International Journal of Electrical and Computer Engineering (IJECE)
Vol. 13, No. 5, October 2023, pp. 5617~5631
ISSN: 2088-8708, DOI: 10.11591/ijece.v13i5.pp5617-5631

Machine and deep learning techniques for detecting internet protocol version six attacks: a review

Arkan Hammoodi Hasan Kabla[1], Mohammed Anbar[1], Shady Hamouda[2], Abdullah Ahmed Bahashwan[1], Taief Alaa Al-Amiedy[1], Iznan Husainy Hasbullah[1], Serri Faisal[2]
[1]National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia, Penang, Malaysia
[2]Department of Business Information Technology, Liwa College of Technology, Abu Dhabi, United Arab Emirates

Article Info

Article history:

Received Jul 31, 2022
Revised Jan 27, 2023
Accepted Feb 10, 2023

Keywords:

DDoS attacks
Deep learning
Intrusion detection system
IPv4
IPv6
Machine learning

ABSTRACT

The rapid development of information and communication technologies has increased the demand for internet-facing devices that require publicly accessible internet protocol (IP) addresses, resulting in the depletion of internet protocol version 4 (IPv4) address space. As a result, internet protocol version 6 (IPv6) was designed to address this issue. However, IPv6 is still not widely used because of security concerns. An intrusion detection system (IDS) is one example of a security mechanism used to secure networks. Lately, the use of machine learning (ML) or deep learning (DL) detection models in IDSs is gaining popularity due to their ability to detect threats on IPv6 networks accurately. However, there is an apparent lack of studies that review ML and DL in IDS. Even the existing reviews of ML and DL fail to compare those techniques. Thus, this paper comprehensively elucidates ML and DL techniques and IPv6-based distributed denial of service (DDoS) attacks. Additionally, this paper includes a qualitative comparison with other related works. Moreover, this work also thoroughly reviews the existing ML and DL-based IDSs for detecting IPv6 and IPv4 attacks. Lastly, researchers could use this review as a guide in the future to improve their work on DL and ML-based IDS.

Corresponding Author:

Mohammed Anbar
National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia
11800 USM, Penang, Malaysia
Email: anbar@usm.my

1. INTRODUCTION

The exponential growth of internet users and applications increases the demands for internet-facing devices that require unique publicly accessible IP addresses, resulting in the internet protocol version 4 (IPv4) addresses pool being depleted. The main reason for this exponential growth is the proliferation of numerous information and communication technologies (ICTs), such as cloud computing, the internet of things (IoT), and wireless technology applications. As a result, internet protocol version 6 (IPv6) was engineered and positioned as the next-generation IP to replace IPv4 in the future and solve the IPv4 address exhaustion issue. According to Google IPv6 adoption data from January 17, 2022, 34.31% of Google users use the IPv6 protocol [1].

One of the most critical protocols in IPv6 is the internet control message protocol version six (ICMPv6). IPv6 cannot function without the service of ICMPv6, whose messages serve various critical purposes. However, the ICMPv6 lacks a built-in authentication scheme, exposing its messages to exploitation by attackers. Furthermore, IPv6 nodes do not validate ICMPv6 messages because they are assumed to be

inherently secure. As a result, all IPv6 nodes in any link-local network are vulnerable to ICMPv6-based distributed denial of service (DDoS) attacks and exposed to spoofed ICMPv6 packets [2].

Even though IPv6 has more security protections than IPv4, it still has several exploitable weaknesses and vulnerabilities that allow attackers to gain unauthorized access or flood the network with massive traffic to deny users access to the required services. In addition, many unique IPv6 characteristics, such as IPv6 multicast addresses, are exploited in many attacks. As a result, IPv6 security needs work as it remains vulnerable to various threats, especially denial-of-service (DoS) and DDoS attacks, which are among the most damaging. Intrusion detection systems (IDSs) are an efficient security tool for detecting attacks on computer networks. However, IPv4-based IDSs cannot detect IPv6 attacks due to differences in the protocol's packet pattern and structure [3]. One solution is adapting machine learning (ML) or deep learning (DL) detection models in IDS, allowing them to detect sophisticated IPv6 attacks in IPv6 networks accurately. In addition, ML and DL techniques have shown impressive results in solving many problems in other fields. As a result, they are becoming more popular among security researchers as a detection model to detect different IPv6 attacks.

This paper has two-fold theoretical contributions: i) a comprehensive review of the IPv4 and IPv6 IDSs based on ML and DL algorithms, and ii) a qualitative comparison between this review study and existing studies in terms of several author-defined metrics. The researchers working in the field related to DL and ML-based IDS may refer to this review in the future as a guideline. This paper's organization is as follows: section 2 presents a qualitative comparison with the existing studies, followed by an overview of the IPv6 protocol in section 3. Section 4 provides an overview of DoS and DDoS attacks. The overview of IDSs and the review of the existing ML and DL-based IDS are discussed in section 5, followed by an in-depth discussion of the current ML and DL-based IDS in section 6. Section 7 highlights the decisive differences between DL and ML. Finally, section 8 concludes this research paper and suggests future research directions.

2. QUALITATIVE COMPARISON WITH EXISTING REVIEWS

The importance of improving cyber security mechanisms to detect or prevent cyber threats cannot be overstated. An example of a defense system that detects network intrusion is IDS. IDS is deployable with other security measures, such as authentication mechanisms or access control. Meanwhile, a large number of ML and DL techniques have been adopted by IDSs, especially after ML techniques proved their efficiency many years ago [4]. The application of neural networks has touched many aspects of our technological lives for decades, such as facial, image, and voice recognition applications. Therefore, researchers are already aware of how DL positively affects us, including its impact on cyber security. Unfortunately, most current works utilize ML or DL for feature selection or classification, but little research has combined ML and DL techniques. This section provides a qualitative comparison between this review study and existing review works on IDS for detecting IPv6 DDoS attacks using ML and DL techniques.

A review by Kaur and Kakkar [5] investigated the use of ML techniques to detect DDoS attacks but ignored DL techniques despite their use for DDoS attack detection. Meanwhile, Alamiedy *et al*. [6] reviewed anomaly-based IDSs, focusing on the performance of the ML classifiers used by the IDS but also ignoring DL-based ones. In addition, Aleesa *et al*. [7] systematically reviewed and analyzed most DL-based IDSs but ignored the ML techniques. Moreover, Ferrag *et al*. [8] presented a survey of DL techniques utilized for cyber security IDS and discussed some ML techniques.

Elejla *et al*. [9] presented an in-depth review that covered most of the ML techniques adopted for ICMPv6-based DDoS detection, even though it does not cover DL. Aldweesh *et al*. [10] discussed and compared DL-based IDSs in a systematic review and highlighted the efficiency of all the reviewed works in terms of their accuracy (AC) but did not include ML-based IDS. Bahashwan *et al*. [11] reviewed IPv6 IDSs for DoS and DDoS attacks detection covering ML and DL techniques, though only superficially since its focus is on the new internet protocol, IPv6, and possible attacks. Hodo *et al*. [12] reviewed ML and DL-based IDS, but not comparatively. A comparative follow-up study highlighting the similarities and differences of different types of IDS could help other researchers decide the most suitable techniques for their needs. Finally, Sharma *et al*. [13] reviewed some IDSs from earlier studies that utilized ML techniques. Table 1 summarizes the existing studies and shows how our work differs.

Table 1 shows that only Bahashwan *et al*. [11] reviewed some ML and DL techniques in IDSs. Therefore, it is clear that there is an apparent lack of study that reviews both ML and DL's adoption in IDS. Moreover, even those covering ML and DL fail to compare the two techniques. However, our work differs from the existing works since it provides i) a thorough review of the ML and DL techniques used in signature-based IDS (SIDS) and anomaly-based IDS (AIDS), ii) an in-depth discussion and insight into existing ML and DL techniques used in SIDS and AIDS, iii) association between the ML and DL techniques with existing related works, and iv) the crucial differences between ML and DL techniques.

Table 1. Qualitative comparison with existing reviews

Author	IPv6 review	IDS classification	Security domain		Techniques		A comparison to previous reviews
			SIDS	AIDS	ML	DL	
Drewek-Ossowicka *et al*. [4]	-	✓	✓	-	✓	-	✓
Aldweesh *et al*. [10]	-	✓	-	✓	-	✓	✓
Aleesa *et al*. [7]	-	✓	✓	-	-	✓	-
Bahashwan *et al*. [11]	✓	✓	✓	-	✓	✓	-
Ferrag *et al*. [8]	-	✓	-	✓	✓	✓	✓
Alamiedy *et al*. [6]	-	✓	-	✓	✓	-	-
Elejla *et al*. [9]	✓	✓	-	✓	✓	-	✓
Hodo *et al*. [12]	-	✓	✓	-	✓	-	-
Sharma *et al*. [13]	-	-	✓	-	✓	-	-
Kaur and Kakkar [5]	-	-	✓	-	✓	-	-
This Review	✓	✓	✓	✓	✓	✓	✓

3. OVERVIEW OF IPv6

IPv6 is a network layer protocol that follows the OSI model standard. However, the IPv6 design differs from the IPv4 in terms of address size (32-bit vs. 128-bit), packet header format, address format, and other features, such as mobility, handling the quality of service whenever required, and end-to-end connectivity, which outperforms the IPv4. Besides, some levels of enhanced security in IPv6 are built into the IPv6 stack, such as the internet protocol security (IPSec) protocol support, unlike IPv4. Unfortunately, IPv6 is still vulnerable to attacks even with the new features.

Nevertheless, due to the much larger address space, probing all IPv6 addresses in the network is impractical for attackers compared to IPv4. However, attackers can leverage some specific IPv6 features for exploitation. For example, sending a spoofed packet to the all-router multicast group (FF02::2) allows attackers to discover routers in the network since all routers will respond with a reply, which exposes their presence [11].

IPv6 introduces two new essential protocols, ICMPv6 and neighbor discovery protocol (NDP). ICMPv6 messages consist of error messages and information messages. ICMPv6 error messages' codes range from 1 to 127, and ICMPv6 information messages' codes range from 128 to 255. The NDP, a subset of ICMPv6, depends on five ICMPv6 information messages for its operation. ICMPv6 is a mandatory part of the IPv6 protocol responsible for many crucial functions, including enabling IPv6 nodes in an IPv6 network to discover their neighbors via the duplicate address detection (DAD) process. DAD is vital to the Stateless address auto-configuration (SLAAC) function, allowing IPv6 nodes to assign unique IPv6 addresses to their network interfaces. Additionally, it supports other crucial features, such as address resolution and identifying the path maximum transmission unit (PMTU). Regrettably, these core features prioritize functionality over security, resulting in adversaries being able to easily perform DoS and DDoS attacks by exploiting the ICMPv6 messages [14].

4. OVERVIEW OF DoS AND DDoS

DoS and DDoS flooding attacks are the most common attacks on IPv6 and IPv4 networks, which could have a destructive impact on the networks. Attackers typically gain control of some infected nodes (called bots) within the local network first before executing DoS or DDoS attacks. Attackers inject a large amount of malicious traffic into the network or send them toward the targeted victim until all available network bandwidth or the victim's computational resources are consumed. In addition, attackers may also inundate the network with spoofed packets from multiple infected nodes to flood the victims' network and servers. The significant difference between a DoS and a DDoS is that the former is triggered from a single source, while the latter involves multiple sources. Figure 1 (see in appendix) illustrates the difference between DDoS and DoS attacks.

5. INTRUSION DETECTION SYSTEMS

Anomaly-based techniques are the most efficient for building sophisticated IDS models by automating the process and creating a practical detection system while reducing human intervention and efforts [15], [16]. In addition, those AIDSs build a robust model by monitoring traffic behaviors based on packet features. In anomaly-based techniques, the classification is based on heuristics or rules rather than patterns or signatures and attempts to detect any abnormality that falls out of regular system operation [17]. The IDS must be strategically placed in the network to detect attacks by collecting and monitoring network traffic. After collecting network data and monitoring the traffic, the IDS will analyze the packets to detect possible threats. Researchers have formulated two different classifications of the IDS model: SIDS and AIDS [18]. SIDS depends on a pre-defined signatures database [19], making it unable to identify attacks

without matching signatures [6]. Therefore, detecting zero-day attacks is impossible for SIDS without the pre-defined signatures in its database [20]. On the other hand, unlike the signature-based model, AIDS does not rely on a pre-defined signatures database but detects the anomalies in the network traffic behaviors [21].

AIDS detects unknown attacks from the anomaly in the network traffic behavior [9]. AIDS could either be programmed or self-learning. Developing a self-learning AIDS involves creating a model for the basic processes using the assigned network traffic aggregated over a specified duration [22]. At the same time, the programmed IDS model works in a system that requires an admin or third party to train the model to detect behavioral changes. In other words, the user is the one that defines the acceptable level for the system's abnormal behavior [23]. Table 2 shows the differences between SIDS and AIDS. There are many techniques employed in AIDS, but ML and DL techniques are among the most efficient and widely used to detect attacks in IPv4 and IPv6 networks. Therefore, this work focuses on the review of AIDS based on ML and DL techniques.

Table 2. Advantages and disadvantages of SIDS vs. AIDS

SIDS	AIDS
Advantages	
It efficiently detects known attacks.	It efficiently detects zero-day attacks.
It is easy to implement, deploy, and update.	Allow for the detection of privilege abuse.
For known attacks, the false positive rate (FPR) is low.	Operating system (OS) agnostic.
	High detection AC and low false alarm rate (FAR).
Disadvantages	
Unable to detect new attacks "zero-day."	It is challenging to stay alert at the right time.
It is challenging to keep attack patterns up to date.	There is unavailability when behavior profiles are being rebuilt (retrained).
Keeping track of attack patterns takes much time.	

5.1. ML-based IDS

Most researchers utilize ML for two primary purposes. First, feature selection reduces the chosen dataset's dimensionality. Second, classifying data as normal or abnormal [16]. ML techniques can detect abnormal attributes within a specified time interval and efficiently distinguish normal and abnormal traffic without human intervention [24], [25]. The following subsections discuss the most common ML techniques adopted in IDS, including some state-of-the-art IDSs that adopted these ML techniques. Figure 2 illustrates the ML-based IDSs techniques used in the reviewed studies.

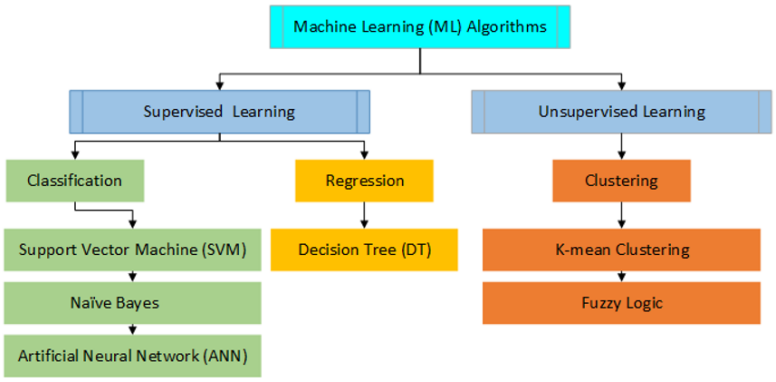

Figure 2. Taxonomy of machine learning techniques

5.1.1. Naïve Bayes

Naïve Bayes (NB) is the most straightforward technique for building classifiers based on Bayesian networks to execute the classification process. First, the classifiers specify class labels into problem cases; then represent feature values' vectors. Finally, the class labels will be drawn depending on specific sets [12]. The following are some approaches that employ NB techniques in their systems.

Fadlil *et al.* [26] proposed a DDoS attack detection approach by statistically analyzing network traffic using NB, achieving significant results in detecting DDoS attacks before it happens. Their approach works by finding network packets' average and standard deviation. Another group of researchers led by Vijayasarathy *et al.* [27] also used the NB classifier for DDoS attack detection. They had done network

modeling for transmission control protocol (TCP) and user datagram protocol (UDP) protocols, achieving a very high detection AC for TCP and UDP-based attacks of 98.6% and 99.5%, respectively.

Salih *et al*. [28] proposed an NB-based approach to detect IPv6 covert channels used by adversaries to circumvent detection by firewalls or IDS. Adversaries create covert channels by sending malicious data to the target using unused flags or bits. The proposed approach used ten extracted features from the traffic in the classification stage: flow label, traffic class, hop limit, source addresses, payload length, ICMPv6 code, ICMPv6 type, ICMPv6 payload, next header, and reserve bit. The authors evaluated their proposed approach using a self-generated dataset and several attacking tools, achieving 94.55% detection accuracy. The high AC is due to the features used related to the targeted attacks. However, this research only detects IPv6 covert channels and does not include DoS and DDoS attacks.

5.1.2. Support vector machine (SVM)

Sain [29] developed the SVM algorithm at AT&T Bell Laboratories in the early 90s. Since then, it has been widely used in network security to detect DDoS attacks with satisfactory results. Consequently, it attracted the attention of many researchers, especially those working with ML-based IDS, for its classification and regression performance [30]. First, the SVM method constructs a set of training examples; then classifies everything into two categories. Finally, it generates a prediction model to classify new samples into one of the two categories.

Many mechanisms utilize the SVM technique in their systems. Subbulakshmi *et al*. [31] created a dataset comprising DDoS attack traffic. Then, the authors worked on detecting the attacks using enhanced SVM (ESVM), followed by detecting the attacks into different classes using the enhanced multi-class SVM (EMCSVM). Then, SVM evaluates the activity of EMCSVM. Meanwhile, [32] used the SVM classification algorithms to build a DDoS attack detection model, achieving an average AC rate of 95.24% by utilizing only a small amount of collected flows.

Zulkiflee *et al*. [33] utilized SVM to detect several IPv6 attacks by identifying a set of features most relevant to the attacks they wish to detect, such as the flood router attack. Flood router attack is a type of DoS flooding attack that exploits ICMPv6 RA messages. They detect this attack using a set of five features: Src IP, Src Port, Dst Port, time interval, and protocol. Then, using these features, the SVM algorithm was applied to a real-world traffic dataset to detect the attacks, achieving an average detection AC rate of 99.95%, indicating that SVM is a good classifier and the strength of the chosen features. Meanwhile, Anbar *et al*. [3] performed feature selection using principal component analysis (PCA) and Information gain ratio (IGR) in their proposed technique. Then, they used an SVM-based predictor model to detect RA flooding attacks, achieving a 98.55% detection AC and only 3.3% FPR using a realistic dataset, indicating their proposed technique's effectiveness in RA flooding attack detection.

5.1.3. Decision tree (DT)

The DT algorithm is a simple technique but one of the most commonly used ML and data mining techniques. Its ability to perform decision analysis [12] makes it suitable as a protective mechanism to observe a category and conclude the category-targeted value. Also, it can represent decisions and make a decision explicitly. This algorithm relies on a learned dataset whenever new data needs to be classified. In other words, it classifies data according to the previously learned dataset [34]. Several mechanisms make use of the DT technique in their systems. For example, Zekri *et al*. [35] designed a DT-based model for detecting DDoS flooding attacks automatically and effectively using their attack signatures. They used this and the C4.5 algorithms to reduce DDoS attacks, achieving an ideal classification with 98.8% accuracy. Also, another mechanism by Pydipalli *et al*. [36] can learn DDoS attack patterns using both signature-based and anomaly-based detection approaches to reap the benefit of both. After the pre-processing step, they performed the training set classification using the C4.5 DT algorithm, achieving a high AC rate of 99.93% in detecting DDoS attacks.

5.1.4. Artificial neural network (ANN)

In 1943, McCulloc and Pitts introduced a set of simple neurons in an ANN to perform computational tasks. The neurons behave like biological networks by replicating the biological neurons' functionality [37]. Afterward, researchers develop neural networks for decision-making applications, such as real-time cyber-attack detection. For example, Saad *et al*. [38] employed the back-propagation neural network (BPNN) algorithm, an ML technique, for DDoS attack detection in IPv6 networks. They first ranked and selected a set of features using IGR and PCA before applying BPNN. After using 80% of the dataset for BPNN training, they used the remaining dataset for testing, achieving 98.3% detection AC. In addition, seven researchers led by Hodo *et al*. [39] used ANN to design a paradigm to analyze threats in IoT network traffic, focusing on classifications of legitimate threat patterns on IoT networks and achieving a very high detection AC of 99.4%.

5.1.5. K-mean clustering

K-mean clustering is a technique to group a dataset into K groups. This algorithm determines K initial cluster centers in a dataset and then refines them by each case joining its closest cluster center. After that, each cluster center updates its cases' average [12]. Several approaches employ the K-mean clustering technique in their systems. For example, Hao *et al*. [40] created a detection model to detect DDoS attacks of undetermined sessions, achieving efficient detection rates (DRs) of DDoS attacks with a reasonable AC rate of 86%. Additionally, Putri *et al*. [41] used the clustering algorithm of K-means in their proposed approach to detect DDoS attacks, achieving a high AC rate of 97.83% and a DR of 98.63%. Promisingly, on WEKA tools, the obtained results are higher for both AC rate (99.69%) and DR (99.01%).

5.1.6. Fuzzy logic (FL)

The FL technique is derived from fuzzy set theory, which deals with approximation rather than precision based on the traditional predicate logic [12]. One of the attractive features of this technique is the handling of real-life uncertainty, making anomaly detection more efficient. Several works use FL algorithms in their systems. For example, Iyengar *et al*. [42] designed a fuzzy logic model based on pre-defined rules that recognize malicious DDoS packets from regular traffic and then perform suitable procedures to mitigate them. In addition, Balarengadurai and Saraswathi [43] used the FL algorithm to create a mechanism to detect and predict DDoS attacks in IEEE 802.15.4 environment. Their fuzzy-based detection and prediction system (FBDPS) mitigates DDoS attacks by checking each sensor node's energy consumption. FBDPS classifies a node as malicious if it consumes an abnormal amount of energy. Moreover, FBDPS can differentiate DDoS attack types based on the malicious node's energy consumption rate.

Yao *et al*. [44] proposed an anomaly-based detection algorithm using the fuzzy technique to detect NDP-based attacks. The evaluation results using real-world network data from the CERNET2 backbone revealed that the approach could detect attacks with high detection AC and low false rates. However, the dataset's malicious and normal traffic data were from two different sources that might produce a biased result. Meanwhile, Saad *et al*. [45] developed an approach based on fuzzy techniques for detecting ICMPv6 echo flooding attacks with high AC and low root means square error (0.26). They evaluated their proposed approach using a real-world dataset comprising 2,000 normal and abnormal network traffic records. However, the work lacks important data, such as information on the testbed, attacking tools, false alarm rate, and detection AC.

5.1.7. Genetic algorithms (GA)

Genetic algorithm is based on evolutionary principles and is one of the most used ML techniques, utilizing biological evaluation to solve different optimization problems [46]. A normal behavior profile is created as a baseline to learn from and compare with unknown patterns to make decisions using a genetic strategy. Many IDS use this algorithm to develop the rules to detect attack patterns.

Many researchers utilize GA in their systems, like Chaudhary and Shrimal [47], who used GA in their proposed model to detect DDoS attacks in mobile ad-hoc networks (MANETs), achieving an 85% DR, an acceptable result for detecting DDoS attacks. Meanwhile, Mizukoshi and Munetomo [48] utilized GA to design a scalable real-time traffic analysis model to detect dan prevent DDoS attacks on a distributed Hadoop infrastructure, achieving outstanding results on the WITZ (96%) and DARPA (98%) datasets. However, the authors only measured the accuracy, not other evaluation metrics like recall, precision, and the F1-Score. Table 3 summarizes the related works on ML-based IDS.

5.2. DL-based IDS

This section describes DL-based IDS. DL is an advanced branch of ML in the learning process since it mimics multiple layers of neurons [49]. Figure 3 illustrates the two main classes of DL-based techniques. As shown in Figure 3, there are two types of DL techniques. First, the generative architecture (or unsupervised) represents the given systems in a graphical representation. These visual models depict dependence for distribution. These graphs consist of nodes and arcs. The nodes represent random variables, while arcs represent the relationship between nodes with millions of parameters [50]. Then, the common statistical distribution represents the products of the nodes and their related variables [51]. Also, hidden variables cannot be observed in the graphical models. The training of generative models does not depend on the labels of data. Instead, these models go through a pre-training stage (unsupervised learning) for classification purposes. The lower layers have been trained separately from the other layers through a pre-training stage, allowing the different layers to be trained layer by layer from bottom to up. After that, all the other layers will be trained after pre-training. The generative architecture has four sub-classes: Recurrent neural network (RNN), deep Boltzmann machine (DBM), deep auto-encoder (DAE), and deep belief networks (DBN). The second type of DL is discriminative architecture (DA). This architecture classification depends on the discriminative power by characterizing the posterior distributions of conditioned classes from

the input data [12]. The discriminative architecture has two sub-classes: RNN and convolutional neural network (CNN). The following subsections provide more details for these sub-classes with related works.

Table 3. Summary of literature on ML-based IDS

Article	Technique	Dataset used	Protocol (IPv4/IPv6)	Detection accuracy	Other performance metrics	Limitations
Fadlil *et al*. [26]	NB	Own collected dataset	IPv4	-	-	The authors did not report any results.
Vijayasarathy *et al*. [27]	NB	DARPA, SETS	IPv4	98.6%	FAR, Miss Rate	Test limitations negated the authors' claim that the system could work at line speeds. Meanwhile, the evaluation only used a limited number of dataset samples.
Salih *et al*. [28]	NB	Own collected dataset	IPv6	94.55%	false negative rate (FNR), true positive rate (TPR)	This research lacks other types of IPv6 attacks, such as DoS and DDoS.
	SVM	Own collected dataset	IPv4	45%, 64%, 86%	AC	The achieved accuracy rates are not the highest.
Subbulakshmi *et al*. [31]	SVM	Own collected dataset	IPv4	96.83%, 95.24%, 93.65%	FAR	The authors only collected a small amount of flow to evaluate their approach. The authors limited their work by not comprehensively simulating the normal data flow.
Ye *et al*. [32]	SVM	Own collected dataset	IPv6	99.95%	Detection AC, FAR	Limited to RA flooding DoS attack detection.
Zulkiflee *et al*. [33]	SVM	Own collected dataset	IPv6	98.55%	FAR, detection AC	Limited to RA flooding DoS attack detection.
Anbar *et al*. [3]	DT/C4.5	Own collected dataset	IPv4	98.8%	True positive (TP), false positive (FP), true negative (TN), false negative (FN), F-measure	The dataset used was not presented clearly.
Zekri *et al*. [35]	DT/C4.5	CICIDS2017	IPv4	99.93%	`ime taken to build a model, Kappa Statistic, mean absolute error (MAE), root nean squared error (RMSE)	The authors used a random and small subset of data from the CICIDS2017 dataset, i.e., not using all the available data. The use of the small evaluation dataset made the approach's performance unrealistic.
Pydipalli *et al* [36]	BPNN	Own collected dataset	IPv6	98.3%	AC	Limited to ICMPv6 echo request DDoS Flooding attack.
Saad *et al*. [38]	ANN	Own collected IoT dataset	IPv4	99.4%	AC	The proposed approach was trained with a small set of only 2,313 samples.
Hodo *et al*. [39]	K-mean Clustering	Vast Challenge 2013: Mini-Challenge 3	IPv4	86%	AC	The detection accuracy is low compared to other approaches.
Hao *et al*. [40]	K-mean Clustering	ISCX	IPv4	99.69%	TP, FP, TN, False Alarm.	The used dataset has an imbalanced class problem.
Putri *et al*. [41]	FL	-	IPv4	86.9%	Sensitivity, specificity, precision, FPR, FNR	There is no information about the used dataset. In addition, the achieved accuracy rate is low compared to other approaches.
Balarengadurai and Saraswathi [43]	FL	Own generated dataset by NS2	IPv4	99.75%	TPR, FPR.	The simulation dataset was collected in a very short time. Although this approach was proposed to deal with big data from the cloud traffic, there is no feature engineering.
Yao *et al*. [44]	FL	CERNET2	IPv6	-	-	The authors did not disclose essential facts about the studies and outcomes. Also, the malicious and normal traffic of the used dataset was generated from two different sources, which could result in a biased outcome.
Saad *et al*. [45]	FL	Own generated dataset	IPv6	-	-	The authors did not disclose details on the experiments and results, such as attacking tools, testbed used, false alarms, and detection accuracy.
Chaudhary and Shrimal [47]	GA	Own collected dataset by Qualnet	IPv4	85%	FPR	Compared to others, many approaches could achieve a higher detection rate. Additionally, this approach can detect only one attack in MANETs.
Mizukoshi and Munetomo [48]	GA	DARPA, WITZ	IPv4	98%	FPR, FNR	The authors did not include reliable metrics like recall, precision, and F1-Score.

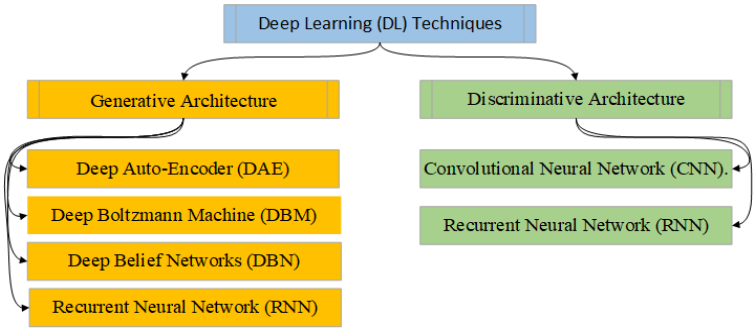

Figure 3. Taxonomy of deep learning techniques

5.2.1. Recurrent neural network

The RNN model is an architecture type with a feedback loop that links layer by layer and stores the last input's data to increase the reliability of the model [18]. This sub-class of deep generative networks can either be unsupervised or supervised. RNN has two types of architecture: i) Jordan RNN, like a feedback loop, connecting all neurons within one layer to the next, and ii) Elman RNN, which only has superficial feedback looping layer by layer. Due to its ability to store information [52], RNN can train with fewer input vectors but can still accurately classify normal and abnormal patterns. RNN can be trained as a discriminative model by pre-segmenting the training data and post-processing the output to transform it into labeled data. RNN uses its discriminative power for classification when the output is explicitly labeled with data in sequence with the input data sequence.

Several researchers use the RNN approach in their systems. For example, Kim *et al*. [53] utilized RNN with a long-short-term memory (RNN-LSTM) architecture to train IDS using KDD Cup '99, achieving higher accuracy and DRs than other IDS classifiers, i.e., 93% AC and 98.88% DR. Meanwhile, Tang *et al*. [52] utilized RNN for IDS in software define networking (SDN)-based networks, achieving an 89% detection accuracy using their proposed gated recurrent unit-RNN (GRU-RNN) when tested on the NSL-KDD dataset. Elejla *et al*. [54] proposed an approach to detect ICMPv6 DDoS flooding attacks using RNN, gated recurrent unit (GRU), and LSTM. They used an ensemble feature technique to select the significant features to detect ICMPv6 DDoS flooding attacks. In addition, the selected features were used as the input to train the DL training model (e.g., RNN, GRU, and LSTM). The authors used a synthetic dataset to evaluate their proposed technique and showed that LSTM outperformed the other two DL models in AC, recall, precision, and FPR.

5.2.2. Deep auto-encoder

The DAE is a generative model with several forms, including denoising and stacked auto-encoders [55]. It is also known as a "deep auto-encoder" because its model has multiple hidden layers. Generally, it has an input layer representing the sample data and two or more hidden layers to transform the features and map them into the output layer where the features would be reconstructed. Auto-encoder training results in a "bottleneck" structure because the hidden layer is more restricted than the input layer [56]. The following methods employ the DAE technique in their systems. Abolhasanzadeh *et al*. [57] proposed an approach based on a DAE to detect IPv4-based attacks by applying bottleneck features to reduce the big data dimensionality, increasing the efficiency of intrusion detection. The authors used the NSL-KDD dataset for evaluation, achieving good AC for real-world intrusion detection. In addition, Farahnakian and Heikkonen [58] proposed a DAE-based IDS and tested it using the KDD Cup '99 dataset, achieving significantly improved AC (96.53%) and DR (95.65%). Ujjan *et al*. [59] proposed sFlow and adaptive polling-based sampling with Snort IDS and a DL-based model to detect various DDoS attacks inside IoT networks with a very high detection AC of 95%. Meanwhile, Asad *et al*. [60] proposed a detection mechanism based on DNN that employs feed-forward back-propagation for accurate DDoS attack detection, achieving a very high detection AC of 98%.

5.2.3. Deep Boltzmann machine

The DBM is one of the generative architectures derived from the general (BM) machine. It is regarded as a good classifier when a substantial amount of unlabeled data is involved in training, followed by fine-tuning with labeled data. Although the DBM's units on the same layer are unconnected, there is a connection between the input and the hidden units, making DBM a unidirectional graphical model. Classic BM has a network of units based on arbitrary decisions to identify whether the states are off or on [55].

However, BM is time-consuming to train as it is a slow-processing algorithm. Reducing the DBM's hidden layers to a single layer result in a restricted Boltzmann machine (RBM). Many researchers use DBM in their systems. For example, Elsaeidy *et al*. [30] utilized deep RBM to extract effective and significant high-level features for detecting different DDoS attacks. Also, Imamverdiyev *et al*. [61] utilized the deep RBM model in their proposed DoS detection method tested on the NSL-KDD dataset.

5.2.4. Deep belief networks

DBN are created by stacking DBM with one or more hidden layers. The ability to learn training data's joint probability distribution without using labeled data puts the DBN in the generative probabilistic model category [12]. DBN can construct the models using either unsupervised pre-training or supervised fine-tuning techniques. The training aims to learn the weights between layers. Several works employed the DBN technique in the systems. For example, Xin and Wang [62] utilized the DBN algorithm to select the features layer by layer to reduce the dimensionality of features. Although the DBN is an unsupervised learning algorithm, it is more suited for use with a large amount of unlabeled data, making it a practical algorithm for network intrusion detection, as shown by the experimental results. Additionally, Alom *et al*. [63] utilized the DBN in their intrusion detection, achieving 97.5% AC in detecting and classifying attacks using the NSL-KDD dataset.

5.2.5. Convolutional neural network

CNN is a deep learning neural network for processing structured arrays of data such as images and is widely used in computer vision. Many applications based on natural language processing successfully use CNN [64]. Training the CNN is more straightforward than other connected networks since it has fewer parameters with a similar quantity of hidden units [63]. More clearly, CNN is biologically inspired and has a multi-layer perceptron. CNN architecture comprises the convolutional layer, the max-pooling (gathering) layer, and the fully connected layer. The max-pooling layer should follow each convolutional layer. Moreover, the last stage comprises many stacked max-pooling and convolutional layers in a neural network to create a fully-connected layer in a non-linear fashion [65].

Many researchers employ CNN in their systems. For example, Fan and Ling-zhi [66] used KDD Cup 99 to test their proposed CNN-based model, achieving a high DR of 97.7%. Meanwhile, Teyou and Ziazet [67] proposed an effective and flexible network-IDS (NIDS) that adopted CNN and tested with the NSL-KDD dataset, achieving a high detection rate of 99.97%. Also, Haider *et al*. [68] proposed a DL-based CNN ensemble solution to detect DDoS attacks in an SDN environment, achieving a high attack detection AC of 99.48%. Moreover, Liu *et al*. [69] implemented DL models in their proposed end-to-end attack detection approach that analyzes the payloads. Their proposed CNN-based payload classification approach (PL-CNN) and RNN-based payload classification approach (PL-RNN) for attack detection achieved 99.36% and 99.98% detection AC, respectively, when tested on the DARPA1998 dataset. This paper comprehensively covers the two main architectures of DL, generative architectures and discriminative architectures. Lately, many researchers have shown interest in utilizing DL techniques in IDS. Table 4 (see in appendix) summarizes the related work on DDoS IDS utilizing DL techniques.

6. DISCUSSION

The different protocol structure of IPv4 and IPv6 makes it almost impossible to create a generalized AIDS that concurrently detects both IPv4 and IPv6-based attacks. However, as shown in Tables 3 and 4, several AIDS have been proposed based on ML and DL techniques. Table 3 presents 19 ML-based AIDS, and the majority (13) are for IPv4 networks. SVM and FL algorithms are the two commonly used algorithms for detecting IPv4 and IPv6-based attacks. Meanwhile, the highest detection AC achieved by ML-based AIDSs for IPv4-based attacks is 99.93% (using a DT) and 99.95% for IPv6-based attacks (using SVM). At the same time, the lowest detection AC is 85% (using GA) and 94.55% (using NB) for IPv4 and IPv6, respectively. As for DL-based AIDS, Table 4 lists five proposed DL-based AIDS, but all five are for detecting IPv4 DDoS attacks. DBN is the most common DL algorithm used in AIDS to detect IPv4-based attacks, even though it achieved the lowest detection AC (73%) compared to CNN, which has the best detection AC for DL-based AIDSs (99.98%). However, it is worth noting that researchers typically evaluated their ML or DL-based AIDSs using self-generated datasets.

7. DIFFERENCES BETWEEN ML AND DL

ML and DL techniques are the best methods to build IDS detection models since they can reduce human efforts [16]. However, if it involves training a massive amount of network traffic from a high-speed network, DL-based IDS is the best choice [4]. Several key differences between ML and DL include

structuring, model building duration, computational complexity, effectiveness in dealing with big data, and evaluation metrics, such as detection AC and dimensionality reduction quality. Highlighting these differences would help researchers select the most appropriate technique. Table 5 shows the differences between ML and DL, which could serve as a quick reference for researchers in the field.

Table 5. Differences between the ML and DL

No.	Machine learning	Deep learning
1.	ML is a subset of artificial intelligence.	DL is a subset of ML.
2.	ML achieved high accuracy and detection rate with small data.	DL achieved high accuracy and detection rate with big data.
3.	Faster to train a model.	Computationally intensive.
4.	ML requires more human involvement and effort.	DL requires less human involvement and effort.
5.	It requires trying different features and classifiers to obtain the best results.	It automatically learns features and classifiers.
6.	Usually, the output is a numerical value like a score.	The output can vary from a score, an element, or text.
7.	The input of ML algorithms should be in numerical form.	The input to the DL algorithms could be text, photo, sound, video, and signals.
8.	It requires a shorter time to build a model.	Require a longer time to build and train the model.
9.	Suitable for thousands of data points.	Suitable for big data, i.e., millions of data points.
10.	Less scalability.	Higher scalability.
11.	ML has a low dependency on hardware computational resources.	DL is highly dependent and has a high consumption of hardware computational resources.
12.	ML has learning limitations.	DL has no theoretical limit to what it can learn.

8. CONCLUSION AND FUTURE RESEARCH DIRECTIONS

ML and DL techniques have shown impressive results in solving problems in many research domains, including cybersecurity. Many researchers have adapted ML and DL techniques in AIDS to detect different IPv4 and IPv6-based attacks with high accuracy. Generally, ML and DL techniques are used as classifiers or for feature selection. However, some researchers use ML and DL techniques for both. This paper provides a qualitative comparison that benchmarks this review study with the existing studies. The benchmark reveals a lack of review studies on ML and DL used in AIDS. In addition, this paper presented a comprehensive review of the adaption of ML and DL techniques in AIDS for detecting IPv4 and IPv6 attacks, such as DoS and DDoS flooding attacks.

Moreover, this study revealed that ML and DL techniques significantly contribute to accurately detecting IPv4 and IPv6 attacks. However, ML techniques are more prevalent in IDS compared to DL techniques. Therefore, it is recommended that a review of ML and DL-based AIDS to detect attacks on SDN and IoT networks is conducted in the future. In addition, other techniques used in AIDS, such as statistical, rule-based, and information theory-based techniques, can also be reviewed. Finally, any literature studies on AIDS in the future should also include evaluation metrics based on detection AC, speed, and time since they are critical for evaluating detection techniques' performance.

APPENDIX

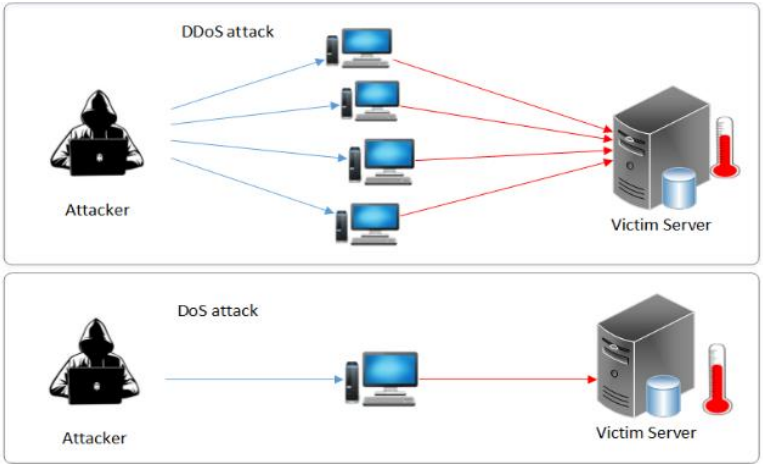

Figure 1. Visual representation of DDoS and DoS attacks architecture

Table 4. Summary of literature on DL-based IDS

Article	Technique	Dataset used	Protocol (IPv4/IPv6)	Detection accuracy	Other performance metrics	Limitations
Kim *et al*. [53]	RNN	KDD CUP 99	IPv4	96.93%	FAR	The authors evaluated their approach by using an old dataset from 1999. This model directly implements LSTM-RNN after collecting samples from the old dataset, i.e., there are no contributions to building an accurate and effective IDS model.
Elejla *et al*. [54]	RNN	NSL-KDD	IPv4	89%	TP, FP, TN, FN	The used dataset has a vast number of redundant records. In addition, other IDS can achieve higher accuracy rates.
Abolhasanzadeh *et al*. [57]	DAE	Own collected. dataset	IPv4	95.06%	AC	The used dataset has many redundant records. The authors directly applied an autoencoder on an old dataset without pre-stages to construct a solid detection model.
Farahnakian and Heikkonen [58]	DAE	KDD CUP 99	IPv4	96.53%	FAR, TP	The authors evaluated their approach by using an old dataset from 1999. In addition, there is no feature engineering that might improve the effectiveness of IDS.
Subbulakshmi *et al*. [31]	DBM	Self-generated dataset	IPv4	-	F-measure	There is no explanation of the achieved accuracy. Also, the authors evaluated their proposed approach with a few evaluation metrics.
Imamverdiyev and Abdullayeva [61]	DBM	NSL-KDD	IPv4	73%	F-measure, G-mean, Precision, recall, sensitivity, specificity, TN, TP	The used dataset has a limitation of a vast number of redundant records. In addition, compared to other approaches, the achieved accuracy rate is not high enough to build an effective detection approach.
Xin and Wang [62]	DBN	KDD CUP99	IPv4	97.82%	TPR, FNR	DBN algorithm is more suitable for selecting features from many unlabeled data, but the authors utilized an old, labeled dataset.
Alom *et al*. [63]	DBN	NSL-KDD	IPv4	97.5%	AC	The dataset has many redundant records. Therefore, this approach seems like a direct implementation of DBN on the old dataset. In addition, there are no more evaluation metrics. The authors evaluated their approach by using an old dataset from 1999.
Fan and Ling-zhi [66]	CNN	KDD CUP 99	IPv4	97.7%	FAR	They used this DL algorithm only for feature extraction, not classification purposes.
Mohammadpour *et al*. [67]	CNN	NSL-KDD	IPv4	99.97%	F-measure	The dataset has many redundant records. In addition, there are no more evaluation metrics for this work. Also, this work is relatively new but features engineering is missing.
Teyou and Ziazet *et al*. [68]	CNN	ISCX 2017	IPv4	99.48%	Precision, Recall, F-score, FPR, FNR	No details about the methodology were provided. It seems like a direct implementation of CNN on the selected dataset.
Liu *et al*. [69]	CNN and RNN	DARPA 1998	IPv4	99.36 %, 99.98%	Precision, Recall, F-measure	The dataset is not comprehensive, as it only comprises IPv4-based attacks.
Liu *et al*. [69]	DNNs	CICIDS 2017	IPv4	98%	F-measure, receiver operating characteristics (ROC)-curve	The detection of this work is based on pre-defined patterns of DDoS attacks, i.e., it cannot detect unknown attacks.
Elejla *et al*. [54]	RNN, GRU, and LSTM	Self-generate dataset	IPv6	98.31%	Recall, Precision, FPR, TPR, FNR, ROC	The RNN model has a low detection AC (92%) and a high FPR.

ACKNOWLEDGEMENTS

Universiti Sains Malaysia supported this work under an external grant (Grant Number 304/PNAV/650958/U154).

REFERENCES

[1] "IPv6 – Google," Google, https://www.google.com/intl/en/ipv6/statistics.html#tab=ipv6-adoption (accessed Apr. 09, 2020).
[2] A. A. Bahashwan, M. Anbar, I. H. Hasbullah, Z. R. Alashhab, and A. Bin-Salem, "Flow-based approach to detect abnormal behavior in neighbor discovery protocol (NDP)," *IEEE Access*, vol. 9, pp. 45512–45526, 2021, doi: 10.1109/ACCESS.2021.3066630.
[3] M. Anbar, R. Abdullah, B. N. Al-Tamimi, and A. Hussain, "A machine learning approach to detect router advertisement flooding attacks in next-generation IPv6 networks," *Cognitive Computation*, vol. 10, no. 2, pp. 201–214, Apr. 2018, doi: 10.1007/s12559-017-9519-8.
[4] A. Drewek-Ossowicka, M. Pietrołaj, and J. Rumiński, "A survey of neural networks usage for intrusion detection systems," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 1, pp. 497–514, 2021, doi: 10.1007/s12652-020-02014-x.
[5] K. Kaur and P. Kakkar, "A review on various machine learning techniques for the detection of DDoS attacks," *International Journal of Innovative Research in Science, Engineering and Technology*, vol. 5, no. 9, 2016, doi: 10.15680/IJIRSET.2016.0509100.
[6] T. A. Alamiedy, M. Anbar, A. K. Al-Ani, B. N. Al-Tamimi, and N. Faleh, "Review on feature selection algorithms for anomaly-based intrusion detection system," in *Recent Trends in Data Science and Soft Computing*, 2019, pp. 605–619.
[7] A. M. Aleesa, B. B. Zaidan, A. A. Zaidan, and N. M. Sahar, "Review of intrusion detection systems based on deep learning techniques: coherent taxonomy, challenges, motivations, recommendations, substantial analysis and future directions," *Neural Computing and Applications*, vol. 32, no. 14, pp. 9827–9858, Jul. 2020, doi: 10.1007/s00521-019-04557-3.
[8] M. A. Ferrag, L. Maglaras, S. Moschoyiannis, and H. Janicke, "Deep learning for cyber security intrusion detection: approaches, datasets, and comparative study," *Journal of Information Security and Applications*, vol. 50, 102419, Feb. 2020, doi: 10.1016/j.jisa.2019.102419.
[9] O. E. Elejla, B. Belaton, M. Anbar, and A. Alnajjar, "Intrusion detection systems of ICMPv6-based DDoS attacks," *Neural Computing and Applications*, vol. 30, no. 1, pp. 45–56, Jul. 2018, doi: 10.1007/s00521-016-2812-8.
[10] A. Aldweesh, A. Derhab, and A. Z. Emam, "Deep learning approaches for anomaly-based intrusion detection systems: a survey, taxonomy, and open issues," *Knowledge-Based Systems*, vol. 189, Feb. 2020, doi: 10.1016/j.knosys.2019.105124.
[11] A. A. Bahashwan, M. Anbar, and S. M. Hanshi, "Overview of IPv6 based DDoS and DoS attacks detection mechanisms," in *Advances in Cyber Security*, 2020, pp. 153–167.
[12] E. Hodo, X. Bellekens, A. Hamilton, C. Tachtatzis, and R. Atkinson, "Shallow and deep networks intrusion detection system: a taxonomy and survey," *arXiv:1701.02145*, pp. 1–43, Jan. 2017.
[13] R. K. Sharma, H. K. Kalita, and P. Borah, "Analysis of machine learning techniques based intrusion detection systems," in *Proceedings of 3rd International Conference on Advanced Computing, Networking and Informatics*, 2016, pp. 485–493.
[14] A. A. Bahashwan, M. Anbar, S. Manickam, I. H. Hasbullah, and M. A. Aladaileh, "Propose a flow-based approach for detecting abnormal behavior in neighbor discovery protocol (NDP)," in *Advances in Cyber Security*, 2021, pp. 401–416.
[15] A. H. H. Kabla, M. Anbar, S. Manickam, and S. Karupayah, "Eth-PSD: a machine learning-based phishing scam detection approach in ethereum," *IEEE Access*, vol. 10, pp. 118043–118057, 2022, doi: 10.1109/ACCESS.2022.3220780.
[16] P. Mishra, V. Varadharajan, U. Tupakula, and E. S. Pilli, "A detailed investigation and analysis of using machine learning techniques for intrusion detection," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 1, pp. 686–728, 2019, doi: 10.1109/COMST.2018.2847722.
[17] A. Javaid, Q. Niyaz, W. Sun, and M. Alam, "A deep learning approach for network intrusion detection system," *Proceedings of the 9th EAI International Conference on Bio-inspired Information and Communications Technologies (formerly BIONETICS)*, 2016, doi: 10.4108/eai.3-12-2015.2262516.
[18] 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, pp. 919–923, doi: 10.1109/ITNG.2010.45.
[19] M. Anbar, R. Abdullah, I. H. Hasbullah, Y.-W. Chong, and O. E. Elejla, "Comparative performance analysis of classification algorithms for intrusion detection system," in *2016 14th Annual Conference on Privacy, Security and Trust (PST)*, Dec. 2016, pp. 282–288, doi: 10.1109/PST.2016.7906975.
[20] P. Winter, E. Hermann, and M. Zeilinger, "Inductive intrusion detection in flow-based network data using one-class support vector machines," in *2011 4th IFIP International Conference on New Technologies, Mobility and Security*, Feb. 2011, pp. 1–5, doi: 10.1109/NTMS.2011.5720582.
[21] D. Kwon, H. Kim, J. Kim, S. C. Suh, I. Kim, and K. J. Kim, "A survey of deep learning-based network anomaly detection," *Cluster Computing*, vol. 22, no. S1, pp. 949–961, Jan. 2019, doi: 10.1007/s10586-017-1117-8.
[22] A. H. H. Kabla *et al.*, "Applicability of intrusion detection system on ethereum attacks: a comprehensive review," *IEEE Access*, vol. 10, pp. 71632–71655, 2022, doi: 10.1109/ACCESS.2022.3188637.
[23] 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, 2020, doi: 10.1109/ACCESS.2020.3000179.
[24] Y. Hamid, M. Sugumaran, and L. Journaux, "Machine learning techniques for intrusion detection," in *Proceedings of the International Conference on Informatics and Analytics*, Aug. 2016, pp. 1–6, doi: 10.1145/2980258.2980378.
[25] T. A. Al-Amiedy, M. Anbar, B. Belaton, A. H. H. Kabla, I. H. Hasbullah, and Z. R. Alashhab, "A systematic literature review on machine and deep learning approaches for detecting attacks in RPL-based 6LoWPAN of internet of things," *Sensors*, vol. 22, no. 9, p. 3400, Apr. 2022, doi: 10.3390/s22093400.
[26] 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.
[27] R. Vijayasarathy, S. V Raghavan, and B. Ravindran, "A system approach to network modeling for DDoS detection using a Na," in *2011 Third International Conference on Communication Systems and Networks (COMSNETS 2011)*, Jan. 2011, pp. 1–10, doi: 10.1109/COMSNETS.2011.5716474.

[28] A. Salih, X. Ma, and E. Peytchev, "No detection and classification of covert channels in IPv6 using enhanced machine learning," in *Proc. of The International Conference on Computer Technology and Information Systems*, 2015, pp. 1–7.
[29] S. R. Sain, "The nature of statistical learning theory," *Technometrics*, vol. 38, no. 4, Nov. 1996, doi: 10.1080/00401706.1996.10484565.
[30] A. Elsaeidy, 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.
[31] 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. 04, no. 02, pp. 737–743, Jun. 2013, doi: 10.21917/ijct.2013.0105.
[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*, vol. 2018, pp. 1–8, 2018, doi: 10.1155/2018/9804061.
[33] M. Zulkiflee, M. Ahmad, S. Sahib, and M. Ghani, "A framework of features selection for IPv6 network attacks detection," *WSEAS Transactions on Communications*, vol. 14, no. 46, pp. 399–408, 2015.
[34] 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.
[35] 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.
[36] S. K. Pydipalli, S. Kasthuri, and J. S, "DDoS detection system using C4.5 decision tree algorithm," *International Research Journal of Engineering and Technology (IRJET)*, vol. 14, no. 10, 2018.
[37] R. Ali and S. Kamthania, "A comparative study of different relevant features hybrid neural networks based intrusion detection systems," *Advanced Materials Research*, vol. 403–408, pp. 4703–4710, Nov. 2011, doi: 10.4028/www.scientific.net/AMR.403-408.4703.
[38] R. M. A. Saad, M. Anbar, S. Manickam, and E. Alomari, "An intelligent ICMPv6 DDoS flooding-attack detection framework (v6IIDS) using back-propagation neural network," *IETE Technical Review*, vol. 33, no. 3, pp. 244–255, May 2016, doi: 10.1080/02564602.2015.1098576.
[39] 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.
[40] 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.
[41] 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.
[42] 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/ijsia.2015.9.9.18.
[43] C. Balarengadurai and S. Saraswathi, "Comparative analysis of detection of DDoS attacks in IEEE 802.15.4 low rate wireless personal area network," *Procedia Engineering*, vol. 38, pp. 3855–3863, 2012, doi: 10.1016/j.proeng.2012.06.442.
[44] L. Yao, L. ZhiTang, and L. Shuyu, "A fuzzy anomaly detection algorithm for IPv6," in *2006 Semantics, Knowledge and Grid, Second International Conference on*, 2006, p. 67, doi: 10.1109/SKG.2006.5.
[45] R. M. A. Saad, "ICMPv6 flood attack detection using DENFIS algorithms," *Indian Journal of Science and Technology*, vol. 7, no. 2, pp. 168–173, Feb. 2013, doi: 10.17485/ijst/2014/v7i2.5.
[46] M. Al-Shalabi, M. Anbar, and T.-C. Wan, "Genetic algorithm based protocols to select cluster heads and find multi-hop path in wireless sensor networks: review," *MATEC Web of Conferences*, vol. 218, 3019, Oct. 2018, doi: 10.1051/matecconf/201821803019.
[47] A. Chaudhary and G. Shrimal, "Intrusion detection system based on genetic algorithm for detection of distribution denial of service attacks in MANETs," *SSRN Electronic Journal*, 2019, doi: 10.2139/ssrn.3351807.
[48] 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.
[49] A. H. Hasan, M. Anbar, and T. A. Alamiedy, "Deep learning approach for detecting router advertisement flooding-based DDoS attacks," *Journal of Ambient Intelligence and Humanized Computing*, pp. 1–15, Nov. 2022, doi: 10.1007/s12652-022-04437-0.
[50] Y. Bengio, "Learning deep architectures for AI," *Foundations and Trends®in Machine Learning*, vol. 2, no. 1, pp. 1–127, 2009, doi: 10.1561/2200000006.
[51] M. A. Ferrag, L. A. Maglaras, H. Janicke, and R. Smith, "Deep learning techniques for cyber security intrusion detection : a detailed analysis," in *6th International Symposium for ICS & SCADA Cyber Security Research 2019*, Sep. 2019, pp. 126–136, doi: 10.14236/ewic/icscsr19.16.
[52] T. A. Tang, D. McLernon, L. Mhamdi, S. A. R. Zaidi, and M. Ghogho, "Intrusion detection in SDN-based networks: deep recurrent neural network approach," in *Deep Learning Applications for Cyber Security*, 2019, pp. 175–195.
[53] 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.
[54] O. E. Elejla, M. Anbar, S. Hamouda, S. Faisal, A. A. Bahashwan, and I. H. Hasbullah, "Deep-learning-based approach to detect ICMPv6 flooding DDoS attacks on IPv6 networks," *Applied Sciences*, vol. 12, no. 12, Jun. 2022, doi: 10.3390/app12126150.
[55] L. Deng, "A tutorial survey of architectures, algorithms, and applications for deep learning," *APSIPA Transactions on Signal and Information Processing*, vol. 3, Jan. 2014, doi: 10.1017/atsip.2013.9.
[56] M. Borovcnik, H.-J. Bentz, and R. Kapadia, "A probabilistic perspective," in *Chance Encounters: Probability in Education*, Dordrecht: Springer Netherlands, 1991, pp. 27–71.
[57] 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.

[58] 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.2018.8323688.
[59] R. M. A. Ujjan, Z. Pervez, K. Dahal, A. K. Bashir, R. Mumtaz, and J. González, "Towards sFlow and adaptive polling sampling for deep learning based DDoS detection in SDN," *Future Generation Computer Systems*, vol. 111, pp. 763–779, Oct. 2020, doi: 10.1016/j.future.2019.10.015.
[60] M. Asad, M. Asim, T. Javed, M. O. Beg, H. Mujtaba, and S. Abbas, "Deepdetect: detection of distributed denial of service attacks using deep learning," *The Computer Journal*, vol. 63, no. 7, pp. 983–994, Jul. 2020, doi: 10.1093/comjnl/bxz064.
[61] 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.
[62] M. Xin and Y. Wang, "Research on feature selection of intrusion detection based on deep learning," in *2020 International Wireless Communications and Mobile Computing (IWCMC)*, Jun. 2020, pp. 1431–1434, doi: 10.1109/IWCMC48107.2020.9148217.
[63] 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.
[64] F. Qu, J. Zhang, Z. Shao, and S. Qi, "An intrusion detection model based on deep belief network," in *Proceedings of the 2017 VI International Conference on Network, Communication and Computing*, Dec. 2017, pp. 97–101, doi: 10.1145/3171592.3171598.
[65] Y. LeCun, "Learning invariant feature hierarchies," in *Computer Vision – ECCV 2012. Workshops and Demonstrations*, 2012, pp. 496–505.
[66] J. Fan and K. Ling-zhi, "Intrusion detection algorithm based on convolutional neural network," *Transactions of Beijing Institute of Technology*, vol. 37, no. 12, pp. 1271–1275, 2017.
[67] G. K. De Teyou and J. Ziazet, "Convolutional neural network for intrusion detection system in cyber physical systems," *Prepr. arXiv.1905.03168*, May 2019.
[68] S. Haider, A. Akhunzada, G. Ahmed, and M. Raza, "Deep learning based ensemble convolutional neural network solution for distributed denial of service detection in SDNs," in *2019 UK/ China Emerging Technologies (UCET)*, Aug. 2019, pp. 1–4, doi: 10.1109/UCET.2019.8881856.
[69] H. Liu, B. Lang, M. Liu, and H. Yan, "CNN and RNN based payload classification methods for attack detection," *Knowledge-Based Systems*, vol. 163, pp. 332–341, Jan. 2019, doi: 10.1016/j.knosys.2018.08.036.

BIOGRAPHIES OF AUTHORS

Arkan Hammoodi Hasan Kabla was born in Iraq in 1993. He received a B.Sc. degree in software engineering in Iraq in 2016 and an M.Sc. degree in internet engineering from Universiti Sains Malaysia (USM), Malaysia, in 2020, where he is currently pursuing the Ph.D. degree with the National Advanced IPv6 Centre (NAv6). His research interests include machine learning, deep learning, anomaly detection, blockchain, and P2P networks. He can be contacted at email: arkantaha93@gmail.com.

Mohammed Anbar obtained his Ph.D. in Advanced Internet Security and Monitoring from University Sains Malaysia (USM). He is currently a senior lecturer at National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia. His current research interests include malware detection, web security, intrusion detection systems (IDS), intrusion prevention systems (IPS), network monitoring, internet of things (IoT), and IPv6 security. He can be contacted at email: anbar@usm.my.

Shady Hamouda is a faculty member at the Department of Information technology at the Department of Business Information Technology, Liwa College of Technology, Abu Dhabi, United Arab Emirates. He has over 13 years of experience and is highly motivated, with a proven track record in Information Systems and Teaching. He got a PhD from the Faculty of Computer Sciences, University Sains Malaysia, and Malaysia. He obtained his master's degree from the Faculty of Information Technology, University Utara Malaysia, Malaysia, and his bachelor's degree from the Faculty of Computer Engineering & Information Technology, Al Azhar University, Palestine. He can be contacted at email: shady.hamouda@ect.ac.ae.

Abdullah Ahmed Bahashwan received a B.Sc. degree in computer applications from Osmania University, Hyderabad, India, in 2012 and an M.Sc. degree in internet engineering from the National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia (USM) in 2020, where he is currently pursuing the Ph.D. degree. His research interests include computer networks, Internet Protocol version 6 (IPv6) security, network security, intrusion detection systems (IDS), cloud computing, software defines networks (SDN), and the Internet of Things (IoT). He can be contacted at email: aalhajran2011@gmail.com.

Taief Alaa Al-Amiedy received a B.Sc. degree in electronics and communication engineering from the University of Kufa, Iraq, and an M.Sc. degree in internet engineering from Universiti Sains Malaysia, Malaysia, where he is currently pursuing a Ph.D. degree with the National Advanced IPv6 Centre (NAv6). His current research interests include mobile and wireless communication, machine and deep learning techniques, network security, intrusion detection systems (IDSs), the internet of things (IoT), and RPL security. He can be contacted at email: taiefalaa@gmail.com**.**

Iznan Husainy Hasbullah received a B.Sc. degree in electrical engineering from Rensselaer Polytechnic Institute, Troy, NY, USA. He is currently pursuing an M.Sc. degree in advanced network security. He has experience working as a Software Developer, a Research and Development Consultant, and a Network Security Auditor before joining the National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia, in 2010, as a Research Officer. His research interests include unified communication, telematics, network security, network protocols, and next-generation networks. He can be contacted at email: iznan@usm.my.

Serri Faisal is an Assistant Professor and the Head of Business Information Technology at the Emirates College of Technology. He holds a bachelor's and a Master of Science in Computer Science from Texas State University and a PhD in Technology Management from Universiti Tun Hussein Onn Malaysia. In addition to teaching for over nine years, he served as a Senior IT Project Manager and an IT Infrastructure Consultant. While working in the industry for over 15 years, he gained broad experience in implementing information technology solutions while leading several key projects in Fortune 500 companies like Dell Technologies, Computer Science Corporation (CSC), and other recognized software and financial companies in the United States. His current academic research is in applications' persuasive system design. He can be contacted at email: serri.faisal@ect.ac.ae.