalisation process scales the network traffic data between 0 and 1 and ensures that all the features have the same scale.

$$n' = \frac{n - \min(fe)}{\max(fe) - \min(fe)} \times (\text{new\_max}(fe) - \text{new\_min}(fe)) + \text{new\_min}(fe) \quad (1)$$

Where,  $fe$  is the network traffic feature,  $n$  is the old value of an individual instance of  $fe$  data,  $n'$  is the new value of an individual instance of  $fe$  data,  $\max(fe)$  is the maximum absolute value of  $fe$ ,  $\min(fe)$  is the minimum

absolute value of fe, new\_max(fe) is the maximum value of the range, and new\_min(fe) is the minimum value of the range.

Phase 3: data labelling—in this phase, an early network traffic monitoring activity is performed by clustering the data into normal and anomaly using suitable algorithms such as K-means, mean-shift, and density-based spatial clustering of applications with noise (DBSCAN), to name a few. The clustering aims to prepare the dataset for the labelling process. The process of data labelling is a complex and time-consuming task [34]. This process involves distinguishing anomalies from normal data using clustering [35]. Then, the individual data instances are labelled based on the clusters identified in the clustering process. As a result, the dataset is ready for supervised machine learning of the model building in the next phase. This phase also prepared the periodical data sampling, the last phase of the cycle. The labelled data are the input for training the classification algorithms, which can automatically identify anomaly data based on what is learned [35].

Phase 4: model building—generally, deep learning models have been tested for their performance and effectiveness in classifying network traffic data and identifying attacks. They are reported in the studies like Wang *et al.* [13], Gamage and Samarabandu [16], Agarwal *et al.* [36], Gadze *et al.* [37], Khempetch and Wuttidittachotti [38], Krishna *et al.* [39], Lee *et al.* [40], Mighan and Kahani [41], Priya *et al.* [42]. Deep learning is more suitable for large datasets than machine learning and has become the most widely used IDS due to its ability to identify previously undiscovered patterns in raw data through multiple layers of modifications [43]. Specifically, this study proposed convolutional deep-learning neural networks as the deep-learning classifier for detecting DDoS attacks. It consists of artificial neurons with weight, biases and activation functions that map the input layer to the output layer [44]. Although convolutional deep-learning neural networks are commonly used in image processing, the potential of the classifier in intrusion detection has also been proven. For example, Shaaban *et al.* [45] used it to classify DDoS attacks on network traffic data at the mission control centre responsible for controlling spacecraft. The classifier had 99% of accuracy in detecting normal and malicious traffic from the network traffic data. Moreover, convolutional deep-learning neural networks are performed using the mathematical function stated in (2) [46].

$$C = [c_1, c_2, c_3, \dots, c_d]^T = K^T \otimes M \quad (2)$$

Where C is the convolutional layer, d is the distance between data points, K is the kernel matrices, M is the input matrices, win is the window matrix, and T is matrix transposition. C is derived from (3), (4), and (5).

$$K = [k_1, k_2, \dots, k_d] \quad (3)$$

$$M = [M_1^{win}, M_2^{win}, \dots, M_d^{win}] \quad (4)$$

$$c_i^j = k_i * (M_i^{win,j})^T \quad (5)$$

The deep learning model is trained using the dataset derived in the previous phase. The outcome of this phase is a deep learning model that is evaluated in the next phase of the proposed mechanism.

Phase 5: model evaluation—the developed model in the previous phase requires evaluation. Model evaluation is a complex process where the model, data set, evaluation method, and hardware and software requirements work simultaneously to maintain accuracy and performance, such as latency, throughput, and memory usage [47]. This study adapted three widely used measures for evaluating the detection model—accuracy, precision, and recall [48]. The evaluation should measure the confusion matrix that shows the correctly classified instances in true-positive (TP) and true-negative (TN) as well as the incorrectly classified instances in false-positive (FP) and false-negative (FN). In addition, the study also measures the true-positive rate (TPR), false-positive rate (FPR), true-negative rate (TNR), false-negative rate (FNR), accuracy, precision, recall, and F-measure as demonstrated by (6) to (9), respectively.

$$Accuracy = \frac{(TPR+TNR)}{(TPR+TNR+FPR+FNR)} \quad (6)$$

$$Precision = \frac{TP}{(TP+FP)} \quad (7)$$

$$Recall = \frac{TP}{(TP+FN)} \quad (8)$$

$$F1 = 2 * \frac{Precision * Recall}{Precision + Recall} \quad (9)$$

Phase 6: DDoS detection-the DDoS detector module performs its tasks in this phase. Traffic data classified as DDoS are analysed in terms of the destination ports, their frequency of occurrence over a while, packet size, and the idle period between packets. Then, it uses information stored in the attack pattern database to classify network data as normal or DDoS attacks. The output of this phase is the detection results that indicate whether a specific network traffic instance is a normal packet or a DDoS attack. Detection results are stored in the database for record and future reference. For any DDoS attack detected, the alert creation phase would be activated. If the particular DDoS incident matches one of the patterns in the database, then an alert is created by the subsequent phase in the mechanism. If none of the existing attack patterns matched, it is detected as a new pattern. Then the data are further processed in the next phase of pattern identification.

Phase 7: attack patterns identification-an attack pattern describes the exploiting computing resources method derived from the concept design patterns [49]. It is the process of identifying the detailed style of DDoS attacks, providing information about the type of attack, attack prerequisites, attack weaknesses, the knowledge required to perform an attack and details of the attack that has taken place. In other words, attack pattern identification involves recognising the formations and methods of a new incident of DDoS attacks and then naming them. Attack pattern identification requires human intervention to validate the recognised patterns and name the attack patterns before storing them in the database. Network administrators must review the generated attack patterns and verify them. This phase also creates an attack pattern rule for the associated attack incidents so that the DDoS detector can use the rule during the matching process.

Phase 8: alert creation-this phase receives the detection results performed by the DDoS detector in phase 6 as its input. It is a concurrent process with attack pattern identifications that respond to the data classified as DDoS attacks. Efficient DDoS detection systems should quickly detect unusual traffic data that could be a DDoS attack. Upon detection of the attack, alerts are created on a group of data traffic that is classified as a DDoS attack. This alert is necessary for response and notification of the incident. Hence, details about DDoS attacks are recorded, including date, time, communication protocol, application, IP source address, and port number. The role of the alerts is like a record or report that lists the occurrence of DDoS attacks for network managers' use, mainly to improve network security defence against DDoS attacks in the future.

Phase 9: notification delivery-an efficient DDoS detection and monitoring system should be equipped with a notification system that provides tools to deliver a message to a group of recipients, i.e. staff involved in network management in the organisation. Messages can be sent via e-mail, mobile phone or any specialised notification device such as a pager. However, with the advancement of smartphone technology today, it is more suitable to be used as a medium to receive messages [50] related to the possibility of DDoS attacks. For example, notifications about possible DDoS attacks can be sent to the network manager's smartphone as push messages. Network managers can receive push messages more quickly because the message appears on the screen without opening the messaging application [50]. Thus, network managers can be notified more quickly and can respond to DDoS attacks that occur.

Phase 10: periodical data sampling-the network traffic size is enormous and continuously running all the time. Hence, the large volume of traffic data is unsuitable for continual processing because it requires high computing resources to operate efficiently. Thus, sampling is a popular technique for data reduction applied in various network management aspects, including DDoS monitoring and detection. Furthermore, the volume of sampled network traffic data to be analysed is smaller than the entire data; consequently, traffic anomalies can be identified effectively [51]. Systematic sampling is one possible traffic data sampling technique. First, a dataset is developed based on the entire network traffic records taken, starting from a particular starting point to the end at the same interval. Then, each record in the sample is systematically selected from the traffic data in a fixed period. The sampling dataset is derived from (10) and (11) [51].

$$X = \{x_i\} \quad (10)$$

Where X is the entire network traffic data and  $i = 1, N$  is the sequence of elements to be sampled.

$$P_i = \begin{cases} 1, & i \bmod k = 0; \\ 0, & i \bmod k \neq 0; \end{cases} \quad (11)$$

Where  $P_i$  is the probability that the element  $x_i$  is selected for the sample, and  $k$  is the sampling period.

The position of the next element to be taken as a sample has been pre-determined. For example, traffic data at every tenth position is selected as an element in the sample. Thus, the network traffic sample is an input

for the model evaluation process in phase 5, constantly repeating at frequent intervals that the network managers can set. The flow chart illustrates the overall process of the proposed mechanism in Figure 4.

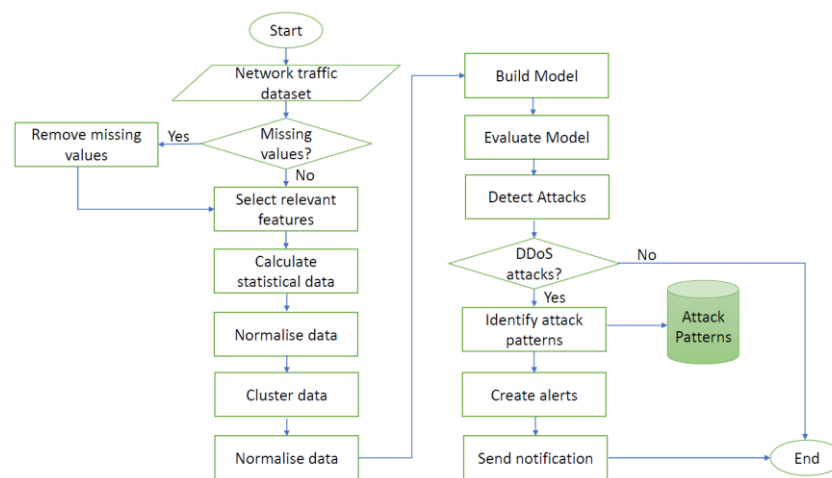


Figure 4. The general flow of the observational mechanism for DDoS attack detection and response

### 3. RESULTS AND DISCUSSION

Public network traffic data were used in the model building and evaluation phases to represent the up-to-date network traffic data with DDoS attacks. This study used the intrusion detection evaluation dataset (CIC-IDS2017) [52]–[54] owned by the Canadian Institute of Cybersecurity at the University of New Brunswick. It is among the newest dataset for DDoS attacks. Specifically, the study utilised a dataset named Friday-Working Hours-Afternoon-DDos.pcap\_ISCX. It has 79 columns representing the features of DDoS attacks, including the label and 225,745 rows of data representing the instances of the network traffic. The first phase of data pre-processing was conducted on the dataset. The data were checked for missing values, and network traffic data containing missing values were removed. Then, the feature selection of phase 2 was conducted on the dataset. This study adapted the features suggested by Panwar *et al.* [55], as listed in Table 1. Then, phase 3 on data labelling was skipped as the data had been labelled as normal and DDoS attacks. 97,718 network traffic data was labelled as normal, while 128,027 instances were labelled as DDoS attacks.

Table 1. Features of the dataset selected for the study

Feature number [55]	Feature label [55]	Description [56]
1	Destination port	"Destination port"
5	Total length of Fwd packets	"Total size of packets in the forward direction."
6	Total length of Bwd packets	"Total size of packets in the backward direction."
8	Fwd packet length min	"Minimum size of packets in the forward direction."
48	ACK flag count	"Number of packets with ACK Flag."
67	Init_Win_bytes_forward	"Number of bytes sent in the initial window in the forward direction."
68	Init_Win_bytes_backward	"Number of bytes sent in the initial window in the backward direction."
78	Idle min	"Minimum time a flow was idle before becoming active."
79	Label	"The target variable, 'Normal' or a DDoS attack."

In training and testing the deep learning model, this study used Waikato environment for knowledge analysis (WEKA), a machine learning workbench developed in 1993 [57]–[61]. It is an open-source data mining and machine learning tool developed by the University of Waikato, New Zealand. Over time, the tool has been improved to cater to researchers' needs in performing machine learning research in various domains. For example, several studies used WEKA for intrusion detection studies [62]–[64]. The WEKA Deeplearning4J package was installed on the workbench for running convolutional deep-learning neural networks. The package was developed using the Deeplearning4j Java library. WEKA was installed on Intel® Core™ i7-1165G7@2.80 GHz processor with 16 GB RAM and Windows 10 operating system.

The CSV file of "Friday-WorkingHours-Afternoon-DDos.pcap\_ISCX" of the CIC-IDS2017 dataset [52]–[54]. Then, the study performed the data pre-processing by performing feature selection, as stated in



Table 1. Then, the data training process was conducted using a ratio of 50-50, followed by the test of the deep learning model. Finally, the classification results and performance measures were derived.

The study by Shaaban *et al.* [45] that used convolutional deep-learning neural networks was not used as a benchmark because the report did not specify the features and tools used to perform the modelling and the evaluation. This study selected another similar study to benchmark the model's performance in classifying the DDoS attacks in the dataset. Ojugo and Yoro [23] adopted eight features to develop the deep neural network model using the same dataset's Python data analysis (Pandas) library. As a result, their deep neural network model had 56 rules with classification accuracy between 0.8 and 0.96. Table 2 lists the characteristics of the model of this study and the one conducted by Ojugo and Yoro [23].

Table 2. The characteristics of the selected benchmark study

Properties/studies	Ojugo and Yoro [23]	The deep learning model of the proposed observational mechanism
Dataset	CIC-IDS2017	CIC-IDS2017
Instances selected from the dataset	12,500	225,745
Attacks	DDoS	DDoS
Features selected from the dataset	<ul style="list-style-type: none"> <li>– Source IP</li> <li>– Source port</li> <li>– Destination IP</li> <li>– Destination port</li> <li>– Protocol</li> <li>– Duration</li> <li>– Packets</li> <li>– Attack Name/Type</li> </ul>	<ul style="list-style-type: none"> <li>– Destination port</li> <li>– Total Length of Fwd packets</li> <li>– Total Length of Bwd packets</li> <li>– Fwd packet length min</li> <li>– ACK flag count</li> <li>– Init_Win_bytes_forward</li> <li>– Init_Win_bytes_backward</li> <li>– Idle Min</li> <li>– Label</li> </ul>
Tools	Pandas library	WEKA Deeplearning4J

This section describes the results of the model evaluation of phase 5 in the proposed mechanism. The deep learning model was set to run on ten epochs. The deep learning network used eight neurons for the input layer and two neurons for the output layer, with eighteen trainable parameters for the training phase. It took 1599.42 seconds to build the model and 61.34 seconds to test it on the training data. The results of the training phase demonstrated that 97.21% (i.e., 219, 452) instances were correctly classified, while 2.79% (i.e., 6, 293) were incorrectly classified. The model correctly classified 91,594 normal and 127,858 DDoS activities. Thus, 91,594 and 127,858 normal and DDoS instances were correctly classified. The model predicted 6,124 instances of normal activities and classified them as DDoS. On the other hand, 169 DDoS instances were incorrectly classified as normal activities. The mean absolute error was 0.0613, and the root mean squared error was 0.1601. Table 3 shows the confusion matrix of the training phase.

Table 3. The confusion matrix of the training phase

n = 225,745	Predicted: normal	Predicted: DDoS
Actual: normal	91,594	6,124
Actual: DDoS	169	127,858

Based on the confusion matrix, the calculation of TPR, FPR, precision, recall, and F-measure were derived as rendered in Table 4. The TPR of the normal and DDoS classes were 0.937 and 0.999, respectively. On the other hand, the false alarm was very low, with 0.001 and 0.063 for normal and DDoS classes. The weighted average of precision, recall and F-measure was 0.973, 0.972, and 0.972, respectively. Overall, the result of the classification process using convolutional deep-learning neural networks demonstrated potential application in classifying normal and DDoS activities, which may lead to effective intrusion detection IDS. It should also consider this study's nine network traffic data features.

Table 4. The performance measures of the model

Class	TPR	FPR	Precision	Recall	F-measure
Normal	0.937	0.001	0.998	0.937	0.967
DDoS	0.999	0.063	0.954	0.999	0.976
Weighted Avg.	0.972	0.036	0.973	0.972	0.972



The performance of the deep learning model was also compared against the model developed by Ojugo and Yoro [23], as depicted in Table 5. Generally, the model can classify the network traffic data into normal and DDoS attacks. It also provides promising outcomes comparable to the deep learning model by Ojugo and Yoro [23]. Although the precision and recall were lower than their results, the accuracy is slightly higher. It is necessary to note that both studies applied different features in detecting DDoS in which the destination port was the only mutual feature used in both models. Therefore, there is an opportunity for other studies that can identify the optimal features for detecting DDoS from the dataset.

Table 5. The performance of the proposed model and Ojugo and Yoro [23]

Studies	The proposed mechanism	Ojugo and Yoro [23]
Accuracy	0.972	0.92
Precision	0.973	1.0
Recall	0.972	0.99

#### 4. CONCLUSION

The study proposes an observational mechanism to detect DDoS attacks from network traffic data. DDoS attacks because significant losses, including money, time, and reputational damage, and can even lead to loss of life in critical computing services. The proposed mechanism focuses on managing network traffic data to detect attack incidents through data processing and clustering. Consistent traffic data sampling helps improve the efficiency of the detection model, and the DDoS detection module compares existing attack patterns to generate new patterns and alerts the network manager if an incident is detected. The proposed approach can be improved by testing other machine learning algorithms or artificial intelligence methods, pre-processing and clustering network traffic data, and managing attack pattern identification. Overall, the proposed approach enhances an organisation's ability to monitor DDoS attack activities within their computing resources.

#### ACKNOWLEDGEMENTS

The authors thank the Ministry of Higher Education Malaysia for funding this study under the Fundamental Research Grant Scheme (Ref: FRGS/2/2014/ICT04/UUM/02/1, UUM S/O Code: 13141), and Research and Innovation Management Centre, Universiti Utara Malaysia for the administration of this study.

#### REFERENCES




- [1] T. G. C. Obasi, "Encrypted network traffic classification using ensemble learning techniques," Carleton University, Ottawa, Ontario, p. 1-184 2020, doi: 10.22215/etd/2020-14171.
- [2] B. Li, E. Erdin, M. H. Gunes, G. Bebis, and T. Shipley, "An overview of anonymity technology usage," *Computer Communications*, vol. 36, no. 12, pp. 1269–1283, Jul. 2013, doi: 10.1016/j.comcom.2013.04.009.
- [3] M. Y. Idris, A. H. Abdullah, and M. A. Maarof, "Iterative window size estimation on self-similarity measurement for network traffic anomaly detection," *International Journal of Computing & Information Sciences*, vol. 2, no. 2, pp. 84–91, 2004.
- [4] Y. Miao, Z. Ruan, L. Pan, J. Zhang, and Y. Xiang, "Comprehensive analysis of network traffic data," *Concurrency and Computation: Practice and Experience*, vol. 30, no. 5, p.1-16, Mar. 2018, doi: 10.1002/cpe.4181.
- [5] S. Y. Ji, B. K. Jeong, and D. H. Jeong, "Evaluating visualization approaches to detect abnormal activities in network traffic data," *International Journal of Information Security*, vol. 20, no. 3, pp. 331–345, Jun. 2021, doi: 10.1007/s10207-020-00504-9.
- [6] S. Y. Huang and Y. N. Huang, "Network traffic anomaly detection based on growing hierarchical SOM," in *Proceedings of the International Conference on Dependable Systems and Networks*, Jun. 2013, pp. 1–2, doi: 10.1109/DSN.2013.6575338.
- [7] Q. Yan and W. Huang, "A DDoS detection and mitigation system framework based on spark and SDN," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 10135 LNCS, 2017, pp. 350–358, doi: 10.1007/978-3-319-52015-5\_35.
- [8] A. H. Azizan *et al.*, "A machine learning approach for improving the performance of network intrusion detection systems," *Annals of Emerging Technologies in Computing*, vol. 5, no. Special issue 5, pp. 201–208, Mar. 2021, doi: 10.33166/AETiC.2021.05.025.
- [9] D. Kshirsagar and S. Kumar, "A feature reduction based reflected and exploited DDoS attacks detection system," *Journal of Ambient Intelligence and Humanized Computing*, vol. 13, no. 1, pp. 393–405, Jan. 2022, doi: 10.1007/s12652-021-02907-5.
- [10] N. H. Al-A'araji, S. O. Al-Mamory, and A. H. Al-Shakarchi, "Classification and clustering based ensemble techniques for intrusion detection systems: A survey," *Journal of Physics: Conference Series*, vol. 1818, no. 1, p. 1-35, Mar. 2021, doi: 10.1088/1742-6596/1818/1/012106.
- [11] S. Das, A. M. Mahfouz, D. Venugopal, and S. Shiva, "DDoS intrusion detection through machine learning ensemble," in *Proceedings - Companion of the 19th IEEE International Conference on Software Quality, Reliability and Security, QRS-C 2019*, Jul. 2019, pp. 471–477, doi: 10.1109/QRS-C.2019.00090.
- [12] S. Anwar *et al.*, "From intrusion detection to an intrusion response system: Fundamentals, requirements, and future directions," *Algorithms*, vol. 10, no. 2, p. 1-24, Mar. 2017, doi: 10.3390/a10020039.
- [13] Z. Wang, Y. Liu, D. He, and S. Chan, "Intrusion detection methods based on integrated deep learning model," *Computers and Security*, vol. 103, p. 1-34, Apr. 2021, doi: 10.1016/j.cose.2021.102177.
- [14] O. E. Elejla, M. Anbar, B. Belaton, and S. Hamouda, "Labeled flow-based dataset of ICMPv6-based DDoS attacks," *Neural*

- Computing and Applications*, vol. 31, no. 8, pp. 3629–3646, Aug. 2019, doi: 10.1007/s00521-017-3319-7.
- [15] N. Bindra and M. Sood, "Evaluating the impact of feature selection methods on the performance of the machine learning models in detecting DDoS attacks," *Romanian Journal of Information Science and Technology*, vol. 23, no. 3, pp. 250–261, 2020.
  - [16] S. Gamage and J. Samarabandu, "Deep learning methods in network intrusion detection: A survey and an objective comparison," *Journal of Network and Computer Applications*, vol. 169, p. 1–21, Nov. 2020, doi: 10.1016/j.jnca.2020.102767.
  - [17] S. Mahadik, P. M. Pawar, and R. Muthalagu, "Efficient intelligent intrusion detection system for heterogeneous internet of things (HetIoT)," *Journal of Network and Systems Management*, vol. 31, no. 1, p. 2, Jan. 2023, doi: 10.1007/s10922-022-09697-x.
  - [18] H. Greenspan, B. V. Ginneken, and R. M. Summers, "Guest editorial deep learning in medical imaging: Overview and future promise of an exciting new technique," *IEEE Transactions on Medical Imaging*, vol. 35, no. 5, pp. 1153–1159, May 2016, doi: 10.1109/TMI.2016.2553401.
  - [19] Y. Lecun, Y. Bengio, and G. Hinton, "Deep learning," *Nature*, vol. 521, no. 7553, pp. 436–444, May 2015, doi: 10.1038/nature14539.
  - [20] I. Goodfellow, Y. Bengio, A. Courville, and Y. Bengio, *Deep learning*. diacriTech, Chennai, United States of America 2016.
  - [21] F. Emmert-Streib, Z. Yang, H. Feng, S. Tripathi, and M. Dehmer, "An introductory review of deep learning for prediction models with big data," *Frontiers in Artificial Intelligence*, vol. 3, p. 1–23 Feb. 2020, doi: 10.3389/frai.2020.00004.
  - [22] A. Shrestha and A. Mahmood, "Review of deep learning algorithms and architectures," *IEEE Access*, vol. 7, pp. 53040–53065, 2019, doi: 10.1109/ACCESS.2019.2912200.
  - [23] A. A. Ojugo and R. E. Yoro, "Forging a deep learning neural network intrusion detection framework to curb the distributed denial of service attack," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 11, no. 2, pp. 1498–1509, Apr. 2021, doi: 10.11591/ijece.v11i2.
  - [24] B. Alothman, "Raw network traffic data preprocessing and preparation for automatic analysis," in *2019 International Conference on Cyber Security and Protection of Digital Services, Cyber Security 2019*, Jun. 2019, pp. 1–5, doi: 10.1109/CyberSecPODS.2019.8885333.
  - [25] M. Arshey and K. S. Angel Viji, "An optimization-based deep belief network for the detection of phishing e-mails," *Data Technologies and Applications*, vol. 54, no. 4, pp. 529–549, Jul. 2020, doi: 10.1108/DTA-02-2020-0043.
  - [26] M. S. Sainin, R. Alfred, and F. Ahmad, "Ensemble meta classifier with sampling and feature selection for data with multiclass imbalance problem," *Journal of Information and Communication Technology*, vol. 20, no. 2, pp. 103–133, Feb. 2021, doi: 10.32890/jict2021.20.2.1.
  - [27] H. Almazini and K. R. Ku-Mahamud, "Grey wolf optimization parameter control for feature selection in anomaly detection," *International Journal of Intelligent Engineering and Systems*, vol. 14, no. 2, pp. 474–483, Apr. 2021, doi: 10.22266/ijies2021.0430.43.
  - [28] C. Kemp, C. Calvert, T. M. Khoshgoftaar, and J. L. Leevy, "An approach to application-layer DoS detection," *Journal of Big Data*, vol. 10, no. 1, p. 2–30, Feb. 2023, doi: 10.1186/s40537-023-00699-3.
  - [29] A. Shiravani, M. H. Sadreddini, and H. N. Nahook, "Network intrusion detection using data dimensions reduction techniques," *Journal of Big Data*, vol. 10, no. 1, p. 1–25, Mar. 2023, doi: 10.1186/s40537-023-00697-5.
  - [30] M. A. Basir, M. S. Hussin, and Y. Yusof, "Integrated bio-search approaches with multi-objective algorithms for optimization and classification problem," *Telkomnika (Telecommunication Computing Electronics and Control)*, vol. 18, no. 5, pp. 2421–2431, Oct. 2020, doi: 10.12928/TELKOMNIKA.V18I5.15141.
  - [31] M. A. Basir, M. S. Hussin, and Y. Yusof, "Ensemble feature selection method Based on bio-inspired algorithms for multi-objective classification problem," in *Advances in Intelligent Systems and Computing*, vol. 1188, 2021, pp. 167–176, doi: 10.1007/978-981-15-6048-4\_15.
  - [32] M. A. Basir, Y. Yusof, and M. S. Hussin, "Optimization of attribute selection model using bio-inspired algorithms," *Journal of Information and Communication Technology*, vol. 18, no. 1, pp. 35–55, Jan. 2019, doi: 10.32890/jict2019.18.1.8280.
  - [33] S. Khan, A. Gani, A. W. A. Wahab, and P. K. Singh, "Feature selection of denial-of-service attacks using entropy and granular computing," *Arabian Journal for Science and Engineering*, vol. 43, no. 2, pp. 499–508, Feb. 2018, doi: 10.1007/s13369-017-2634-8.
  - [34] K. Shiimoto, "Network intrusion detection system based on an adversarial auto-encoder with few labeled training samples," *Journal of Network and Systems Management*, vol. 31, no. 1, p. 5, Jan. 2023, doi: 10.1007/s10922-022-09698-w.
  - [35] A. Feizollah, N. B. Anuar, R. Salleh, and F. Amalina, "Comparative study of k-means and mini batch k-means clustering algorithms in android malware detection using network traffic analysis," in *Proceedings - 2014 International Symposium on Biometrics and Security Technologies, ISBAST 2014*, Aug. 2015, pp. 193–197, doi: 10.1109/ISBAST.2014.7013120.
  - [36] A. Agarwal, M. Khari, and R. Singh, "Detection of DDOS attack using deep learning model in cloud storage application," *Wireless Personal Communications*, vol. 127, no. 1, pp. 419–439, Nov. 2022, doi: 10.1007/s11277-021-08271-z.
  - [37] J. D. Gadze, A. A. Bamfo-Asante, J. O. Agyemang, H. Nunoo-Mensah, and K. A.-B. Opare, "An investigation into the application of deep learning in the detection and mitigation of DDOS attack on SDN controllers," *Technologies*, vol. 9, no. 1, p. 1–22, Feb. 2021, doi: 10.3390/technologies9010014.
  - [38] T. Khempetch and P. Wuttidittachotti, "Ddos attack detection using deep learning," *IAES International Journal of Artificial Intelligence*, vol. 10, no. 2, pp. 382–388, Jun. 2021, doi: 10.11591/ijai.v10.i2.pp382-388.
  - [39] A. Krishna, M. A. Ashik Lal, A. J. Mathewkutty, D. S. Jacob, and M. Hari, "Intrusion detection and prevention system using deep learning," in *Proceedings of the International Conference on Electronics and Sustainable Communication Systems, ICESC 2020*, Jul. 2020, pp. 273–278, doi: 10.1109/ICESC48915.2020.9155711.
  - [40] T. H. Lee, L. H. Chang, and C. W. Syu, "Deep learning enabled intrusion detection and prevention system over SDN networks," in *2020 IEEE International Conference on Communications Workshops, ICC Workshops 2020 - Proceedings*, Jun. 2020, pp. 1–6, doi: 10.1109/ICCWorkshops49005.2020.9145085.
  - [41] S. N. Mighan and M. Kahani, "A novel scalable intrusion detection system based on deep learning," *International Journal of Information Security*, vol. 20, no. 3, pp. 387–403, Jun. 2021, doi: 10.1007/s10207-020-00508-5.
  - [42] G. M. Priya, S. M. Shalinie, and P. M. Priya, "Deep learning framework for early detection of intrusion in virtual environment," *International Journal of Business Intelligence and Data Mining*, vol. 17, no. 3, pp. 393–411, 2020, doi: 10.1504/IJBIDM.2020.109296.
  - [43] A. S. Dina, A. B. Siddique, and D. Manivannan, "A deep learning approach for intrusion detection in Internet of things using focal loss function," *Internet of Things (Netherlands)*, vol. 22, p. 100699, Jul. 2023, doi: 10.1016/j.iot.2023.100699.
  - [44] S. K. Pandey and R. R. Janghel, "Classification of electrocardiogram signal using an ensemble of deep learning models," *Data Technologies and Applications*, vol. 55, no. 3, pp. 446–460, Jun. 2021, doi: 10.1108/DTA-05-2020-0108.
  - [45] A. R. Shaaban, E. Abd-Elwanis, and M. Hussein, "DDoS attack detection and classification via convolutional neural network




- (CNN)," in *Proceedings - 2019 IEEE 9th International Conference on Intelligent Computing and Information Systems, ICICIS 2019*, Dec. 2019, pp. 233–238, doi: 10.1109/ICICIS46948.2019.9014826.
- [46] P. Wang *et al.*, "Semantic clustering and convolutional neural network for short text categorization," in *ACL-IJCNLP 2015 - 53rd Annual Meeting of the Association for Computational Linguistics and 7th International Joint Conference on Natural Language Processing of the Asian Federation of Natural Language Processing, Proceedings of the Conference - Short Paper*, 2015, pp. 352–357, doi: 10.3115/v1/p15-2058.
- [47] A. Dakkak, C. Li, J. Xiong, and W. Hwu, "MLModelScope: a distributed platform for model evaluation and benchmarking at scale," *arXiv e-prints*, p. 1-16, 2020, [Online]. Available: <http://arxiv.org/abs/2002.08295>, doi: 10.48550/arXiv.2002.08295.
- [48] R. Ma, X. Chen, and R. Zhai, "A DDoS attack detection method based on natural selection of features and models," *Electronics (Switzerland)*, vol. 12, no. 4, p. 1059, Feb. 2023, doi: 10.3390/electronics12041059.
- [49] A. Madhuri and L. A. Ramana, "Attack patterns for detecting and preventing ddos and replay attacks," *International Journal of Engineering Science and Technology*, vol. 2, no. 9, pp. 4850–4859, 2010.
- [50] N. Katuk, N. H. Zakaria, and K.-R. Ku-Mahamud, "Mobile phone sensing using the built-in camera," *International Journal of Interactive Mobile Technologies (IJIM)*, vol. 13, no. 02, p. 1-13, Feb. 2019, doi: 10.3991/ijim.v13i02.10166.
- [51] A. N. Mahmood, J. Hu, Z. Tari, and C. Leckie, "Critical infrastructure protection: resource efficient sampling to improve detection of less frequent patterns in network traffic," *Journal of Network and Computer Applications*, vol. 33, no. 4, pp. 491–502, Jul. 2010, doi: 10.1016/j.jnca.2010.01.003.
- [52] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "Toward generating a new intrusion detection dataset and intrusion traffic characterization," in *ICISSP 2018 - Proceedings of the 4th International Conference on Information Systems Security and Privacy*, 2018, vol. 2018-Janua, pp. 108–116, doi: 10.5220/0006639801080116.
- [53] R. Panigrahi and S. Borah, "A detailed analysis of CICIDS2017 dataset for designing intrusion detection systems," *International Journal of Engineering and Technology(UAE)*, vol. 7, no. 3.24 Special Issue 24, pp. 479–482, 2018.
- [54] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "A detailed analysis of the CICIDS2017 data set," in *Communications in Computer and Information Science*, vol. 977, 2019, pp. 172–188, doi: 10.1007/978-3-030-25109-3\_9.
- [55] 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," *SSRN Electronic Journal*, p. 1-10, 2019, doi: 10.2139/ssrn.3394103.
- [56] N. O. Mathur, "Application of autoencoder ensembles in anomaly and intrusion detection using time-based analysis," University of Cincinnati, p. 1-18, 2020.
- [57] S. Lang, F. Bravo-Marquez, C. Beckham, M. Hall, and E. Frank, "WekaDeeplearning4j: a deep learning package for Weka based on Deeplearning4j," *Knowledge-Based Systems*, vol. 178, pp. 48–50, Aug. 2019, doi: 10.1016/j.knosys.2019.04.013.
- [58] E. Frank, M. A. Hall, and I. H. Witten, "The WEKA workbench," in *Data Mining: Practical Machine Learning Tools and Techniques*, 2017, pp. 553–571, doi: 10.1016/b978-0-12-804291-5.00024-6.
- [59] M. Hall, E. Frank, G. Holmes, B. Pfahringer, P. Reutemann, and I. H. Witten, "The WEKA data mining software," *ACM SIGKDD Explorations Newsletter*, vol. 11, no. 1, pp. 10–18, Nov. 2009, doi: 10.1145/1656274.1656278.
- [60] G. Holmes, A. Donkin, and I. H. Witten, "WEKA: a machine learning workbench," in *Proceedings of ANZIIS '94 - Australian New Zealand Intelligent Information Systems Conference*, pp. 357–361, doi: 10.1109/ANZIIS.1994.396988.
- [61] I. H. Witten, E. Frank, L. E. Trigg, M. A. Hall, G. Holmes, and S. J. Cunningham, "Weka: practical machine learning tools and techniques with java implementations," 1999.
- [62] Z. Zainudin, S. M. Shamsuddin, and S. Hasan, "Deep learning for image processing in WEKA environment," *International Journal of Advances in Soft Computing and its Applications*, vol. 11, no. 1, pp. 1–21, 2019.
- [63] M. K. Vanam, B. A. Jiwani, A. Swathi, and V. Madhavi, "WITHDRAWN: High performance machine learning and data science based implementation using Weka," *Materials Today: Proceedings*, p. 1-7, Feb. 2021, doi: 10.1016/j.matpr.2021.01.470.
- [64] S. Farhat, M. Abdelkader, A. Meddeb-Makhlouf, and F. Zarai, "Comparative study of classification algorithms for cloud IDS using NSL-KDD dataset in WEKA," in *2020 International Wireless Communications and Mobile Computing, IWCMC 2020*, Jun. 2020, pp. 445–450, doi: 10.1109/IWCMC48107.2020.9148311.

## BIOGRAPHIES OF AUTHORS






**Norliza Katuk**    obtained her bachelor's degree in information technology from University Utara Malaysia in 2000 and her master's degree in computer science from Universiti Teknologi Malaysia in 2002. She obtained her Doctoral degree in information technology from Massey University, New Zealand, in 2012. She is an associate professor at the School of Computing, Universiti Utara Malaysia. Her research interests cover multidisciplinary areas, including information security and privacy, cybersecurity awareness, Internet technology, IoT, disaster management, e-learning and human-computer interaction. She can be contacted at email: [k.norliza@uum.edu.my](mailto:k.norliza@uum.edu.my).






**Mohamad Sabri Sinal**    is a senior lecturer at School of Computing Universiti Utara Malaysia. He obtained his PhD in Bioinformatics from Shibaura Institute of Technology, Tokyo, Japan. He conducted research related to electrocardiography, electrocardiogram, artificial neural networks, atrial fibrillation, computational intelligence, and heart failure. He can be contacted at email: [msabri@uum.edu.my](mailto:msabri@uum.edu.my).



**Mohammed Gamal Ahmed Al-Samman**    is an international lecturer at Universiti Utara Malaysia. He received his bachelor's degree in computer Engineer and Information Technology from Sana'a University, Yemen, a master's degree in Information Technology, and a PhD in computer science (specialising in Networked Computing) from Universiti Utara Malaysia. His research area of interest includes future internet architecture like information-centric networks, named data networks, and their impacts on the internet of things, vehicular adhoc networks blockchain, and network security research. Other research areas include internet governance, information security, and the machine learning field. He can be contacted at email: [alsamman@uum.edu.my](mailto:alsamman@uum.edu.my).



**Ijaz Ahmad**    has completed his bachelor's in computer science with distinction. Later, he completed his MS in Information Security from the National University of Sciences and Technology, Pakistan. Since 2013, he has been working as Director of Quality Assurance and Senior Lecturer in the Faculty of Information Technology at Majan University College, Oman. He is also a Senior Fellow of the UK Higher Education Academy AdvanceHE. His areas of interest include cyber security, ethical hacking, cryptography, cloud computing and social media analytics. He can be contacted at email: [ijaz.ahmad@majancollege.edu.om](mailto:ijaz.ahmad@majancollege.edu.om).