

DDoS attacks detection using machine learning and deep learning techniques: analysis and comparison

Mahmood A. Al-Shareeda¹, Selvakumar Manickam¹, Murtaja Ali Saare²

¹National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia, Penang, Malaysia

²Department of Computer Technology Engineering, Shatt Al-Arab University College, Basrah, Iraq

Article Info

Article history:

Received Jul 26, 2022

Revised Sep 30, 2022

Accepted Nov 3, 2022

Keywords:

Deep learning

Distributed denial of service

Intrusion detection system

Machine learning

ABSTRACT

The security of the internet is seriously threatened by a distributed denial of service (DDoS) attacks. The purpose of a DDoS assault is to disrupt service and prevent legitimate users from using it by flooding the central server with a large number of messages or requests that will cause it to reach its capacity and shut down. Because it is carried out by numerous bots that are managed (infected) by a single botmaster using a fake IP address, this assault is dangerous because it does not involve a lot of work or special tools. For the purpose of identifying and analyzing DDoS attacks, this paper will discuss various machine learning (ML) and deep learning (DL) techniques. Additionally, this study analyses and comparatives the significant distinctions between ML and DL techniques to aid in determining when one of these techniques should be used.

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



Corresponding Author:

Selvakumar Manickam

National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia

Gelugor, Penang, Malaysia

Email: selva@usm.my

1. INTRODUCTION

Numerous significant websites have recently been subjected to outside attacks. Because they cannot afford any neglect, not even for a brief period, many large corporations and government agencies are exposed [1]–[4]. The present network services should be less susceptible to attacks as a result of any flaws that could result in significant losses for both customers and businesses. Not all modern attacks have the same old goals as making money or getting sensitive information. Some of them are designed to halt services so that users can no longer use the intended service as long as the attacker can do so [5]–[7].

A single botmaster can command a large number of bots (zombies) to transmit a large volume of messages that completely consume the bandwidth in a distributed denial of service (DDoS) assault [8]–[10]. The primary target of a DDoS attack is the central service point. This kind of attack happens extremely quickly. As a result, detecting DDoS attacks is a significantly better security tactic than detecting crackers. DDoS attacks, however, are also updated in tandem with the development of security measures [11]–[13]. Since the former relies solely on the detection of anomalies or anomalous behavior, anomaly-based detection is thought to be more modern than signature-based detection in response to that [14]–[16]. The main motivation of this paper is to investigate the most often used machine learning (ML) and deep learning (DL) techniques for intrusion detection system (IDS), as well as to discuss when it is appropriate to employ each type of technique. The major contributions of this work are listed as follows: i) we present and analyze the related work based on ML and DL to detect DDoS attacks in detail; ii) we display the outcomes of both DL and ML methods based on IDS or DDoS attack detection; and iii) we draw attention to the clear distinctions between DL and ML methods.

The remainder of this paper is structured as follows. Section 2 describes IDS and DDoS attacks in details. We present the summaries of ML and DL approaches based on related works in sections 3 and 4, receptivity. Section 5 discuss the related work based on ML and DL approaches. Finally, section 6 concludes this paper.

2. BACKGROUND

2.1. Intrusion detection system

Strategically designed IDS watch network traffic for signs of attacks. IDS will examine the packets to find any potential risks after gathering information from networks and watching the traffic. The IDS can be categorized in a variety of ways, according to various studies, including Debar *et al.* [17] and Hindy *et al.* [18]. They have previously developed questionnaires and taxonomies to categorize IDS. This study will be based on the classification of [19], where they combined a sober classification with earlier trustworthy classifications and added DL to it. Host-based, network-based, or a hybrid of the two are the three types of data collection. On the basis of location, these sources are grouped. The IDS come in two different models. First, IDS is based on signatures (SIDS), which is reliant on appearances prior to attacks. Without possessing the attacks' specific signatures, this style cannot detect attacks. Anomaly-based IDS (AIDS), the second approach, does not rely on plans of attack, in contrast to the signature-based model.

This paper will focus on anomaly-based IDS, which is the most effective strategy. One of AIDS's most frequently cited benefits is its capacity to identify previously unidentified attacks by spotting an anomaly in network traffic. From a different angle, AIDS might be an IDS that is either self-learning or programmed. By developing a method for the fundamental operations with the allocated network traffic accumulated over a constrained period of time, self-learning AIDS is accomplished [20]. More specifically, users are the ones who decide how out of the ordinary a behaviour is in the system [21].

2.2. Distributed denial of service attack

DDoS attacks intimidate networks at the moment since they target sensitive and significant centers. Furthermore, DDoS attacks are growing quickly, leaving little time for a proper response [22], [23]. New DDoS launch platforms, such Ox-booter, appeared in late 2018, according to Kaspersky Lab. These services support attacks with additional bandwidth of up to 420 Gb/s and more than 16,000 infected bots. Due to its simplicity and low price, this platform is extremely risky. Anyone can use this straightforward interface to execute one of numerous attacks against their target for only \$20 to \$50. Due to the low cost, attackers today do not need specialised tools or extra effort to damage their target. To put it another way, these illicit platforms that promote DDoS attacks were using internet of things (IoT) devices to conduct this attack [24]. Additionally, a DDoS attack is simple to execute because to the IoT, which allows the Internet to pervade practically every aspect of human existence [25].

2.3. DDoS attack

DDoS attacks are currently regarded as the most dangerous assaults on the internet. DDoS attack perpetrators try to stop authorised users from using services. These attacks pose a risk due to the possibility of simultaneous attack from multiple sources. Therefore, until it is blocked, it will be hard to reveal the actual IP address that causes this harm. DDoS assaults also use legitimate channels to send a tonne of messages. When this happens, the packets will come from trustworthy websites like colleges or companies that cannot be censored or shut down [26]. DDoS assault is simply depicted in Figure 1.

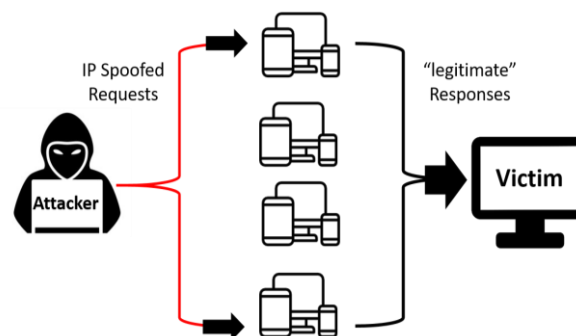


Figure 1. DDoS attacks

Think of the hypothetical situations where victim 'Y' has an IP address of 2.2.2.2 and attacker 'X' has an IP address of 1.1.1.1. Using IP address 'Y,' 'X' can send request packets to example.com. Then, "X" requests information from example.com, such as "tell me all you know about 'Z,'" in addition to saying "hello." Following that, example.com will give 'Y' IP address a tonne of information that the attackers don't actually need. Additionally, an attacker "X" can request that example.com, example1.com, and example2.com give him or her "Y's IP address with a massive data set that is larger than "Y's" actual storage space." One outcome is that "Y" might not be able to respond to inquiries or carry out his duties [27]. Figure 2 illustrates the types of DDoS attacks with their examples. DDoS assaults typically fall into one of three categories: i) volume-based attacks, attacks that flood a target with a large volume of traffic in an effort to take advantage of its bandwidth; ii) protocol-based attacks, attacks that take advantage of a layer 3 or layer 4 vulnerability by consuming the processing power of the attacker target or middle-level crucial resources like a firewall, which can result in service interruption; and iii) application layer attacks, attacks that connect to a victim in a reasonable way to take advantage of a vulnerability in layer 7 and use transactions and monopolising processes to overtax the server's resources.

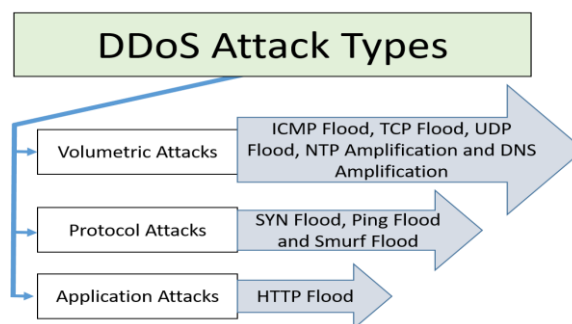


Figure 2. DDoS attack types with their examples

3. MACHINE LEARNING BASED FOR IDS

Because a signature-based IDS takes a long time to develop, test, and deploy everytime an unexpected assault happens, there is an urgent need to rely on less human reliant solutions in IDS. By offering a system that can learn from data and deliver predictions about the unseen data by employing the learnt data, anomaly-based IDS based on ML technology provides a solution for this problem [28]. The most typical use of ML techniques will be covered in the sentences that follow. Additionally, a detailed description of each approach used in IDS will be added along with recent relevant publications [29]. The several types of ML IDS are shown in Figure 3. Table 1 lists the method and advantage of ML approaches in details.

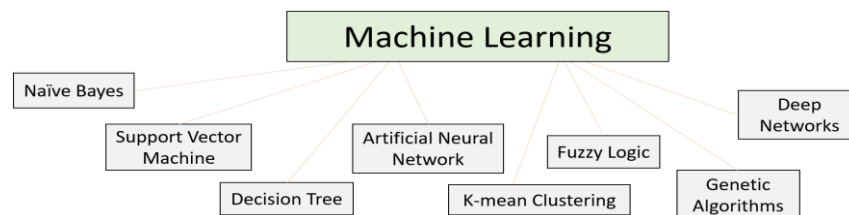


Figure 3. ML techniques

3.1. Naive Bayes

The classification procedure is carried out using this technique, which is based on bayesian networks. Naive Bayes (NB) is regarded as the simplest and most straightforward method for creating classifiers. Class labels for issue scenarios are specified by the classifiers. The classifier then displays feature value vectors. The class labels will have been drawn based on a few particular sets. Fadhil *et al.* [30] suggested a method for developing DDoS attack detection that involved statistically analysing network traffic using NB. As a properly designed, practically implemented model for DDoS attack detection, in [31] also used the NB classifier.

Table 1. Method and advantage of ML approaches

	Method	Advantage
Fadlil <i>et al.</i> [30]	Create a new method for detecting DDoS attacks.	Anticipated to function in conjunction with IDS to forecast the occurrence of DDoS attacks.
Ye <i>et al.</i> [32]	It is followed by the extraction of the switch flow table's 6-tuple characteristic values and the creation of a DDoS attack model.	Our work is useful for identifying DDoS attacks in software defined networking (SDN).
Lucky <i>et al.</i> [33]	Deployed in low-cost settings for effective, speedy detection and mitigation of DDoS attacks.	The design is examined, and the findings demonstrate that the new architecture adds no extra burden to the monitored network.
Putri <i>et al.</i> [34]	On the testbed ISCX dataset, Snort finds up to 42 alerts of a DoS assault.	Because of the disparity in accuracy between value and the clustering tool WEKA, mneg-cluster data packets are randomly chosen from a data value pack and utilised to calculate the centroid's value.
Chaudhary and Shrimal [35]	The goal of this study is to create a genetic algorithm-based IDS for DDoS attacks in MANETs.	According to the implementation results, the suggested IDS, which is based on evolutionary algorithms, can effectively identify DDoS attacks on MANETs.

3.2. Support vector machine

Vapnik was the first to suggest this approach, and since then it has shown excellent outcomes to garner more interest in ML research. SVM can perform regression and classification using supervised learning [36]. A dataset that includes the DDoS assault was produced by Subbulakshmi *et al.* [37] who subsequently worked to identify this attack using enhanced support vector machines (ESVM). By merging the SVM classification techniques, Ye *et al.* [32] created a model for DDoS attack detection in 2018.

3.3. Decision tree

One of the most popular and basic methods used in data mining and ML is the decision tree. The category-targeted value is determined using observations about a category and a decision tree as a protection mechanism. As a result, it will categorise data in accordance with the previously learnt dataset [38]. A decision tree-based method was created by Zekri *et al.* [39] for automatically and successfully identifying signature-based DDoS flooding assaults. A ML model capable of learning from assault patterns according to both anomaly-based DDoS attack detection and signature-based DDoS attack detection were created in [32] as well, taking advantage of both of their advantages.

3.4. Artificial neural network

In order to execute computational tasks, a set of basic neurons were originally introduced to artificial neural network (ANN) in 1943 by McCulloch and Pitts. These neurons had functioning that was identical to that of biological neurons, and they resembled biological networks [40]. In order to identify and mitigate known and unidentified DDoS attacks in a real-time setting, Saied *et al.* [41] developed a model. Seven writers created a paradigm for danger assessment of IoT utilising ANN to counter these attacks within the framework of [42].

3.5. K-mean clustering

One of the most popular methods for dividing a dataset into K groups is clustering. This approach refines the K initial cluster centers in a data set by each case that will enter the nearest cluster center after first identifying the initial cluster centres. To identify DDoS attacks of unknown sessions, Hao *et al.* [43] developed a detection algorithm. Suggested a method for identifying DDoS attacks using the clustering algorithm of K-means, and they attained a 97.83% accuracy rate [33].

3.6. Fuzzy logic

This method was developed using fuzzy set theory. This theory's reasoning, which is based on conventional predicate logic, is approximate rather than precise. In order to distinguish malicious packets from legitimate traffic and take appropriate action to prevent DDoS attacks, Iyengar and Ganapathy [44] developed a fuzzy logic model according to a set of predetermined rules. A mechanism for anticipating and detecting DDoS assaults in IEEE 802.15.4 was developed by an author of Balarengadurai and Saraswathi [45] by utilising fuzzy logic algorithm.

3.7. Genetic algorithms

One of the most common ML methods that is according to evolutionary concepts is this algorithm. To put it more plainly, this method approaches problem-solving much like a biological examination [46]. A developed method based on evolutionary algorithms for DDoS attack detection in mobile ad hoc networks was proposed by Chaudhary and Shrimal [34] in 2019. A scalable, real-time traffic mode analysis based on

evolutionary algorithms has been developed by [47] for the detection and mitigation of DDoS assaults on the Hadoop distributed processing infrastructure.

4. DEEP LEARNING BASED FOR IDS

As an early technique to identify aberrant behaviour in a network, ML-based intrusion detection methods were criticised for their shortcomings, including low throughput and high false positive rates. It has been demonstrated that deep networks offer benefits through the traditional detection based on ML techniques in hodo’s study of intrusion detection technologies [19]. A method is utilised to train layers of hierarchical networks utilising unsupervised learning greedily with prehensility, taking inspiration from the human brain. Other methods that rely on the fundamentals of DL have been developed since the discovery of deep networks. Deep networks architecture has typically been divided into two categories: generative architecture and discriminative architecture [19]. The two primary structures and the included approaches are shown in Figure 4. Table 2 lists method and advantage of DL approaches in details.

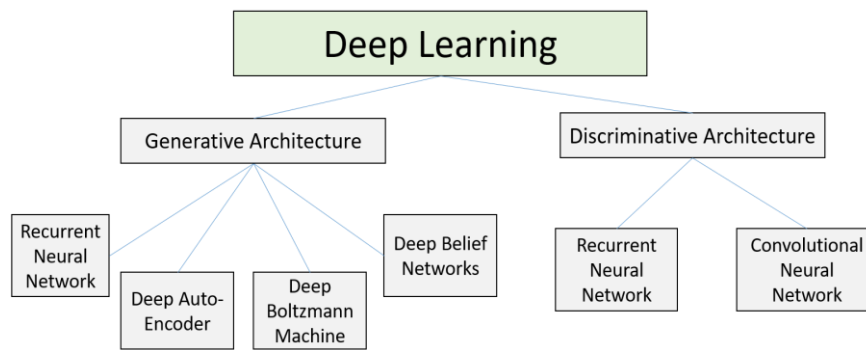


Figure 4. DL techniques

Table 2. Method and advantage of DL techniques

	Method	Advantage
Tang <i>et al.</i> [48]	An IDS for SDNs that is enabled by gated recurrent unit RNN (GRU-RNN)	Our test findings demonstrate that the proposed GRU-RNN does not impair network performance
Farahnakian and Heikkonen [49]	A strategy that uses DL for IDS. One of the most well-known DL models is used in our method, called DAE	To prevent overfitting and local optimum, the proposed DAE model is trained in a greedy layer-wise manner
Elsaeidy <i>et al.</i> [50]	A system for smart city intrusion detection based on restricted boltzmann machines (RBMs)	The effectiveness of the suggested method in very accurate attack detection. Additionally, the suggested approach performs better than the classification model used without the features learning stage
Imamverdiyev and Abdullayeva [51]	Comparison of the suggested method’s accuracy with that of gaussian-bernoulli RBM, DBN type DL approaches, and bernoulli-bernoulli RBM on DoS attack detection is provided	The suggested multilayer deep gaussian-bernoulli type RBM yields higher accuracy.
Liu <i>et al.</i> [52]	To increase the validity and effectiveness of feature extraction, a convolutional neural network (CNN) modelling approach for intrusion detection was applied. The convolution kernel was chosen and convolved with the data to extract local correlation	The new approach can raise classification accuracy for jobs involving intrusion detection and recognition
Mohammadpour <i>et al.</i> [53]	Suggest using DL to create an efficient and adaptable network intrusion detection system (NIDS)	The learning process for IDS can be used with CNNs (IDSs)

4.1. Generative architecture

The goal of generative models is to depict the existing systems graphically. These graphical representations show distributional dependence. These graphs have nodes and arcs in them. The relationships

between the nodes, which can have millions of parameters, are represented by arcs, which stand in for random variables [54], [55].

The shared statistical distribution thus represents the nodes' and their associated variables' products [56]. In addition, there are factors that are hidden from view in the graphical models. The labels of the data are not necessary for generative model training. These models are therefore connected to supervised learning. For classification purposes, these models go through an unsupervised learning pre-training stage. The lower layers were taught separately from the other layers during a pre-training step, enabling the other layers to be trained one layer at a time, starting at the bottom and working up. After pre-training, all subsequent layers will be trained [56]. Deep auto-encoders (DAE), recurrent neural networks (RNN), deep belief networks (DBN) and deep boltz-mann machines (DBM) are the four sub-classes of generative models.

4.1.1. Recurrent neural network

Both supervised and unsupervised deep generative networks fall under this category. In order to boost model dependability, the RNN model uses a sort of architecture called a feedback loop that links layers one after another in addition to storing the data from the most recent input [57]. IDS was trained using KDD Cup'99 by [58] utilising RNN with long short-term memory (LSTM) architecture. In SDN-based networks in 2018, Tang *et al.* [48] used RNN for IDS.

4.1.2. Deep auto-encoder

One of the categories of generative models is DAE. There are various variations, including stacked auto-encoder and denoising auto-encoder [59]. To avoid learning its identity function, the auto-encoder trains in a bottleneck structure where the hidden layer is more tethered than the input layer [60].

The proposed method, which relies on a DAE to detect attacks, was tested using the NSL-KDD dataset in [61]. In order to aid in the detection of intrusions, this experiment employed bottleneck characteristics to the dimensionality reduction of the large amount of data. Using a DAE, Farahnakian and Heikkonen [49] developed a solution for an IDS in 2018.

4.1.3. Deep boltzmann machine

When trained on a large volume of unlabeled data and fine-tuned with labelled data, DBM is one of the generative architectures that is regarded as a decent classifier. A link exists between the input units and the hidden units in DBM but not between units on the same layer. DBM is therefore a unidirectional graphical model [62]. Deep RBM was used by Elsaedy *et al.* [50] in 2019 to extract high-level characteristics. After that, apply the newly learnt features to the identification of various DDoS attacks. The deep RBM model's learned features were quite useful and noteworthy. An approach to identify DoS attacks based on a deep RBM model was proposed in 2018 by Imamverdiyev *et al.* [51].

4.1.4. Deep belief networks

DBN is created by stacking DBM with one or more hidden layers. Using data that has been labelled, RBMs can learn a common probability distribution of training data. It is regarded as a probabilistic generative model as a result [63]. To minimise the dimensionality of the features in this work [64], they have chosen features layer by layer using the DBN technique. The capabilities of DBN were used by Alom *et al.* [65] for intrusion detection. The proposed approach, which was evaluated on the NSL-KDD dataset, is capable of both detecting and categorising assaults.

4.2. Discriminative architecture

The second class of deep network architecture is discriminative architecture. The discriminative power of this model, which is determined by describing the posterior distributions of conditioned classes from the input data, determines how well it can classify data. Discriminative architecture has two subclasses: RNN and CNNs.

4.2.1. Recurrent neural network

In order to convert the output of an RNN employed as a discriminative model for training data into labelled data, pre-segmentation and post-processing are necessary. When the output data explicitly follows the input data sequence and is labelled, RNN also uses the discriminative power for classification [66].

4.2.2. Convolutional neural network

CNN is the second kind of discriminative deep networks, along with several convolutional and gathering layers stacked in an array to produce a multi-layer neural network [65], [67]. The max pooling layer should come after each convolutional layer. Finally, the fully-connected layer is formed nonlinearly by stacking various traditional and max pooling layers in the neural system [68]. KDD Cup'99 was utilised by

Liu *et al.* [52] to test the CNN-based suggested model. A powerful and adaptable NIDS that uses CNN was proposed by Mohammadpour *et al.* [53] for use with the NSL-KDD dataset.

5. RESULTS AND DISCUSSION

In this section, we present the summaries of ML and DL approaches based related works mentioned in sections 3 and 4, respectively. The papers that use ML approaches to detect DDoS assaults are compiled in Table 3. While, the related works that based on DL techniques are summarized in Table 4.

Table 3. Summary of ML-based related works

	Technique	Accuracy (%)	Dataset used
Fadlil <i>et al.</i> [30]	NB	-	MITRLADUY
Ye <i>et al.</i> [31]	SVM	95.24	-
Zekri <i>et al.</i> [39]	Decision tree		Own
Lucky <i>et al.</i> [32]	Decision tree	99.93	CIC 2017 and 2019
Putri <i>et al.</i> [33]	K-mean clustering	99.69	ISCX
Chaudhary and Shrimal [34]	Genetic algorithm	85	Own (two)

Table 4. Summary of DL techniques-based related works

	Technique	AC (%)	Accuracy	Data-set used
Tang <i>et al.</i> [48]	RNN	89	IDS in SDN	NSL-KDD
Farahnakian and Heikkonen [49]	DAE	96.53	IDS	KDD-CUP'99
Elsaeidy <i>et al.</i> [50]	DBM	-	Features extraction	Smart water distribution plant
Imamverdiyev and Abdullayeva [51]	DBM	-	DoS detection	NSL-KDD
Liu <i>et al.</i> [52]	CNN	97.7	IDS	KDD 99
Mohammadpour <i>et al.</i> [53]	CNN	99.97	IDS	NSL-KDD

Additionally, DL and ML methodologies diverge significantly. The situations in which ML or DL approaches are most appropriate could be determined with the help of these points. After summarising related works based on both ML and DL method, significant points have been identified. For instance, when the amount of data was larger, DL approaches outperformed ML techniques in terms of accuracy. The key distinctions between DL and ML are outlined in Table 5.

Table 5. ML and DL comparison

ML	DL
A subset of AI is ML	ML includes DL
With little data, ML was able to attain high accuracy and detection rates	With a large amount of data, DL exhibited good accuracy and detection rates
Faster to train a model	highly computational
More human engagement and effort are needed for ML	Human effort and involvement are reduced with DL
Various characteristics and classifiers must be tried in order to get the best results	automatically picks up classifiers and features
The output is typically a numerical number, such as a score	Anything from a score, an element, or free text can be the output

6. CONCLUSION

More than 25% of internet users in 2018 used IPv6 networks, according to the internet society. As a result, IPv6 networks will be completely dependent on the internet, particularly in light of the IoT and its enormous IP requirement. This indicates that future networks' data will be larger than IPv4 networks' data. IPv6 networks are additionally quicker than IPv4 networks. DL approaches are anticipated to yield higher accuracy and detection rates in the new networks as a result of the comparison in this research. In spite of everything, ML techniques have been fully applied to the detection of DDoS attacks, and they have produced the above-mentioned excellent results. DL methods are still thought to be superior methods for handling larger amounts of data. Additionally, assaults have their own ever evolving defences against IDS. Although not on IPv6 networks, DL techniques have been employed for DDoS attack detection. The outcomes of both ML and DL strategies based on DDoS attack detection or IDS are shown in this paper's conclusion. This paper also emphasises the clear distinctions between DL and ML methods. In future work, we extend this work by proposing new model to detect DDoS attacks for IDS.

REFERENCES




- [1] A. Agarwal, R. Singh, and M. Khari, "Detection of DDoS attack using ids mechanism: A review," in *2022 1st International Conference on Informatics (ICI)*, Apr. 2022, pp. 36–46, doi: 10.1109/ICI53355.2022.9786899.
- [2] M. A. Al-Shareeda and S. Manickam, "Man-in-the-middle attacks in mobile ad hoc networks (MANETs): Analysis and evaluation," *Symmetry*, vol. 14, no. 8, p. 1543, Jul. 2022, doi: 10.3390/sym14081543.
- [3] M. A. Al-Shareeda, M. Anbar, I. H. Hasbullah, and S. Manickam, "Survey of authentication and privacy schemes in vehicular ad hoc networks," *IEEE Sensors Journal*, vol. 21, no. 2, pp. 2422–2433, Jan. 2021, doi: 10.1109/JSEN.2020.3021731.
- [4] M. Alaa, A. A. Zaidan, B. B. Zaidan, M. Talal, and M. L. M. Kiah, "A review of smart home applications based on internet of things," *Journal of Network and Computer Applications*, vol. 97, pp. 48–65, Nov. 2017, doi: 10.1016/j.jnca.2017.08.017.
- [5] R. R. Papalkar and A. S. Alvi, "Analysis of defense techniques for DDos attacks in IoT—A review," *ECS Transactions*, vol. 107, no. 1, pp. 3061–3068, Apr. 2022, doi: 10.1149/10701.3061ecst.
- [6] A. S. Albahri *et al.*, "Role of biological data mining and machine learning techniques in detecting and diagnosing the novel coronavirus (COVID-19): A systematic review," *Journal of Medical Systems*, vol. 44, no. 7, pp. 1–11, Jul. 2020, doi: 10.1007/s10916-020-01582-x.
- [7] M. A. Al-Shareeda *et al.*, "CM-CPPA: Chaotic map-based conditional privacy-preserving authentication scheme in 5g-enabled vehicular networks," *Sensors*, vol. 22, no. 13, p. 5026, Jul. 2022, doi: 10.3390/s22135026.
- [8] G. Baldini and I. Amerini, "Online distributed denial of service (DDoS) intrusion detection based on adaptive sliding window and morphological fractal dimension," *Computer Networks*, vol. 210, pp. 1–13, Jun. 2022, doi: 10.1016/j.comnet.2022.108923.
- [9] M. A. Al-Shareeda *et al.*, "Chebyshev polynomial-based scheme for resisting side-channel attacks in 5g-enabled vehicular networks," *Applied Sciences*, vol. 12, no. 12, p. 5939, Jun. 2022, doi: 10.3390/app12125939.
- [10] A. A. Zaidan *et al.*, "A survey on communication components for IoT-based technologies in smart homes," *Telecommunication Systems*, vol. 69, no. 1, pp. 1–25, Sep. 2018, doi: 10.1007/s11235-018-0430-8.
- [11] F. Musumeci, A. C. Fidanci, F. Paolucci, F. Cugini, and M. Tornatore, "Machine-Learning-enabled DDoS attacks detection in P4 programmable networks," *Journal of Network and Systems Management*, vol. 30, no. 1, pp. 1–27, Jan. 2022, doi: 10.1007/s10922-021-09633-5.
- [12] V. Gaur and R. Kumar, "Analysis of machine learning classifiers for early detection of DDoS attacks on IoT devices," *Arabian Journal for Science and Engineering*, vol. 47, no. 2, pp. 1353–1374, Feb. 2022, doi: 10.1007/s13369-021-05947-3.
- [13] J. G. Greener, S. M. Kandathil, L. Moffat, and D. T. Jones, "A guide to machine learning for biologists," *Nature Reviews Molecular Cell Biology*, vol. 23, no. 1, pp. 40–55, Jan. 2022, doi: 10.1038/s41580-021-00407-0.
- [14] M. Talal *et al.*, "Smart home-based IoT for real-time and secure remote health monitoring of triage and priority system using body sensors: Multi-driven systematic review," *Journal of Medical Systems*, vol. 43, no. 3, pp. 1–34, Mar. 2019, doi: 10.1007/s10916-019-1158-z.
- [15] Z. Liu, L. Qian, and S. Tang, "The prediction of DDoS attack by machine learning," in *Third International Conference on Electronics and Communication; Network and Computer Technology (ECNCT 2021)*, Mar. 2022, pp. 681–686, doi: 10.1117/12.2628658.
- [16] M. A. Al-Shareeda, M. Anbar, S. Manickam, and I. H. Hasbullah, "A secure pseudonym-based conditional privacy-preservation authentication scheme in vehicular ad hoc networks," *Sensors*, vol. 22, no. 5, p. 1696, Feb. 2022, doi: 10.3390/s22051696.
- [17] H. Debar, M. Dacier, and A. Wespi, "A revised taxonomy for intrusion-detection systems," *Annales Des Télécommunications*, vol. 55, no. 7, pp. 361–378, Jul. 2000, doi: 10.1007/BF02994844.
- [18] H. Hindy *et al.*, "A taxonomy of network threats and the effect of current datasets on intrusion detection systems," *IEEE Access*, vol. 8, pp. 104650–104675, Jun. 2020, doi: 10.1109/ACCESS.2020.3000179.
- [19] E. Hodo, X. Bellekens, A. Hamilton, C. Tachtatzis, and R. Atkinson, "Shallow and deep networks intrusion detection system: A taxonomy and survey," Jan. 2017.
- [20] S. Axelsson, "Intrusion detection systems: A survey and taxonomy," pp. 1–27, 2000, doi: 10.1.1.1.6603.
- [21] A. Qayyum, M. H. Islam, and M. Jamil, "Taxonomy of statistical based anomaly detection techniques for intrusion detection," in *Proceedings of the IEEE Symposium on Emerging Technologies, 2005.*, 2005, pp. 270–276, doi: 10.1109/ICET.2005.1558893.
- [22] U. Islam *et al.*, "Detection of distributed denial of service (DDoS) attacks in IoT based monitoring system of banking sector using machine learning models," *Sustainability*, vol. 14, no. 14, p. 8374, Jul. 2022, doi: 10.3390/su14148374.
- [23] M. H. Ali *et al.*, "Threat analysis and distributed denial of service (DDoS) attack recognition in the internet of things (IoT)," *Electronics*, vol. 11, no. 3, p. 494, Feb. 2022, doi: 10.3390/electronics11030494.
- [24] A. Aljuhani, "Machine learning approaches for combating distributed denial of service attacks in modern networking environments," *IEEE Access*, vol. 9, pp. 42236–42264, 2021, doi: 10.1109/ACCESS.2021.3062909.
- [25] S. Wani, M. Imthiyas, H. Almohamedh, K. M. Alhamed, S. Almotairi, and Y. Gulzar, "Distributed denial of service (Ddos) mitigation using blockchain—a comprehensive insight," *Symmetry*, vol. 13, no. 2, p. 227, Jan. 2021, doi: 10.3390/sym13020227.
- [26] J. Mirkovic and P. Reiher, "A taxonomy of DDoS attack and DDoS defense mechanisms," *ACM SIGCOMM Computer Communication Review*, vol. 34, no. 2, pp. 39–53, Apr. 2004, doi: 10.1145/997150.997156.
- [27] E. Džaferović, A. Sokol, A. A. Almisreb, and S. M. Norzeli, "DoS and DDoS vulnerability of IoT: A review," *Sustainable Engineering and Innovation*, vol. 1, no. 1, pp. 43–48, Jun. 2019, doi: 10.37868/sei.v1i1.36.
- [28] A. R. Wani, Q. P. Rana, U. Saxena, and N. Pandey, "Analysis and detection of ddos attacks on cloud computing environment using machine learning techniques," in *2019 Amity International Conference on Artificial Intelligence (AICAI)*, Feb. 2019, pp. 870–875, doi: 10.1109/AICAI.2019.8701238.
- [29] E. Alpaydin, *Introduction to machine learning*, 4th ed. Cambridge: MIT Press, 2020.
- [30] A. Fadlil, I. Riadi, and S. Aji, "Review of detection DDOS attack detection using naive bayes classifier for network forensics," *Bulletin of Electrical Engineering and Informatics*, vol. 6, no. 2, pp. 140–148, Jun. 2017, doi: 10.11591/eei.v6i2.605.
- [31] R. Vijayarathay, S. V. Raghavan, and B. Ravindran, "A system approach to network modeling for DDoS detection using a Naive Bayesian classifier," in *2011 Third International Conference on Communication Systems and Networks (COMSNETS 2011)*, Jan. 2011, pp. 1–10, doi: 10.1109/COMSNETS.2011.5716474.
- [32] J. Ye, X. Cheng, J. Zhu, L. Feng, and L. Song, "A DDoS attack detection method based on SVM in software defined network," *Security and Communication Networks*, pp. 1–8, 2018, doi: 10.1155/2018/9804061.
- [33] G. Lucky, F. Jjunju, and A. Marshall, "A lightweight decision-tree algorithm for detecting DDoS flooding attacks," in *2020 IEEE 20th International Conference on Software Quality, Reliability and Security Companion (QRS-C)*, Dec. 2020, pp. 382–389, doi: 10.1109/QRS-C51114.2020.00072.
- [34] N. A. Putri, D. Stiawan, A. Heryanto, T. W. Septian, L. Siregar, and R. Budiarto, "Denial of service attack visualization with clustering using K-means algorithm," in *2017 International Conference on Electrical Engineering and Computer Science*

- (ICECOS), Aug. 2017, pp. 177–183, doi: 10.1109/ICECOS.2017.8167129.
- [35] A. Chaudhary and G. Shrimal, "Intrusion detection system based on genetic algorithm for detection of distribution denial of service attacks in MANETs," in *Proceedings of International Conference on Sustainable Computing in Science, Technology and Management (SUSCOM), Amity University Rajasthan, Jaipur-India*, 2019, pp. 370–377, doi: 10.2139/ssrn.3351807.
- [36] V. N. Vapnik, "An overview of statistical learning theory," *IEEE Transactions on Neural Networks*, vol. 10, no. 5, pp. 988–999, 1999, doi: 10.1109/72.788640.
- [37] T. Subbulakshmi, P. Parameswaran, C. Parthiban, M. Mariselvi, J. A. Anusha, and G. Mahalakshmi, "A unified approach for detection and prevention of ddos attacks using enhanced support vector machines and filtering mechanisms," *ICTACT Journal on Communication Technology*, vol. 4, no. 2, pp. 737–743, Jun. 2013, doi: 10.21917/ijct.2013.0105.
- [38] J. Singh and M. J. Nene, "A survey on machine learning techniques for intrusion detection systems," *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 2, no. 11, pp. 4349–4355, 2013.
- [39] M. Zekri, S. El Kafhali, N. Aboutabit, and Y. Saadi, "DDoS attack detection using machine learning techniques in cloud computing environments," in *2017 3rd International Conference of Cloud Computing Technologies and Applications (CloudTech)*, Oct. 2017, pp. 1–7, doi: 10.1109/CloudTech.2017.8284731.
- [40] A. Nazir, "A comparative study of different artificial neural networks based intrusion detection systems," *International Journal of Scientific and Research Publications*, vol. 3, no. 7, pp. 2250–3153, 2013, doi: 10.1.1.415.1490.
- [41] A. Saied, R. E. Overill, and T. Radzik, "Detection of known and unknown DDoS attacks using Artificial Neural Networks," *Neurocomputing*, vol. 172, pp. 385–393, Jan. 2016, doi: 10.1016/j.neucom.2015.04.101.
- [42] E. Hodo *et al.*, "Threat analysis of IoT networks using artificial neural network intrusion detection system," in *2016 International Symposium on Networks, Computers and Communications (ISNCC)*, May 2016, pp. 1–6, doi: 10.1109/ISNCC.2016.7746067.
- [43] X. Hao, B. Meng, and K. Gu, "Detecting DDoS attack based on PSO clustering algorithm," in *Proceedings of the 2016 3rd International Conference on Materials Engineering, Manufacturing Technology and Control*, 2016, pp. 670–674, doi: 10.2991/icmemtc-16.2016.133.
- [44] N. C. S. N. Iyengar and G. Ganapathy, "Chaotic theory based defensive mechanism against distributed denial of service attack in cloud computing environment," *International Journal of Security and Its Applications*, vol. 9, no. 9, pp. 197–212, Sep. 2015, doi: 10.14257/ijssia.2015.9.9.18.
- [45] C. Balarengadurai and S. Saraswathi, "Fuzzy based detection and prediction of DDoS attacks in IEEE 802.15. 4 low rate wireless personal area network," *International Journal of Computer Science Issues (IJCSI)*, vol. 10, no. 6, pp. 293–301, 2013.
- [46] P. G. Majeed and S. Kumar, "Genetic algorithms in intrusion detection systems: A survey," *International Journal of Innovation and Applied Studies*, vol. 5, no. 3, pp. 233–240, 2014.
- [47] M. Mizukoshi and M. Munetomo, "Distributed denial of services attack protection system with genetic algorithms on Hadoop cluster computing framework," in *2015 IEEE Congress on Evolutionary Computation (CEC)*, May 2015, pp. 1575–1580, doi: 10.1109/CEC.2015.7257075.
- [48] T. A. Tang, L. Mhamdi, D. McLernon, S. A. R. Zaidi, and M. Ghogho, "Deep recurrent neural network for intrusion detection in SDN-based networks," in *2018 4th IEEE Conference on Network Softwarization and Workshops (NetSoft)*, Jun. 2018, pp. 202–206, doi: 10.1109/NETSOFT.2018.8460090.
- [49] F. Farahnakian and J. Heikkonen, "A deep auto-encoder based approach for intrusion detection system," in *2018 20th International Conference on Advanced Communication Technology (ICACT)*, Feb. 2018, pp. 178–183, doi: 10.23919/ICACT.2018.8323687.
- [50] A. Elsaedy, K. S. Munasinghe, D. Sharma, and A. Jamalipour, "Intrusion detection in smart cities using restricted boltzmann machines," *Journal of Network and Computer Applications*, vol. 135, pp. 76–83, Jun. 2019, doi: 10.1016/j.jnca.2019.02.026.
- [51] Y. Imamverdiyev and F. Abdullayeva, "Deep learning method for denial of service attack detection based on restricted boltzmann machine," *Big Data*, vol. 6, no. 2, pp. 159–169, Jun. 2018, doi: 10.1089/big.2018.0023.
- [52] Y. Liu, S. Liu, and X. Zhao, "Intrusion detection algorithm based on convolutional neural network," *DEStech Transactions on Engineering and Technology Research*, vol. 37, no. 12, pp. 1271–1275, Mar. 2018, doi: 10.12783/dtetr/iceta2017/19916.
- [53] L. Mohammadpour, T. C. Ling, C. S. Liew, and C. Y. Chong, "A convolutional neural network for network intrusion detection system," in *Proceedings of the Asia-Pacific Advanced Network*, 2018, pp. 50–55.
- [54] S. S. Husain, E.-J. Ong, D. Minskiy, M. Bober-Irizar, A. Irizar, and M. Bober, "Subcellular protein localisation in the human protein atlas using ensembles of diverse deep architectures," May 2022.
- [55] A. Nguyen *et al.*, "Deep federated learning for autonomous driving," in *2022 IEEE Intelligent Vehicles Symposium (IV)*, Jun. 2022, pp. 1824–1830, doi: 10.1109/IV51971.2022.9827020.
- [56] M. I. Jordan, Z. Ghahramani, T. S. Jaakkola, and L. K. Saul, "An introduction to variational methods for graphical models," *Machine learning*, vol. 37, no. 2, pp. 183–233, 1999, doi: 10.1023/A:1007665907178.
- [57] L. O. Anyanwu, J. Keengwe, and G. A. Arome, "Scalable intrusion detection with recurrent neural networks," in *2010 Seventh International Conference on Information Technology: New Generations*, 2010, vol. 6, no. 1, pp. 919–923, doi: 10.1109/ITNG.2010.45.
- [58] J. Kim, J. Kim, H. Le Thi Thu, and H. Kim, "Long short term memory recurrent neural network classifier for intrusion detection," in *2016 International Conference on Platform Technology and Service (PlatCon)*, Feb. 2016, pp. 1–5, doi: 10.1109/PlatCon.2016.7456805.
- [59] E. Qafzezi, K. Bylykbashi, P. Ampririt, M. Ikeda, K. Matsuo, and L. Barolli, "A survey on advances in vehicular networks: Problems and challenges of architectures, radio technologies, use cases, data dissemination and security," in *International Conference on Advanced Information Networking and Applications*, 2022, pp. 602–613, doi: 10.1007/978-3-030-99619-2_56.
- [60] K. P. Murphy, *Machine learning: A probabilistic perspective*. Cambridge: MIT Press, 2012.
- [61] B. Abolhasanzadeh, "Nonlinear dimensionality reduction for intrusion detection using auto-encoder bottleneck features," in *2015 7th Conference on Information and Knowledge Technology (IKT)*, May 2015, pp. 1–5, doi: 10.1109/IKT.2015.7288799.
- [62] S. Mandapati, S. Kadry, R. L. Kumar, K. Sutham, and O. Thinnukool, "Deep learning model construction for a semi-supervised classification with feature learning," *Complex & Intelligent Systems*, pp. 1–11, Jan. 2022, doi: 10.1007/s40747-022-00641-9.
- [63] P. J. Sajith and G. Nagarajan, "Intrusion detection system using deep belief network & particle swarm optimization," *Wireless Personal Communications*, vol. 125, no. 2, pp. 1385–1403, Jul. 2022, doi: 10.1007/s11277-022-09609-x.
- [64] B. Wang, S. Sun, and S. Zhang, "Research on feature selection method of intrusion detection based on deep belief network," in *Proceedings of the 2015 3rd International Conference on Machinery, Materials and Information Technology Applications*, 2015, pp. 556–561, doi: 10.2991/icmmita-15.2015.107.
- [65] M. Z. Alom, V. Bontupalli, and T. M. Taha, "Intrusion detection using deep belief networks," in *2015 National Aerospace and Electronics Conference (NAECON)*, Jun. 2015, pp. 339–344, doi: 10.1109/NAECON.2015.7443094.




- [66] J. Hasneen and K. M. Sadique, "A survey on 5G architecture and security scopes in SDN and NFV," in *Applied Information Processing Systems*, 2022, pp. 447–460, doi: 10.1007/978-981-16-2008-9_43.
- [67] V. Parganiha, S. P. Shukla, and L. K. Sharma, "Cloud intrusion detection model based on deep belief network and grasshopper optimization," *International Journal of Ambient Computing and Intelligence (IJACI)*, vol. 13, no. 1, pp. 1–24, Jan. 2022, doi: 10.4018/IJACI.293123.
- [68] Y. LeCun, "Learning invariant feature hierarchies," in *European conference on computer vision*, 2012, pp. 496–505, doi: 10.1007/978-3-642-33863-2_51.

BIOGRAPHIES OF AUTHORS






Mahmood A. Al-Shareeda    obtained his Ph.D. in Advanced Computer Network from University Sains Malaysia (USM). He is currently a Postdoctoral Fellow at National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia. His current research interests include network monitoring, internet of things (IoT), vehicular ad hoc network (VANET) security and IPv6 security. He can be contacted at email: alshareeda022@gmail.com



Selvakumar Manickam    is currently working as an Associate Professor at National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia. His research interests include Cybersecurity, Internet of Things, Industry 4.0, and Machine Learning. He has authored and co-authored more than 160 articles in journals, conference proceedings, and book reviews and graduated 13 PhDs. He has 10 years of industrial experience prior to joining academia. He is a member of technical forums at national and international levels. He also has experience building IoT, embedded, server, mobile, and web-based applications. He can be contacted at email: selva@usm.my.



Murtaja Ali Saare    Murtaja Ali Saare is an Assistant Professor at the Department of Computer Technology Engineering, Shatt Al-Arab University College, Iraq. He received his master's degree in Information Technology at Universiti Utara Malaysia (UUM), in 2017. He completed his Ph. D at School of Computing, Sintok, UUM, Kedah, Malaysia, in 2021. His research interest includes aging and cognition, e-health, and human-centered computing. He has published his research work in reputable Scopus indexed journal. He can be contacted at email: mmurtaja88@gmail.com and murtaja.a.sari@sa-uc.edu.iq.