REVIEW OF IDS, ML AND DEEP NEURAL NETWORK TECHNIQUE IN DDOS ATTACKS

Om Vasu Prakash Salmakayala, Saeed Shiry Ghidary,
and Christopher Howard

School of Digital, Technology, Innovation and Business at
Staffordshire University,
Stoke on Trent, Staffordshire-ST4 2DE, United Kingdom

ABSTRACT

Intrusion Detection Systems (IDS) and firewalls often struggle to identify malicious packets, creating opportunities for threat actors to exploit vulnerabilities. Advanced tactics are used by threat actors to bypass these detection mechanisms. They employ evasion techniques, such as adjusting anomalies or thresholds in anomaly-based systems and injecting ambiguity into packet data, which confuses IDS and firewalls. Despite previous applications of machine learning (ML) in cybersecurity, challenges persist. This research aims to review traditional IDS failures and examine the evolution of ML and deep neural networks (DNN) from their basic functionalities to advanced mechanisms. This study also summarizes the types of ML and DNN, along with their techniques in various applications, both individually and in combination, with a focus on detecting ICMPv4/ICMPv6 DDoS attacks and the necessity of integrating both to mitigate such attacks.

KEYWORDS

AI, ML, DDOS-attack, DNN, ICMPv6.

1. INTRODUCTION

With the rapid advancements in emerging computing technologies, including Cloud computing and the Internet of Things (IoT), the incidence of Distributed Denial of Service (DDoS) attacks has witnessed a substantial surge in frequency. This escalating trend poses a significant and pervasive threat, establishing DDoS attacks as one of the most formidable challenges in the realm of cybersecurity. The widespread adoption of cloud-based infrastructures and the interconnected nature of IoT devices contribute to the amplification of these attacks, underscoring the pressing need for robust cybersecurity measures to mitigate and counteract the escalating risks on the Internet [1]. There are many attacks in the network targeting some important services and systems to break/crash resulting in the freezing of business thus causing great financial loss. The most targeted service is Denial of Service (DoS) which is at the Host level and Distributed Denial of Service (DDoS) which is at the Core level are among them. There are many preventive techniques to stop DDoS, yet the attackers can succeed due to the change of approaches based on the vulnerabilities present in the victim's network, applications, protocols and infrastructure. Most of the earlier researchers have come up with anomaly detection which is to find a pattern of certain problems that is based on a behavior at the Network layer. Such patterns are often referred to as anomalies, outliers, discordant observations, etc. [2]. As per Martin Holkovic, there are

David C. Wyld et al. (Eds): DMSE, CSEIT, NeTCoM, SPM, CIoT, NCS, NLPD, ArIT, CMLA – 2024
pp. 319-338, 2024. CS & IT - CSCP 2024 DOI: 10.5121/csit.2024.141424

network managements that are maintained based on a rule-based system, for example, the Supervisory Control and Data Acquisition (SCADA) network used for maintaining or troubleshooting. These systems are mainly used for per-flow or packet analysis and their limitations are not extendable and should have good language knowledge and not userfriendly [3]. Saad developed a rule-based approach for anomaly behaviour detection using Snort's novel functionalities to enhance an open-source network intrusion detection system. It is similar to the mechanism that is used by anti-virus tools such as Kaspersky's where the Yara rule is employed for identifying malicious activity in files and malware. The same or a combination can be applied to DDoS attacks [4].

2. IMPLEMENTATION METHOD FOR REVIEW OF ML AND DNN

Figure 1 illustrates the block diagram indicating the basic steps implemented for preparing the review of IDS, ML, and DNN.

- **Resources exploring:** The process begins with available resources that were explored such as Scival, Google Scholar and online University Library.

- **Publication list:** Papers were collected related to the publication list shown in Figure 1 using the Keywords search IDS, DoS, DDoS, IDS, etc., and also a further combination of small phrases of these keywords like "A review of IDS or DNN or ML", "Detection of DDoS attacks using DNN, Detection of ICMP attacks using ML/AI", etc.

- **Domain-based filtration:** The above list is further filtered specifically based on the Networking security domain. These could be related to SDN, IDS, Wireless security, cybersecurity, etc.

- **Segregation based on AI/ML techniques:** Further, these were segregated based on DNN, RNN, GRU, CNN, LSTM, ML, etc. with respect to ICMPv6.

- **Collection based on a combination of year and number of citations:** These were further filtered based on the year and number of citations. Mostly last 3 to 5 years were shortlisted and citations generally from 5 or more are considered. However, if it is a recent and current year and the paper is related to the above parameters and has no citations or less than 5 are also considered.

- **Based on Abstract, research gap, etc.:** Once these were collected, they were finalized focusing more on the abstract, research gap related to DDoS attacks mitigation using DNN/ML techniques, future research and conclusion. Based on the main motivation of the paper these finalized papers are summarized and further important notes are prepared to add those summaries to build a research paper. The entire work was finally transformed into a research paper reviewing DDoS attacks, narrowing down more on ICMP-related attacks, based on IDS, ML, and DNN methodologies.

Further, a list of researchers list is also provided in each section with brief details of their work. Figure 1 illustrates a simple block diagram of how the review method is implemented

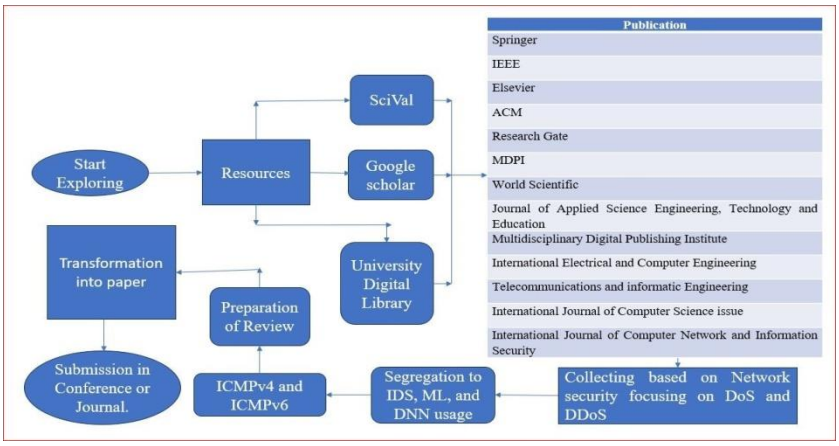

Fig.1. Implementation Method for Review of ML and DNN

3. RELATED WORK

In the realm of DDoS Attacks using Malware, two primary methodologies exist, Signature-based Detection and Anomaly-based Detection. While Signature-based detection has historically been effective, it falters when confronting malicious scripts or bots due to their continual mutation. As these methods evolve, so do their signatures, rendering traditional detection methods ineffective against new variants. In contrast, Anomaly-based detection techniques, which operate on the premise that malicious behaviour deviates from normal traffic patterns, have gained prominence for their adaptability to detect emerging new variations in real-world scenarios due to which current IDS detections are failed [1]. Advanced Persistent Threat (APT) attacks represent a distinct form of network intrusion, leveraging coordinated human actions rather than automated scripts. APT attacks entail persistent monitoring and engagement with a target entity until specific objectives are met. In contrast, Distributed Denial of Service (DDoS) attacks seek to disrupt network functionality by overwhelming resources, often lacking further strategic goals. The Mirai botnet, a notable instance of a DDoS attack, incapacitated numerous websites, including Twitter, Netflix, Reddit, and GitHub, for several hours in October 2016. Presently, Mirai variants emerge daily, posing ongoing threats capable of inflicting substantial harm to networks [5]. Internet Protocol Version 6 (IPv6) is the most recent generation of Internet protocol. The transition from the current Internet Version 4 (IPv4) to IPv6 raised new issues and the most crucial issue is security vulnerabilities. Most vulnerabilities are common between IPv4 and IPv6, e.g. Evasion attacks, Distributed Denial of Service (DDoS) and Fragmentation attacks. According to the IPv6 RFC (Request for Comment) recommendations, there are potential attacks against various Operating Systems. Discrepancies between the behaviour of several Operating Systems can lead to Intrusion Detection System (IDS) evasion, Firewall evasion, Operating System fingerprint, Network Mapping, DoS/DDoS attack and Remote code execution attack [7].

4. TRADITIONAL IDS

In rule-based detection, the system identifies required behaviors from network traffic and gathers information about potential vulnerabilities. Leveraging this knowledge, it detects abnormal events and raises alarms when attacks are detected. This method entails establishing a set of rules that define common attack patterns and deriving conclusions from these rules and gathered data. Incoming traffic instances are then compared against these rules to identify any instances of suspicious behaviour and inconsistencies within the system.

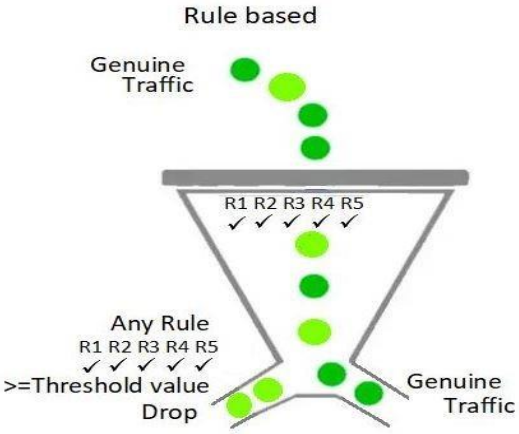

Fig.2. Logical approach of Rule base anomaly

Figure 2 depicts the logical approach to capture the anomaly behaviour by an IDS without any ML or any AI employed. The system employs continuous monitoring to detect anomalous traffic patterns, which signify deviations from the norm. While it efficiently identifies systematic attacks, abrupt alterations in network behaviour or conditions beyond preset parameters pose a challenge. Additionally, the detection method relies on Boolean association rules to unveil irregularities among attributes. However, as the number of attributes increases, the process slows down, making the management of numerous rules difficult [8]. Aamir conducted a comprehensive examination of Distributed Denial of Service (DDoS) attacks and associated defence strategies, focusing on contemporary DDoS defence mechanisms leveraging entropy fluctuations, traffic anomalies, neural networks, and application layer defences. Additionally, they offered insights into traditional techniques such as traceback and packet filtering. Furthermore, they shed light on emerging threats facilitated by new tools like botnet fluxing, GET floods, and reflector attacks, which present formidable challenges in detection and mitigation [9]. Khamruddin proposed a three-step rule-based approach for DDoS attack detection and classification. Initially, the destination router, connected to the victim, continuously monitors traffic patterns. Secondly, upon detecting an attack, the destination router attempts to balance the load using Network Address Translation (NAT). Thirdly, upon attack detection, various attack signatures are pushed back to upstream routers, prompting them to monitor traffic and apply suitable mitigation mechanisms based on the type of attack identified [10]. Bdair presented a concise examination of DDoS (Distributed Denial of Service) attacks, shedding light on the vulnerabilities of intrusion detection systems in the context of IPv6. Various detection mechanisms, such as anomaly, signature, and hybrid approaches, were outlined. An emphasis was placed on the growing interest in anomaly-based detection, utilizing rulebased methodologies. Additionally, he also pointed out the susceptibility of unsecured messages within the ICMPv6 protocol. Moreover, he hinted at proposing an Optimization Algorithm technique, aiming to enhance the intrusion detection system either through adoption or hybridization with a meta-heuristic algorithm, thus increasing its capability to detect DDoS attacks [11].

Bahashwan Provided an overview of IPv6 DDoS attack detection emphasising signature, anomaly, Rule, Entropy, Machine Learning and Deep learning-based mechanisms and techniques. It also briefs about the approach to detect, mitigate, and classify IPv6 attacks and effectively summarises their advantages and disadvantages [12]. Wu, Zhijun presented a novel research approach utilizing time-frequency analysis for the classification and mitigation of DDoS attacks, encompassing both FDDoS and LDDoS variants. Subsequently, he developed and evaluated a practical filtering system to validate the efficacy of the proposed method. The results

demonstrated significant filtering effectiveness against both FDDoS and LDDoS attacks, ensuring uninterrupted and stable service provision to legitimate users [13]. Rajat Tandon introduced AMON-SENSS, an open-source solution engineered to address the demands of scalable and precise DDoS detection, along with signature generation within expansive networks. AMON-SENSS adopts a hash-based binning strategy featuring multiple bin layers to ensure scalability, while simultaneously leveraging traffic analysis at various granularities. Additionally, it implements advanced techniques such as traffic volume and traffic asymmetry change-point detection to effectively pinpoint malicious activities. Consequently, their findings demonstrate AMONSENSS's outperformed in terms of metrics like accuracy, latency, and network signature quality compared to existing commercial alternatives [6].

For example, Saad has framed 5 rules in his research on ICMPv6 DDOS detection which are explained below:

"**Rule 1:** One-way connection density in IPv6 networks which is inbound link utilization (bytes/s). The ICMPv6 packets that are sent without a corresponding response packet create a one-way connection (OC). ICMPv6OC is the ratio of OC packets to all packets in a sampling time interval T. If this exceeds the predetermined value, then it implies an abnormal behaviour is detected.

Rule 2: Generally, in ICMPv6 flow, a packet set with the same five-component group (IPv6 source, IPv6 destination, source port, destination port and protocol), is used in the network analysis. The number of packets that belong to a certain ICMPv6 flow is called the length of ICMPv6 flow. This rule is to detect the anomaly behaviour if the average length of ICMPv6 flow exceeds the given threshold.

Rule 3: The ratio between inbound and outbound packets is usually steady. However, in an ICMPv6 anomalous behaviour attack, the ratio of this traffic increases rapidly. This rule is to determine as an attack if the anomaly behaviour that exceeds the given threshold value.

Rule 4: The ratio of ICMPv6 echo request packet is the rate of set of ICMPv6 packet arrival to that of length of time interval (T1, T2, T3 ,..Tn). This rule is to detect the anomaly behaviour if the rate of ICMPv6 packet echo request arrivals from a network to the set at the same length of time interval exceeds a threshold value count.

Rule 5: In this rule, the count is used to determine the same number of sources IPv6 and the destination IP address. This rule is to detect the anomaly behaviour, if the number of packets has the same IPsrcont address source and IPdscont address destination exceeds the threshold value." [4].

Abnormal activities exceeding or deviating the threshold are concluded as an attack. The ICMPv6 has emerged based on the limitation of address space in the IPv4. However, IPv6 was developed with neighbour discovery protocol i.e. NDP which has vulnerabilities that can be exploited by attackers to launch an attack in the form of ICMPv6 which includes the lack of exchange of message authentication of NDP. Some of the attacks related to ICMPv6 are network reconnaissance attacks, routing headers, fragment headers and multicasting. The preceding discussion outlines the utilization of rule-based mechanisms for detecting and mitigating DDoS attacks, particularly focusing on ICMPv6 packets. However, as technology evolves, new attack vectors emerge, posing challenges at both hardware and application levels. This evolution has spurred the adoption of automation, leading to the integration of machine learning (ML), artificial intelligence (AI), and deep neural networks (DNN) to enhance defence mechanisms against these evolving threats. As technology progresses, attackers become more sophisticated, adapting their

methods to circumvent traditional defences. This paper aims to provide a comprehensive overview of ML and AI techniques employed by various researchers, exploring their efficacy in addressing DDoS attacks. Additionally, it seeks to identify novel approaches or methodologies that offer promising results while acknowledging their inherent limitations.

5. A BRIEF REVIEW OF ML

Based on the basic threshold and comparison mechanism in the previous section where IDS are designed and why they fail in detecting the attack methods or techniques used by the threat attackers. This section focuses on the Various techniques and algorithms used in ML. Ojugo conducted a study comparing machine learning methods for DDoS detection. They contrasted the Hidden Markov Model with an Experimental Hybrid (Memetic) Genetic Algorithm Trained Neural Network, which was based on a RuleGenerated and Fitness Function Model. Their evaluation utilized IDS datasets (CIDDS2017), comprising labelled network flow data for anomaly-based traffic. They allocated 70% of the dataset for training and 30% for testing, achieving a fitness range between 0.8 and 0.865. Their results indicated an estimated 80% classification accuracy for detection [14]. Liang conducted a thorough empirical evaluation of machine learning-based DDoS detection methods, with a primary focus on addressing the class imbalance problem. They underscored the importance of feature selection, advocating for a model-oriented approach. Their evaluation, employing datasets from CAIDA and DARPA, utilized the correlation coefficient across various algorithms including Decision Trees (DT), Support Vector Machines (SVM), Radial Basis Function SVM (RBF-SVM), Polynomial SVM (Poly-SVM), K-Nearest Neighbour (KNN), K-Means, Naive Bayes (NB), Artificial Neural Networks (ANN), and D-Ward. Remarkably, their approach achieved a DWard score of 77.03%, outperforming other algorithms in the evaluation [15]. Alharbi developed an improved KNN algorithm, termed GR-AD-KNN, to enhance the detection of ICMPv6 DoS attacks. This algorithm utilizes the information gain rate to assign weights to different features, allowing them to have varying degrees of influence on the classification process. By integrating the concept of offset increment average distance, the measurement of the target point is refined, enhancing the algorithm's stability. This refinement specifically addresses the varying impact of long and short-distance sample points on decisionmaking, leading to more reliable detection outcomes[31]. Zewdie has developed an evaluation framework utilizing machine learning techniques to detect Denial of Service (DoS) and Distributed Denial of Service (DDoS) intrusions. By applying algorithms such as K-Nearest Neighbour, Decision Trees, and Random Forests, she conducted experiments using the CIC-IDS2017 dataset. The results revealed impressive precision metrics, with accuracies ranging from 92.19% to 99.66% [32]. Manjula implemented three classifiers K-Nearest Neighbour (KNN), Random Forest, and Naive Bayes on datasets generated using Wireshark besides applying the LOIC attack tool. Among these, the Random Forest classifier achieved the highest accuracy of 96.75%, demonstrating the model's effectiveness in detecting ICMP, TCP, and UDP flood attacks [33]. Further, secondary research in the form of a summary table about ML used by different authors for DDoS and IDS attacks was provided in Figure 3.

Objective	Algorithm	Dataset	FS Approach	Classification Type	IDS Domain	Ref.
Traffic awareness-based IDS to maintain regulated traffic in SDN.	RF	KDD'99	RF Based on vote count of correct classes.	Binary Classification: Normal class and Anomaly class.	Flow-based	C. Song, Y. Park, K. Golani, Y. Kim, K. Bhatt, and K. Goswami, "Machine-learning based threat-aware system in software defined networks," 2017 26th Int. Conf. Comput. Commun. Networks, ICCCN 2017, 2017.
Recognition of DDoS anomaly flows in SDN.	KNN	Self-Collected data From multiple data centres.	Not Mentioned	Binary Classification: Normal and DDoS.	Flow-based	H. Peng, Z. Sun, X. Zhao, S. Tan, and Z. Sun, "A Detection Method for Anomaly Flow in Software Defined Network," IEEE Access, vol. 6, pp. 27809–27817, 2018.
Detection of DDoS attack in SDN using a meta-huristic method.	Fitting Curve, Pattern Recognition, Time Series	NSL-KDD	Manual Selection	Multiclass Classification: Normal, DoS, R2L, Probe, U2R, and Unknown.	Flow-based	A. Abubakar and B. Pranggono, "Machine Learning Based Intrusion Detection System for Software Defined Networks," Int. Conf. Emerg. Secur. Technol., pp. 138–143, 2015.
SVM based IDS for SDN in cloud data centre.	SVM	DARPA 1998	Manual Selection	Multiclass Classification: Normal, DoS, U2R, R2L, and Probe.	Flow-based Packet-based Log-based	Q. Schueller, K. Basu, M. Younas, M. Patel, and F. Ball, "A Hierarchical Intrusion Detection System using Data Center," in 2018 28th International Telecommunication Networks and Applications Conference (ITNAC), 2018, pp. 1–6.
Analyse flow statistics and develop an SVM based real-time DDoS attack detection and resistance model.	SVM	KDD'99	Not Mentioned	Binary Classification: Normal class and DDoS class.	Flow-based	L. Yang and H. Zhao, "DDoS attack identification and defence using SDN based on machine learning method," in Proceedings - 2018 15th International Symposium on Pervasive Systems, Algorithms and Networks, I-SPAN 2018, 2019, pp. 174–178.
Build a Two-level ML based IDS in SDN.	ID3	Not Mentioned.	Genetic algorithm	Not Mentioned.	Flow-based Packet-based	[V. Vetriselvi, P. S. Shruti, and S. Abraham, "Two-level intrusion detection system in SDN using machine learning," in Proceedings of the International Conference on Communications and Cyber Physical Engineering, 2018, pp. 449–461.
DDoS attack (TCP-SYN and ICMP Flood) detection in the SDN enabled ISP networks.	KNN, XG Boost	CAIDA 2007	Based on Time window monitoring and entropy calculation	Binary Classification: Normal and DDoS.	Flow-based Statistics based	N. N. Tuan, P. H. Hung, N. D. Nghia, N. Van Tho, T. Van Phan, and N. H. Thanh, "A DDoS attack mitigation scheme in ISP networks using machine learning based on SDN," Electron., vol. 9, no. 3, pp. 1–19, 2020.
Building a robust classification system to detect DDoS attack by reducing the dependency on outdated data.	J48, Bayes Net, Random Tree, REP Tree, NB, LR.	UNB-ISCX, CTU 13, ISOT.	Manual Selection based on neighbouring nodes.	Binary Classification: Normal and DDoS.	Flow-based	A. Banitalebi Dehkordi, M. R. Soltanaghaei, and F. Z. Boroujeni, "The DDoS attacks detection through machine learning and statistical methods in SDN," J. Supercomput., vol. 77, no. 3, pp. 2383–2415, 2020
Low-rate DDoS attack detection using ONOS controller and ML methods.	J48, REP Tree, RF Random Tree, SVM, MLP	CIC-DDoS-2019	Manual selection	Binary Classification: Normal and DDoS.	Flow-based	J. A. Perez-Diaz, I. A. Valdovinos, K. K. R. Choo, and D. Zhu, "A Flexible SDN-Based Architecture for Identifying and Mitigating LowRate DDoS Attacks Using Machine Learning," IEEE Access, vol. 8, pp. 155859–155872, 2020
SYN-Flood DDoS attack detection in SDN.	RF, LR, KNN, SVM	CICIDS, DARPA 2009	Ranker algorithm	Binary Classification: Benign and Malicious.	Flow-based Packet-based	J. Aiken and S.-H. Sandra, "Investigating Adversarial Attacks against Network Intrusion Detection Systems in SDNs," in IEEE Conference 44 on Network Functions Virtualization and Software Defined Networks, 2019, pp. 1–7
Performance analysis of four ML algorithms to identify DDoS attack in the SDN.	MLP, DT, SVM, RF	Simulated Data.	Experimental Trail-based	Binary Classification: Normal and DDoS.	Flow-based	R. Santos, D. Souza, W. Santo, A. Ribeiro, and E. Moreno, "Machine learning algorithms to detect DDoS attacks in SDN," Concurr. Comput. Pract. Exp., vol. 32, no. 16, pp. 1–14, 2020
SVM incorporated with selective IP traceback-based IDS mechanism for SDN.	SVM	NSL-KDD	Manual Selection	Binary Classification: Normal and Attack.	Flow-based	P. Hadem, D. K. Saikia, and S. Moulik, "An SDN-based Intrusion Detection System using SVM with Selective Logging for IP Traceback," Comput. Networks, vol. 191, no. September 2020, p. 108015, 2021.
DDoS Flooding Occurrence recognition and mitigation scheme in SDN.	SVM	Real-Time Traffic Collected from home office and ISP.	Shannon Entropy	Binary Classification: Normal and DDoS.	Flow-based	D. Hu, P. Hong, and Y. Chen, "FADM: DDoS Flooding Attack Detection and Mitigation System in Software-Defined Networking," in GLOBECOM 2017-2017 IEEE Global Communications Conference., 2017, pp. 1–7
DDoS attack detection using feature selection and ML-based techniques in SDN.	SVM, ANN, KNN, NB	Self-Generated Simulated Data	Filter, Wrapper and Embedded based method.	Multiclass Classification: Normal, TCP, ICMP, and UDP.	Flow-based	H. Polat and O. Polat, "Detecting DDoS Attacks in Software-Defined Networks Through Feature Selection Methods and Machine Learning Models," sustainability, vol. 12, no. 3,1035, 2020
Detection and Mitigation of DDoS attack in SDN though φ-entropy incorporating with SVM and KNN classifier.	KNN, SVM	Synthetic Data generated using Hping3 and Nping.	Shannon entropy & φ-entropy	Multiclass Classification: Normal, SYN, ICMP, UDP, ACK, TCP Connection, and Flash event.	Flow-based Statistics based	G. Sun, W. Jiang, Y. Gu, D. Ren, and H. Li, "DDoS Attacks and Flash Event Detection Based on Flow Characteristics in SDN," in Proceedings of AVSS 2018-15th IEEE International Conference on Advanced Video and Signal-Based Surveillance, 2018, pp. 1–6.
Advanced-SVM-based DDoS Detection in SDN.	SVM	Real-Time Traffic	Manual Selection	Binary Classification: Normal and DDoS.	Flow-based	M. M. Oo, S. Kamolphiwong, and T. Kamolphiwong, "The Design of SDN Based Detection for Distributed Denial of Service (DDoS) Attack," ICSEC - 21st Int. Comput. Sci. Eng. Conf., vol. 6, pp. 258– 263, 2018.

Fig.3. ML Summary Table [23]

5.1. Types of ML

Machine learning is a subset of artificial intelligence (AI) focused on developing algorithms that allow computers to learn from and make predictions or decisions based on data. Figure 4 illustrates a simple Machine Learning Classifier.[36]

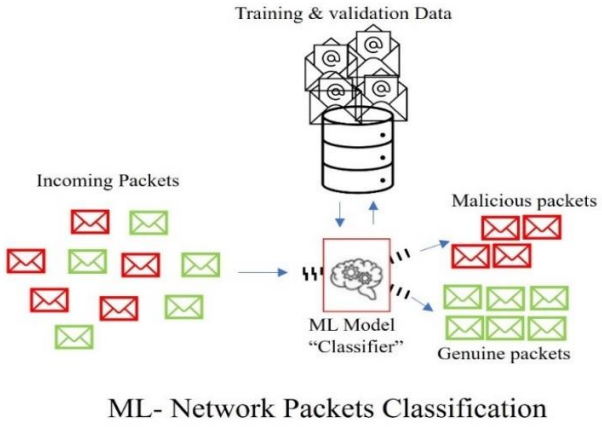

Fig.4. ML as a Classifier

I. **Supervised ML:** Itis a machine learning type where a model is trained using labelled data. In this context, "labelled data" means that each training example is paired with an output label. The goal of supervised learning is to learn a mapping from inputs to outputs based on these examples so that the model can predict the output labels for new, unseen data. They are used for spam detection, image recognition, speech, text, voice, etc.

- **Linear Regression**: Used for regression problems.
- **Logistic Regression**: Used for binary classification problems.
- **Decision Trees**: Used for both classification and regression problems.
- **Support Vector Machines (SVM)**: Used for classification tasks.
- **k-Nearest Neighbours (k-NN)**: Used for both classification and regression tasks.
- **Naive Bayes**: Used for classification problems. [35]

II. **Unsupervised ML**: Itis a machine learning type where a model is trained using data that does not have labelled responses. In this approach, the algorithm tries to learn the underlying structure or distribution in the data to uncover hidden patterns or groupings without any prior knowledge of the outcomes. They are used for mainly Clustering purposes like Hierarchical, special big data, Images, health records, Network Logs, etc.

- **K-Means Clustering**: Partitions data into K distinct clusters.
- **Hierarchical Clustering**: Builds a hierarchy of clusters.
- **DBSCAN**: Clusters data based on density, identifying clusters of arbitrary shape.
- **Principal Component Analysis (PCA)**: Reduces the dimensionality of the data while preserving as much variance as possible.
- **t-SNE:** Reduces dimensionality, particularly useful for visualizing highdimensional data.
- **Apriori Algorithm**: Finds frequent itemset and association rules in transactional datasets. [36]

III. **Semi-supervised ML:** It is a type of machine learning that falls between supervised and unsupervised learning. It involves training a model using a combination of a small amount of labelled data and a large amount of unlabelled data. This approach leverages the abundance of unlabelled data, which is often cheaper and easier to obtain, while still making use of the labelled data to guide the learning process. These are used in the Detection, identification and recognition of spam mails, images, speech, etc. along with clustering these huge data into required categories.

- **Label Propagation**: Uses graph-based methods to spread labels from labelled to unlabelled data.
- **Hierarchical Clustering**: Builds a hierarchy of clusters using either a top-down (divisive) or bottom-up (agglomerative) approach.
- **DBSCAN (Density-Based Spatial Clustering of Applications with Noise)**: Groups points that are closely packed together, marking outliers as noise.
- **Semi-Supervised Support Vector Machines (S3VM)**: Extends SVMs to handle unlabelled data.
- **Principal Component Analysis (PCA)**: Transforms data into a set of linearly uncorrelated components by maximizing the variance.
- **Independent Component Analysis (ICA)**: Separates a multivariate signal into additive, independent non-Gaussian components. [38].

IV. **Reinforcement learning ML:**It is a type of machine learning where it learns to make decisions by performing certain actions within an environment to maximize some notion of cumulative reward. Unlike supervised learning, where the model learns from a dataset of labelled examples, reinforcement learning is based on the idea of learning from interactions with the environment.

- **Q-Learning**: Learns the value of state-action pairs, aiming to find the optimal policy by iteratively updating Q-values.
- **Deep Q-Networks (DQN)**: Combines Q-learning with deep networks to handle high-dimensional state spaces.
- **SARSA**: Similar to Q-learning but considers the action taken by the policy in the next state.
- **Proximal Policy Optimization (PPO)**: A policy gradient method that balances exploration and exploitation with stable updates.
- **Actor-Critic Methods**: Uses two models, an actor (policy) and a critic (value function), to improve learning efficiency. [36]

5.2. ML Applications

In the new era of technology, security is a most important domain where ML is used for facial recognition and iris scans are in high demand along with fingerprint authentication. ML based facial recognition technology is used to identify extremists in crowded places, ranging from visitors at airports to participants at mass gatherings, ceremonial events, and other high-security settings. In educational institutes ML is employed in automatic attendance systems within professional institutes, providing a more secure alternative to conventional methods such as keys and identity cards, which can be easily stolen. Handwriting recognition applications facilitate the processing of large volumes of handwritten documents, particularly in universities, exam centres, and police investigations where verifying fraudulent signatures and questioned documents is essential [37]. ML is also used in speech recognition, which translates spoken words into text and offers numerous benefits across various sectors. In healthcare, military, and automotive systems, it helps create voice interfaces and voice assistants, improving accessibility. Additionally, speech recognition supports language translation, easing communication barriers. Machine learning is widely applied across various domains, including robotics, virtual personal assistants, video games, pattern recognition, natural language processing, data mining, traffic prediction, transportation networks, product recommendations, stock market forecasts, medical diagnoses, fraud detection, agricultural advice, and search engine result refinement [38]. ML has proven instrumental in detecting various tumours and abnormalities and processing them for medical records in real-time applications. It also includes the statistical analysis of medical documentation, setting a high standard in the field. ML applications extend to pricing predictions,

scientific research, marketing campaigns, banking, and fraudulent transactions. Techniques logically with associated with distinct Ml algorithms implemented with TensorFlow and Keras, are used for credit card fraud detection, saving significant amount of money for cost recoveries and insurance in the financial sector[39].

6. A BRIEF REVIEW OF DNN

Kumar and his team conducted a comparative analysis of various Deep Learning techniques, including Long Short-Term Memory (LSTM), Bidirectional LSTM, Stacked LSTM, and Gated Recurrent Unit (GRU). They structured the unstructured dataset CICDDoS2019, provided in CSV format, and performed preprocessing by eliminating values such as NaN and infinity. Numerical values underwent standardization, while class values were encoded using label encoders. The pre-processed data was then fed into the aforementioned Deep Learning techniques, allocating 80% for training and 20% for evaluation from the CSV file. Among these techniques, Stacked LSTM emerged as the most effective, achieving a remarkable accuracy of 99.55% compared to others [16]. Asad and his team introduced a Deep Neural Network model employing a feed-forward backpropagation architecture, comprising seven layers to classify network flows and discern between attacks and normal traffic. The architecture includes three layers: input, hidden, and output. The input layer accommodates 66 features along with a bias factor, while the hidden layer initializes synaptic weights and connections to aid in classification computations. The output layer offers probabilities of benign traffic or a DDoS attack. They evaluated their model using CIDCIDS2017 dataset achieving 98% accuracy [17].

Assis introduced a defence system focused on analysing single IP flow records, employing the Gated Recurrent Units (GRU) deep learning method to identify DDoS and intrusion attacks. The model was evaluated against various machine learning approaches using the CICDDoS2019 and CICIDS2018 datasets. Additionally, a lightweight mitigation approach was proposed and assessed, with performance tests conducted on real IP flow data from a large-scale network. The results showcased promising detection rates, achieving an accuracy of 97.1%.[18]. Cil developed a DNN model with three hidden layers, each consisting of 50 neurons and utilizing sigmoid activation functions. This model was designed to detect DDoS attacks using the CICDDoS2019 dataset, achieving an impressive accuracy of 97.1%. a systematic review [19]. Christian Callegari proposed a deep learning-based approach for network attack detection utilizing Recurrent Neural Networks (RNN), Convolutional Neural Networks (CNN), Long Short-Term Memory (LSTM), and Gated Recurrent Units (GRU). This approach was tested using datasets of traffic traces collected from the MAWI Lab archive, achieving an accuracy of 89.99% [34]

Figure 5, further provides the summary of the researcher's study on detection related to DDoS attacks using DNN that is still in process and according to Cloudflare’s Q1 2024 report, Domain Name System (DNS) based DDoS attacks have become the most prominent attack-vector, with their share among all network-layer attacks continuing to grow. From the first quarter of 2024, it is clear that the share of DNS-based DDoS attacks increased by 80% year-over-year, reaching approximately 52%. Despite this surge, and due to the overall increase in all types of DDoS attacks, L3/4 attacks still account for 30% of the total. ICMP-related DDoS attacks occupy 1.5%, alongside other types of attacks such as TCP, UDP, and RST floods [20].

6.1. Types of DNN

Deep learning uses artificial neurons that mimic the human brain. A perceptron, or artificial neuron, receives inputs with assigned weights, computes a function, and provides an output. Figure 6 illustrates the basic structure of a Deep neural network. Inputs are summed, transformed

by an activation function, and produce an output, with input significance determined by weight. Adjusting the bias parameter fine-tunes the output for each perceptron. Activation functions, such as sigmoid, tanh, ReLU, and SoftMax, transform inputs into outputs. Multiple neurons are used together to process complex inputs and reach conclusions[37].

I. **Supervised DNN:** It is a powerful type in the realm of AI, capable of tackling complex tasks where a model learns to map input data to output labels through multiple layers of neural networks. This comes under supervised, because it relies on labelled datasets where the input data is paired with the correct output. They have become a cornerstone in fields ranging from computer vision to natural language processing due to their ability to extract and learn hierarchical labelled features from the data automatically[40].

Characteristics	Models used	Nature of learning	DL types	Dataset	Attacks detected	Ref.
Storing the non-attacked data in cloud to provide security and avoiding the entry of DDOS attacks	Feature Selection Based Whale Optimization DNN	Supervised	Discriminative	CICIDS2017	DoS Slowloris, DoS Slow HTTP Test, DoS Hulk and DoS Golden Eye, DDoS LOIC	Agarwal, A., Khari, M., Singh, R. Detection of DDOS Attack using Deep Learning Model in Cloud Storage Application. Wireless Personal Communications, 2021, 1-21. https://doi.org/10.1007/s11277-021-08271-z
Reduction in execution time and saving of processing power	Deep Neural Network (DNN) based on Improved Genetic Algorithm (IGA) and Simulated Annealing	Supervised	Discriminative	CICIDS2017, NSL-KDD version 2015 and CIDDS-001.	DoS Slowloris, DoS Slow HTTP Test, DoS Hulk and DoS Golden Eye, HTTP DoS, DDoS attack using UDP, TCP, or HTTP requests	Chiba, Z., Abghour, N., Moussaid, K., Rida, M. Intelligent Approach to Build a Deep Neural Network based IDS for Cloud Environment using Combination of Machine Learning Algorithms. Computers and Security, 2019, 86, 291-317. https://doi.org/10.1016/j.cose.2019.06.013
Reduced feature engineering process and processing time. Suitable in resource constraint environment.	CNN	Supervised	Discriminative	ISCX2012, CIC2017 and CSECIC2018	DoS slowloris, DoS Slow http test, DoS Hulk, DoS Golden Eye, BFSSH ,Http DoS, DDoS(TCP, ICMP)	Doriguzzi -Corin, R., Millar, S., Scott-Hayward, S., Martinez-del-Rincon, J., Siracusa, D. LUCID: A Practical, Lightweight Deep Learning Solution for DDoS Attack Detection. IEEE Transactions on Network and Service Management. 2020, 17(2), 876-889. https://doi.org/10.1109/TNSM.2020.2971776
Highest evaluation metrics in terms of recall, precision, F-score, and accuracy. Reduce the data dimensionality by automatically extracting the features from input data	RNN with Autoencoder	Unsupervised	Generative	CICDDoS2019	SYN flood attacks, MSSQL attacks, UDP-Lag, LDAP attacks, UDP flood attacks, Port Scan, and NetBIOS attacks, Web DDoS attacks, SSDP DDoS	Elsayed, M. S., Le-Khac, N. A., Dev, S., Jurcut, A. D. DDoSNET: A Deep-learning Model for Detecting Network Attacks. Proceedings of IEEE 21st International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM), Cork, Ireland, August 31 - September 03, 2020, 391-396. arXiv:2006.13981.
Comparative analysis of deep learning techniques for DoS/DDoS attacks detection	DNN, CNN, RNN, RBM, DBN, DBM, DA	Supervised & unsupervised	Discriminative & Generative	CIC IDS 2018	Slowloris DoS Slow http test, DoS Hulk, DoS Golden Eye, DDoS LOIC-UDP, DDoS LOIC-HTTP	Ferrag, M. A., Maglaras, L., Janicke, H., Smith, R. Deep Learning Techniques for Cyber Security Intrusion Detection: A Detailed Analysis. Proceedings of 6th International Symposium for ICS & SCADA Cyber Security Research 2019 (ICS-CSR), Athens, Greece, September 10-12, 2019, 126-136. https://doi.org/10.14236/ewic/icscsr19.16
Hyper-parameter tuning using Bayesian Optimization to reduce search space and choose optimal values for hyperparameters	Ensemble models and AE based deep learning classifiers	Unsupervised	Generative and Discriminative	Digiturk and Labris	SYN ACK DDoS, ICMP DDoS, FIN DDoS, HTTP_GET flooding,	Gormez, Y., Aydin, Z., Karademir, R., Gungor, V. C. A Deep Learning Approach with Bayesian Optimization and Ensemble Classifiers for Detecting Denial of Service Attacks. International Journal of Communication Systems, 2020, 33(11), e4401. https://doi.org/10.1002/dac.4401
Hyper-parameters tuning for designing an optimal model	CNN	Supervised	Discriminative	KDD CUP 99 and CSE-CIC-IDS 2018	DoS-Hulk, DoS Slow HTTP Test, DoS-Golden Eye, DDoS-LOIC-HTTP DDoS-HOIC, Neptune Attack, Smurf Attack	Kim, J., Kim, J., Kim, H., Shim, M., Choi, E. CNN-Based Network Intrusion Detection against Denial-of-Service Attacks. Electronics. 2020, 9(6), 916. https://doi.org/10.3390/electronics9060916
Trained, deployed, and tested the solution in a physical environment. Reduce the strength of the attack before it reaches the victim	ANN	Supervised	Discriminative	simulated using Java Neural Network Simulator (JNNS)	NL/TL DoS (TCP, UDP and ICMP DDoS attacks)	Saied, A., Overill, R. E., Radzik, T. Detection of Known and Unknown DDoS Attacks using Artificial Neural Networks. Neurocomputing, 2016, 172, 385-393. https://doi.org/10.1016/j.neucom.2015.04.101
Ability to learn the spatial and temporal features of a long sequence of data.	HAST-IDS includes CNN (to learn low level spatial features) and LSTM (to learn high level temporal features)	Supervised	Discriminative	DARPA1998 and ISCX2012	BFSSH, Http DoS, DDoS(TCP, ICMP)	Wang, W., Sheng, Y., Wang, J., Zeng, X., Ye, X., Huang, Y., Zhu, M. HAST-IDS: Learning Hierarchical Spatial-Temporal Features using Deep Neural Networks to Improve Intrusion Detection. IEEE Access, 2017, 6, 1792-1806. https://doi.org/10.1109/ACCESS.2017.2780250
Ability to address class imbalance problem.	SGM-CNN (SGM-combination of Synthetic Minority Over-Sampling Technique (SMOTE) and under-sampling for clustering based on Gaussian, Mixture Model (GMM))	Supervised	Discriminative	UNSW-NB15 and CICIDS2017	DoS-Hulk, DoS Slow HTTP Test, DoS-Golden Eye, DoS-Slowloris, DDoS-LOIC-HTTP DDoS-HOIC, Bot Net attacks, general DoS attacks (UDP,TCP)	Zhang, H., Huang, L., Wu, C. Q., Li, Z. An Effective Convolutional Neural Network based on SMOTE and Gaussian Mixture Model for Intrusion Detection in Imbalanced Dataset. Computer Networks, 2020, 177, 107315. https://doi.org/10.1016/j.comnet.2020.107315

Fig.5. DNN summary Table [25]

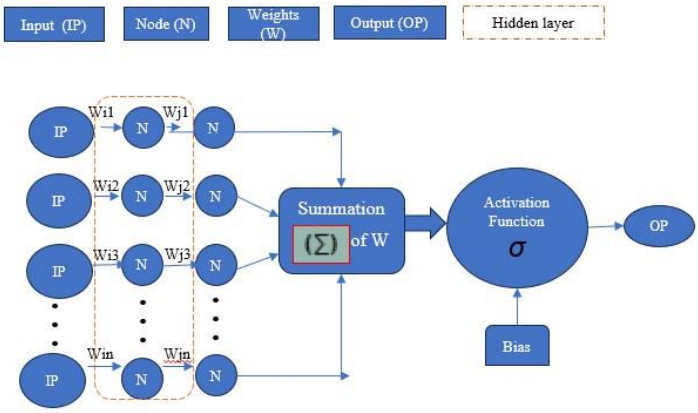

Fig.6. DNN Basic Functionality Neural Network structure

- **Deep Feedforward Networks**: Extend MLPs with more layers to capture complex patterns in the data.
- **Multi-Layer Perceptron (MLPs)**: The simplest type of DNN, consisting of fully connected layers where each neuron is connected to every neuron in the next layer.
- **LeNet**: One of the earliest Convolutional Neural Networks **(**CNN) architectures, designed for digit recognition.
- **AlexNet**: A deeper CNN that won the ImageNet competition in 2012, sparking widespread interest in deep learning.
- **VGGNet**: Known for its simplicity and use of very deep networks with small convolutional filters.
- **ResNet**: Introduces residual connections to allow training of extremely deep networks.
- **Inception (GoogLeNet)**: Uses a combination of convolutions with different filter sizes to capture diverse features.
- **MobileNet**: Optimized for mobile and embedded vision applications by using depthwise separable convolutions.
- **Vanilla Recurrent Neural Networks (RNNs)**: Used for sequential data, with connections forming cycles to capture temporal dependencies.
- **Long Short-Term Memory (LSTM)**: Addresses the vanishing gradient problem in RNNs, suitable for long-term dependencies.
- **Gated Recurrent Unit (GRU)**: A simpler alternative to LSTMs, also effective for capturing long-term dependencies.
- **Bidirectional RNNs**: Processes sequences in both forward and backward directions for better context understanding.
- **Attention Mechanisms**: Allows the model to focus on relevant parts of the input sequence.
- **Transformers**: Uses self-attention mechanisms to handle sequential data without relying on recurrence, leading to models like BERT and GPT.
- **Graph Convolutional Networks (GCNs)**: Extends convolutions to graph-structured data. [40]

II. Unsupervised DNN: It isdesigned to learn patterns and representations from data without explicit labels. Techniques of generative networks, dimensionality reduction and clustering are frequently counted within this category.

- **Autoencoder:** It is a neural network that learns to encode the input data into a compressed representation and then decode it back to the original data.
- **Basic Autoencoders**: Consists of an encoder and a decoder with a bottleneck layer in between.

- **Denoising Autoencoders (DAEs)**: Trained to reconstruct clean input from a corrupted version, enhancing robustness.
- **Sparse Autoencoders**: Use sparsity constraints on the hidden layers to learn more meaningful representations.
- **Variational Autoencoders (VAEs)**: Learn probabilistic latent representations, allowing for generating new data samples.
- **Generative Adversarial Networks (GANs):** It consists of two neural networks, a generator and a discriminator, that compete with each other.
- **Basic GANs**: The generator creates fake data samples, while the discriminator distinguishes between real and fake samples.
- **Deep Convolutional GANs (DCGAN)**: Use convolutional layers to generate highquality images.
- **Conditional GANs (cGANs)**: Generate data conditioned on specific inputs or classes.
- **Basic Self-Organizing Maps (SOMs)**: Organize data into a grid where similar data points are closer together.
- **Hierarchical SOMs**: Stack multiple SOM layers to capture more complex patterns.
- **Basic Restricted Boltzmann Machines (RBMs)**: Consists of visible and hidden layers with undirected connections.
- **Deep Belief Networks (DBNs)**: Stack multiple RBMs to form deep networks for more complex data representations.
- **Deep Embedded Clustering (DEC)**: Learns feature representations and cluster assignments simultaneously.
- **Deep Clustering Networks (DCNs)**: Integrate deep neural networks with traditional clustering methods like k-means. [37]

III. Semi-Supervised DNN: It leverages both labelled and unlabelled data to improve learning performance, especially when labelled data is scarce. Here are key types and techniques used in semi-supervised DNNs

- **Improved Generative Adversarial Networks (IGAN):** The discriminator not only distinguishes between real and fake samples but also classifies real samples into their respective categories.
- **Mean Teacher**: Involves a teacher model (an exponential moving average of the student model) providing stable targets for the student model.
- **Virtual Adversarial Training (VAT)**: Regularizes the model to be robust to adversarial perturbations of the input.
- **Iterative Pseudo-Labelling**: Continuously updates the pseudo-labels as the model improves during training.
- **Self-Training with Confidence Thresholding**: Only uses pseudo-labels for samples where the model's prediction confidence exceeds a certain threshold.
- **Label Propagation**: Labels are propagated through the graph based on data point similarities.
- **Graph Convolutional Networks (GCNs)**: Extend convolutions to graph-structured data, useful for leveraging relationships between labelled and unlabelled data. [42]

V. Reinforcement DNN: It integrates deep learning with reinforcement learning (RL) to enable agents to learn complex behaviours and decision-making policies from high dimensional sensory inputs. Here are the key types and techniques used in reinforcement DNNs

- **Basic Deep Q-Networks (DQNs)**: Uses a deep neural network to approximate the Qvalue function, which represents the expected reward of taking an action in a given state. Stores agent’s experiences and samples them randomly to break correlations and stabilize

training. Uses a separate network for generating target Q-values to stabilize training by reducing the risk of oscillations or divergence.

- **Double DQN (DDQN)**: Addresses the overestimation bias in DQNs by decoupling the selection of the best action from the evaluation of that action. It uses the main network to select actions and the target network to evaluate them.
- **Dueling DQN Network Architecture**: Separates the estimation of state value and advantage functions to provide more stable value function estimates.
- **Reinforce:** A straightforward policy gradient method that updates the policy directly in the direction that maximizes expected rewards.
- **Actor-Critic Methods**: Combines value function estimation (critic) with policy optimization (actor) to improve learning efficiency and stability.
- **Asynchronous Advantage Actor-Critic (A3C)**: Uses multiple workers to asynchronously update a global network, improving training speed and exploration.
- **Proximal Policy Optimization (PPO)**: Uses a surrogate objective with clipped probability ratios to ensure more stable updates.
- **Trust Region Policy Optimization (TRPO):** Constrains policy updates to a trust region to ensure stable and reliable policy improvement, avoiding large updates that could destabilize learning. [43]

6.2. Applications of DNN

Well-known companies such as Microsoft, Google, and Facebook handle vast amounts of Big Data and employ deep neural networks (DNNs) like ChatGPT for natural language processing (NLP) and large language models (LLMs) for speech, voice, and text recognition. These companies also process massive image datasets using convolutional neural networks (CNNs) techniques such as LeNet, AlexNet, VGGNet, ResNet, Inception (GoogLeNet), and MobileNet. For graph-oriented tasks, Graph Convolutional Networks (GCNs) and Graph Attention Networks (GATs) are utilized[35]. In the medical domain, U-Net is used for image segmentation, Mask R-CNN for instance segmentation, and YOLO for object detection. Companies like Uber collaborate with AI labs to develop AIdriven vehicle technologies[39]. According to Forbes, the Auto industry developing systems for smart autonomous driving using reinforcement DNNs to assist in navigation without maps[40].

These DNNs are also applied in IoT and mobile devices, implementing efficient and reliable deep architectures to analyse noisy and complex sensor data while conserving device resources. A low-power deep neural network inference engine has been suggested, which uses both the central processing unit (CPU) and the digital signal processor (DSP) of mobile devices without significantly overloading the hardware[41]. In network and cybersecurity, CNN-related techniques, reinforcement techniques, or hybrid models are deployed to detect various network attacks. This often involves applying dimensionality reduction for feature selection to enhance processing time and using ensemble techniques to improve model performance and achieve superior scores[42]

Figure 7 illustrates the Cloudflare statistics on DDoS attacks that exist and are one of the deadliest attacks where the IT industry is still suffering. The DDoS attacks in the current IT industry provide a good understanding that the ICMP DDoS attacks are very high when compared to other attacks.

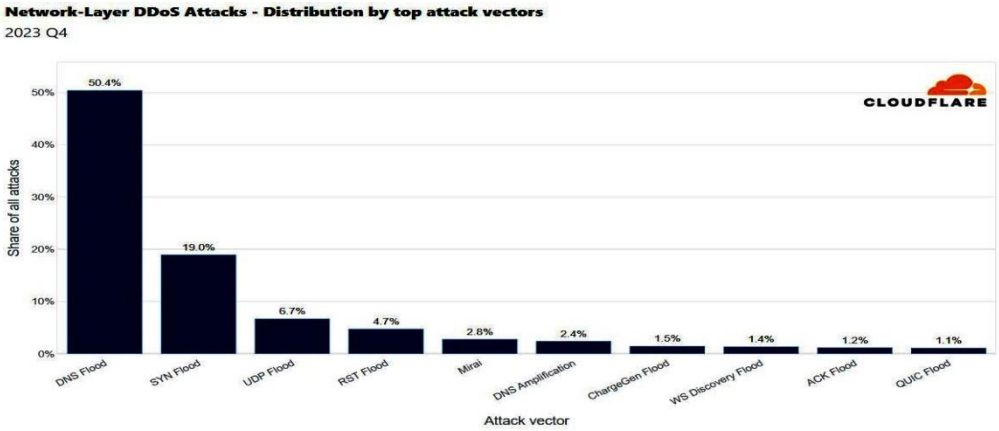

Fig.7. DDOS attacks in 2024 Q1 [20]

Dao introduced Multi-access Edge Computing (MAEC-X) technologies as a potent defence against DDoS attacks, particularly within 5G networks. MAEC-X operates as a hybrid solution, strategically positioned at the edge of the network to intercept and neutralize DDoS threats before they reach their targets. By leveraging MAEC computation, sophisticated DDoS prevention strategies can be localized, enhancing their efficacy in countering malicious traffic. In essence, MAEC-X harnesses the combined processing power of edge nodes at both the source and destination ends, creating a multi-tiered defence system that filters and prevents volumetric DDoS attacks effectively [21]. Li introduced a novel detection approach tailored for the joint entropy calculation, unveiling the Quintile Deviation Check (QuinDC) algorithm. QuinDC facilitates RTVD, an acronym for RealTime Volumetric Detection, specifically engineered for combatting DDoS threats within the Internet of Things (IoT). This pioneering mechanism promises a real-time, highefficiency framework for promptly identifying volumetric DDoS assaults in IoT environments. It achieves this through the strategic utilization of a sliding time window, a single directional filter, and the QuinDC algorithm, meticulously designed to enhance detection outcomes [22]. Mohammad Tayyab reviewed DoS and DDoS attack detection in ICMPv6 using ML techniques, discussing single classifiers (e.g., SVM, KNN, Decision Trees, NB) and hybrid classifiers. They detailed how classifiers, trained on DARPA 1999 and generic datasets, achieved detection rates of 94.47% and 96.55%, respectively. Open challenges related to performance, scalability, efficiency, benchmarks, imbalance, and evaluation metrics were addressed. Additionally, Blockchain applicability for detecting ICMPv6 DDoS attacks was proposed as a new research direction [26]. Hwang and colleagues proposed an unsupervised deep learning model using CNNs for early network traffic anomaly detection. This model automatically profiles traffic features from raw patterns, focusing on the first few packets to learn and determine non-linear relationships, achieving partial end-to-end learning. Trained on raw data, it builds a classifier to differentiate benign traffic and detect anomalies accurately. Using the 277.1 GB Miraibased DDoS dataset from Robert Gordon University, their evaluation with PyTorch and TensorFlow achieved nearly 100% accuracy, with less than 1% false alarms and false negatives, using just two packets and 80 bytes from each packet [27].

Ahmed Issa introduced an innovative deep-learning classification approach by combining two widely used algorithms, CNN and LSTM. The model was designed with a 7-layer deep neural network consisting of a 1D CNN layer with kernel and stride parameters, followed by a MaxPooling 1D layer, using ReLU as the activation function, and Softmax for the output layers. This model was evaluated using the NSL-KDD dataset, which comprises 40 features and includes various types of attacks. The model achieved an impressive accuracy rate of 99.20% (Issa and Albayrak, 2023) [28]. Omar Elejla introduced an innovative method for identifying ICMPv6

flooding DDoS attacks in IPv6 networks. This approach leverages deep learning and incorporates an ensemble feature selection technique, utilizing chi-square and information gain ratio methods to identify crucial features for accurate attack detection. The model employs an LSTM network trained on the selected features, resulting in impressive detection accuracy rates: 87.1% for an RNN, 99.4% for LSTM, and 99.11% for a GRU [29]. Hasan provided good insight into ML and DL techniques focusing on ICMPv6 DDoS attacks and their usage to detect and mitigate. He also provides the differences between both and a review of the adaption of ML and DL techniques in AIDS for detecting IPv4 and IPv6 attacks, such as DoS and DDoS flooding attacks [30]. Our study and exploration led us to researchers who have delved into DDoS attacks across multiple protocols including ICMP, TCP, and UDP using ML and DNN. Subsequently, our investigation zeroed in on ICMP DDoS attacks prevalent in diverse domains such as IoT, vehicular, enterprise networks, SDN, etc. Similar research related to both DNN and ML was summarised in Figure 8.

Name of the Paper	Method Used	Types of DDOS Attacks detected	Data set used	Ref. No.
The impact and mitigation of ICMP based economic denial of sustainability attack in cloud computing environment using software defined network	Traditional rule based	ICMP DDoS flood attacks	Data sets generated using HPING3 tool	Shah, S.Q.A., Khan, F.Z. and Ahmad, M., 2021. The impact and mitigation of ICMP based economic denial of sustainability attack in cloud computing environment using software defined network. Computer Networks, 187, p.107825.
Attack detection analysis in software-defined networks using various machine learning method	KNN, SVM, XGB,ANN	ICMP,TCP,UDP	Generated in SDN environment	Wang, Y., Wang, X., Ariffin, M.M., Abolfathi, M., Alghatani, A. and Almutairi, L., 2023. Attack detection analysis in software-defined networks using various machine learning method. Computers and Electrical Engineering, 108, p.108655.
Modified Flower Pollination Algorithm (MFPA) for ICMPv6-Based DDoS Attacks Anomaly Detection	MFPA	ICMPv6	Generated	Alghuraibawi, A.H.B., Manickam, S., Abdullah, R., Alyasseri, Z.A.A., Jasim, H.M. and Sani, N.S., 2023. Modified Flower Pollination Algorithm for ICMPv6-Based DDoS Attacks Anomaly Detection. Procedia Computer Science, 220, pp.776-781.
DADCNF: Diagnoser design for Duplicate Address Detection threat using Conjunctive Normal Form	Conjunctive Normal Form-based Discrete Event System diagnose (CNF based DES)	ICMPv6	Generated	Seth, A.D., Biswas, S. and Dhar, A.K., 2023. DADCNF: Diagnoser design for duplicate address detection threat using conjunctive Normal form. Computer Networks, 222, p.109539.
A comprehensive study of DDoS attack detecting algorithm using GRU-BWFA classifier	Gated Recurrent Uni -Bidirectional weighted feature averaging(GRU-BWFA)	TCP-SYN, UDP flood, ICMP-echo, HTTP flood, Slow Loris, Slow Post, a	SNMP-MIB dataset	Gangula, R., Mohan, V.M. and Kumar, R., 2022. A comprehence study of DDoS attack detecting algorithm using GRU-BWFA classifier. Measurement: Sensors, 24, p.100570.
An approach to on-stream DDoS blitz detection using machine learning algorithms	Naive Bayes, KNN and Random Forest	ICMP, TCP, or UDP	Data set generated using Loic attacking tool	Manjula, H.T. and Mangla, N., 2023. An approach to on-stream DDoS blitz detection using machine learning algorithms. Materials Today: Proceedings, 80, pp.3492-3499.
Zone-based stable and secure clustering technique for VANETs	K-means	ICMP , Roadside unit, (RSU)	Data sets generated using network simulator, NS2.35,	Sharma, S. and Awasthi, S.K., 2024. Zone-based stable and secure clustering technique for VANETs. Simulation Modelling Practice and Theory, 130, p.102863.
An Investigation into the Application of Deep Learning in the Detection and Mitigation of DDoS Attack on SDN Controllers. Technologies	LSTM and CNN	TCP, UDP, and ICMP flood attacks	Dataset generated using Mininet and Floodlight	Gadze, J.D., Bamfo-Asante, A.A., Agyemang, J.O., Nunoo-Mensah, H. and Opare, K.A.B., 2021. An Investigation into the application of deep learning in the detection and mitigation of DDOS attack on SDN controllers. Technologies, 9(1), p.
LUCID: A Practical, Lightweight Deep Learning Solution for DDoS Attack Detection	CNN	DoS slowloris, DoS Slow http test, DoS Hulk, DoS Golden Eye, BFSSH, Http DoS, DDoS(TCP, ICMP)	ISCX2012, CIC2017 and CSECIC2018	Doriguzzi-Corin, R., Millar, S., Scott-Hayward, S., Martinez-del-Rincon, J. and Siracusa, D., 2020. LUCID: A practical, lightweight deep learning solution for DDoS attack detection. IEEE Transactions on Network and Service Management, 17(2), pp.876-889.
A Deep Learning Approach with Bayesian Optimization and Ensemble Classifiers for Detecting Denial of Service	Ensemble models and AE based deep learning classifiers	SYN ACK DDoS, ICMP DDoS, FIN DDoS, HTTP_GET flooding,	Digiturk and Labris	Gormez, Y., Aydin, Z., Karademir, R. and Gungor, V.C., 2020. A deep learning approach with Bayesian optimization and ensemble classifiers for detecting denial of service attacks. International Journal of Communication Systems, 33(11), p.e4401.
A DDoS attack mitigation scheme in ISP networks using machine learning based on SDN	KNN, XGBoost	TCP-SYN and ICMP Flood	CAIDA 2007	Tuan, N.N., Hung, P.H., Nghia, N.D., Tho, N.V., Phan, T.V. and Thanh, N.H., 2020. A DDoS attack mitigation scheme in ISP networks using machine learning based on SDN. Electronics, 9(3), p.413.
Detecting DDoS Attacks in Software-Defined Networks Through Feature Selection Methods and Machine Learning Models	SVM, ANN, KNN, NB	TCP, ICMP, and UDP.	Self-Generated Simulated Data	Polat, H., Polat, O. and Cetin, A., 2020. Detecting DDoS attacks in software-defined networks through feature selection methods and machine learning models. Sustainability, 12(3), p.1035.
A Real Time Deep Learning Based Approach for Detecting Network Attacks	MLP, RNN, CNN, LSTM and GRU	HTTP, ICMP, TCP, UDP,...	MAWI Data sets (Measurement and Analysis on the WIDE Internet)	Callegari, C., Giordano, S. and Pagano, M., 2024. A Real Time Deep Learning based Approach for Detecting Network Attacks. Big Data Research, p.100446.
BotStop : Packet-based efficient and explainable IoT botnet detection using machine learning	BotStop classifier - XGB classifier	ICMP, TCP, UDP	Na-BaIoT data set,	Alani, M.M., 2022. BotStop: Packet-based efficient and explainable IoT botnet detection using machine learning. Computer Communications, 193, pp.53-62.
A deep learning based intelligent framework to mitigate DDoS attack in fog environment	LSTM	TCP, UDP and ICMP	Hogzilla Dataset	Priyadarshini, R. and Barik, R.K., 2022. A deep learning based intelligent framework to mitigate DDoS attack in fog environment. Journal of King Saud University-Computer and Information Sciences, 34(3), pp.825-831.

Fig.8. ICMP summary Table [24]

7. CONCLUSION

Based on the above discussion and data provided in the aforementioned study, ongoing research into Intrusion Detection Systems (IDS) targeting DDoS attacks is evident. ML and DNN have

revolutionized AI, with DNNs distinguished by their highlevel performance through advanced model engineering. They have the potential to transform various domains like Cybersecurity, Networking, Healthcare, Transportation, Logistics, Big Data, IoT, Communication, Automobile, Investigations, etc., and this transformation has already begun. While DNNs often outperform traditional ML, both technologies play significant roles, especially when combined. As data and computing power grow, the capabilities of ML and DNNs will expand further. Despite their vast potential, challenges and ethical considerations must not be overlooked. Ensuring these technologies are used responsibly and transparently is essential as they continue to evolve.

7.1. Critical Evaluation

Section 4 discussed the mechanisms used in traditional IDS and how easily a threat actor can evade them. Section 5 explored various ways to mitigate DDoS attacks using different machine learning (ML) techniques. Section 5.1 outlined various mechanisms for mitigating these attacks, with Figure 4 illustrating an example. Section 5.2 examined the application of ML across various domains, highlighting its advantages over traditional IDS. Section 6 delved into how researchers could innovatively deploy various deep neural network (DNN) techniques to mitigate these attacks. Figure 6 illustrates the basic functionality of DNNs, including input layers, weights in the connected neural network nodes, mathematical functions, hidden layers, and the activation function that finally delivers the output. Section 6.1 discussed the various techniques present in DNNs, while Section 6.2 highlighted the applications of DNNs and their superiority over ML techniques. This section also focused on ICMP DDoS attacks, and the different techniques deployed using ML, DNN, and combinations of both to mitigate these attacks.

7.2. Future Works

Despite current efforts to mitigate these attacks, statistics from Cloudflare reveal that DDoS attacks continue to pose a significant threat within the IT industry. This underscores a pressing need to explore additional procedures, methods, techniques, approaches, and innovative combinations resulting in hybrid models using these DNN and ML techniques to prevent DDoS attacks entirely or minimize their impact. Consequently, the aim is to examine existing techniques and provide a comprehensive review in the form of a research paper. This review will justify the selection of techniques and approaches and identify novel methods that demonstrate effectiveness in combating DDoS attacks, and similar cyberattacks, for budding researchers.

REFERENCES

[1] Mishra, N. and Pandya, S., 2021. Internet of things applications, security challenges, attacks, intrusion detection, and future visions: A systematic review. IEEE Access, 9, pp.59353-59377

[2] Yang, Z., Liu, X., Li, T., Wu, D., Wang, J., Zhao, Y. and Han, H., 2022. A systematic literature view of methods and datasets for anomaly-based network intrusion detection. Computers & Security, 116, p.102675.

[3] Holkoviˇc, Martin., Ryˇsavy´, O. and Dudek, J., 2019, September. Automating network security analysis at packet-level by using a rule-based engine. In Proceedings of the 6th Conference on the Engineering of Computer Based Systems (pp. 1-8).

[4] Saad, R.M., Anbar, M. and Manickam, S., 2018. Rule-based detection technique for ICMPv6 anomalous behaviour. Neural Computing and Applications, 30, pp.3815-3824.

[5] Wang, N., Chen, Y., Xiao, Y., Hu, Y., Lou, W. and Hou, Y.T., 2022. Manda: On adversarial example detection for network intrusion detection system. IEEE Transactions on Dependable and Secure Computing, 20(2), pp.1139-1153.

[6] Tandon, Rajat., Charnsethikul, P., Kallitsis, M. and Mirkovic, J., 2022, December. AMONSENSS: Scalable and Accurate Detection of Volumetric DDoS Attacks at ISPs. In GLOBECOM 2022-2022 IEEE Global Communications Conference (pp. 3399-3404). IEEE.

[7] Tajdini, M., 2018. Developing an advanced IPv6 evasion attack detection framework. Liverpool John Moores University (United Kingdom).

[8] Kaur, P., Kumar, M. and Bhandari, A., 2017. A review of detection approaches for distributed denial of service attacks. Systems Science & Control Engineering, 5(1), pp.301-320.

[9] Aamir, M. and Zaidi, M.A., 2014. Ddos attack and defense: Review of some traditional and current techniques. arXiv preprint arXiv:1401.6317.

[10] Khamruddin, M. and Rupa, C., 2012, December. A rule based DDoS detection and mitigation technique. In 2012 Nirma University International Conference on Engineering (NUiCONE) (pp. 1-5). IEEE.

[11] Bdair, A.H., Abdullah, R., Manickam, S. and Al-Ani, A.K., 2020. Brief of intrusion detection systems in detecting ICMPv6 attacks. In Computational Science and Technology: 6th ICCST 2019, Kota Kinabalu, Malaysia, 29-30 August 2019 (pp. 199-213). Springer Singapore.

[12] Bahashwan, A.A., Anbar, M. and Hanshi, S.M., 2020. Overview of IPv6 based DDoS and DoS attacks detection mechanisms. In Advances in Cyber Security: First International Conference, ACeS 2019, Penang, Malaysia, July 30–August 1, 2019, Revised Selected Papers 1 (pp. 153167). Springer Singapore.

[13] Wu, Z., Cui, W. and Gao, P., 2021, May. Filtration method of DDoS attacks based on time frequency analysis. In 2021 7th IEEE Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing,(HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS) (pp. 75-80). IEEE.

[14] Ojugo, A. and Eboka, A.O., 2020. An Empirical Evaluation On Comparative Machine Learning Techniques For Detection of The Distributed Denial of Service (DDoS) Attacks. Journal of Applied Science, Engineering, Technology, and Education, 2(1), pp.18-27.

[15] Liang, X. and Znati, T., 2019, February. An empirical study of intelligent approaches to DDoS detection in large scale networks. In 2019 International Conference on Computing, Networking and Communications (ICNC) (pp. 821-827). IEEE.

[16] Kumar, K. and Behal, S., 2021, March. Distributed denial of service attack detection using deep learning approaches. In 2021 8th International Conference on Computing for Sustainable Global Development (INDIACom) (pp. 491-495). IEEE.

[17] Asad, M., Asim, M., Javed, T., Beg, M.O., Mujtaba, H. and Abbas, S., 2020. Deep detect: detection of distributed denial of service attacks using deep learning. The Computer Journal, 63(7), pp.983-994.

[18] Assis, M.V., Carvalho, L.F., Lloret, J. and Proenc¸a Jr, M.L., 2021. A GRU deep learning system against attacks in software-defined networks. Journal of Network and Computer Applications, 177, p.102942.

[19] Cil, A.E., Yildiz, K. and Buldu, A., 2021. Detection of DDoS attacks with feed forward-based deep neural network model. Expert Systems with Applications, 169, p.114520.

[20] Cloudflare, 2024. DDoS Attack Trends for 2024 Q1 https://radar.cloudflare.com/reports/ddos2024-q1

[21] Dao, N.N., Vu, D.N., Lee, Y., Park, M. and Cho, S., 2018, January. MAEC-X: DDoS prevention leveraging multi-access edge computing. In 2018 International Conference on Information Networking (ICOIN) (pp. 245-248). IEEE.

[22] Li, J., Liu, M., Xue, Z., Fan, X. and He, X., 2020. RTVD: A real-time volumetric detection scheme for DDoS in the Internet of Things. IEEE Access, 8, pp.36191-36201.

[23] Ahmed, M.R., Shatabda, S., Islam, A.M. and Robin, M.T.I., 2023. Intrusion Detection System in Software-Defined Networks Using Machine Learning and Deep Learning Techniques–A Comprehensive Survey. Authorea Preprints.

[24] Malliga, S., Nandhini, P.S. and Kogilavani, S.V., 2022. A comprehensive review of deep learning techniques for the detection of (distributed) denial of service attacks. Information Technology and Control, 51(1), pp.180-215.

[25] Mittal, M., Kumar, K. and Behal, S., 2023. Deep learning approaches for detecting DDoS attacks: A systematic review. Soft computing, 27(18), pp.13039-13075.

[26] Tayyab, M., Belaton, B. and Anbar, M., 2020. ICMPv6-based DoS and DDoS attacks detection using machine learning techniques, open challenges, and blockchain applicability: A review. IEEE Access, 8, pp.170529-170547.

[27] Hwang, R.H., Peng, M.C., Huang, C.W., Lin, P.C. and Nguyen, V.L., 2020. An unsupervised deep learning model for early network traffic anomaly detection. IEEE Access, 8, pp.3038730399.

[28] Issa, A.S.A. and Albayrak, Z., 2023. DDoS attack intrusion detection system based on hybridization of cnn and lstm. Acta PolytechnicaHungarica, 20(2), pp.1-19.

[29] Elejla, O.E., Belaton, B., Anbar, M., Alabsi, B. and Al-Ani, A.K., 2019. Comparison of classification algorithms on ICMPv6-based DDoS attack detection. In Computational Science and Technology: 5th ICCST 2018, Kota Kinabalu, Malaysia, 29-30 August 2018 (pp. 347-357). Springer Singapore.

[30] Hasan Kabla, A.H., Anbar, M., Hamouda, S., Bahashwan, A.A., Al-Amiedy, T.A., Hasbullah, I.H. and Faisal, S., 2023. Machine and deep learning techniques for detecting internet protocol version six attacks: a review. International Journal of Electrical & Computer Engineering (2088-8708), 13(5).

[31] Alharbi, Y., Alferaidi, A., Yadav, K., Dhiman, G. and Kautish, S., 2021. Denial-of-Service Attack Detection over IPv6 Network Based on KNN Algorithm. Wireless Communications and Mobile Computing, 2021(1), p.8000869.

[32] Zewdie, T.G. and Girma, A., 2022, February. An evaluation framework for machine learning methods in the detection of DoS and DDoS intrusion. In 2022 International Conference on artificial intelligence in Information and communication (ICAIIC) (pp. 115-121). IEEE.

[33] Manjula, H.T. and Mangla, N., 2023. An approach to on-stream DDoS blitz detection using machine learning algorithms. Materials Today: Proceedings, 80, pp.3492-3499.

[34] Callegari, C., Giordano, S. and Pagano, M., 2024. A Real Time Deep Learning based Approach for Detecting Network Attacks. Big Data Research, p.100446.

[35] Sharma, N., Sharma, R. and Jindal, N., 2021. Machine learning and deep learning applicationsa vision. Global Transitions Proceedings, 2(1), pp.24-28.

[36] Hassanien, A.E.; Chang, K.C.; Mincong, T. (Eds.) Advanced Machine Learning Technologies and Applications; Springer Nature: Singapore, 2021; Volume 1141.

[37] Taye, M.M., 2023. Understanding of machine learning with deep learning: architectures, workflow, applications and future directions. Computers, 12(5), p.91.

[38] Du, K.-L.; Swamy, M.N.S. Support Vector Machines. In Neural Networks and Statistical Learning; Springer: Berlin/Heidelberg, Germany, 2019; pp. 593–644.

[39] Chakraborty, C., Bhattacharya, M., Pal, S. and Lee, S.S., 2023. From machine learning to deep learning: An advances of the recent data-driven paradigm shift in medicine and healthcare. Current Research in Biotechnology, p.100164.

[40] Srinivas, T., Aditya Sai, G. and Mahalaxmi, R., 2022. A comprehensive survey of techniques, applications, and challenges in deep learning: A revolution in machine learning. International Journal of Mechanical Engineering, 7(5), pp.286-296.

[41] Kim, D., Choi, J., Ahn, S. and Park, E., 2023. A smart home dental care system: integration of deep learning, image sensors, and mobile controller. Journal of Ambient Intelligence and Humanized Computing, pp.1-9.

[42] Al-Fawa'reh, M., Al-Fayoumi, M., Nashwan, S. and Fraihat, S., 2022. Cyber threat intelligence using the PCA-DNN model to detect abnormal network behavior. Egyptian Informatics Journal, 23(2), pp.173-185.

[43] Sarker, I.H., 2021. Deep cybersecurity: a comprehensive overview from neural network and deep learning perspective. SN Computer Science, 2(3), p.154.

AUTHORS

Mr. Om Salamkayala: I am a qualified M.Sc in Forensics Computing and also a PgCHPE fellow. Currently pursuing final year PhD from Staffordshire University. I gained over 8 years of IT experience out of 6 years in the core industry related to Digital Forensics. I am also currently working as a Part-Time Lecturer at Staffordshire University.

Dr. Saeed: works with Staffordshire University as a Lecturer. He did his Ph.D in Robotics and Intelligent Systems from Kobe University. He started his career with leadership roles like chairing the Amirkabir Robotic Center and collaborating with international researchers from Japan, France, Australia, and the USA. Teaching was also integral to his professional journey, with experience in designing graduate and undergraduate courses spanning Machine Learning, Robotics, and Computer Architecture. His contributions to the academic community are evident through numerous publications in esteemed journals and conferences, showcasing expertise in AI, robotics, and related domains.

Mr. Howard: has 30+ years of professional experience in networking, both technical and academic and is a Chartered Electronics Engineer. He works with Staffordshire University in a course director capacity and with his leadership abilities involved in the design and development of course curricula development at various levels. His main teaching interests are in Cyber and Networks at both undergraduate and postgraduate levels. His expertise extends to international partner relations, quality assurance, and staff development across Greece, China, and Vietnam. Additionally, he pioneered flexible learning awards for part-time students, focusing on Cisco qualifications like CCNA, CCNP, and CCNA Security, and active member of the University's Cisco Academy.