REVIEW ARTICLE UHD JOURNAL OF SCIENCE AND TECHNOLOGY

Innovative Machine Learning Strategies for DDoS Detection: A Review

Omar Mohammed Amin Ali[1], Rebin Abdulkareem Hamaamin[2], Barzan Jalal Youns[3], Shahab Wahhab Kareem[3]

[1]Department of IT, Chamchamal Technical Institute, Sulaimani Polytechnic University, KRG, Iraq.
[2]Computer Science, College of Sciences, Charmo University, Chamchamal, Sulaimani, KRG, Iraq.
[3]Department of Technical Information Systems Engineering, Technical Engineering College, Erbil Polytechnic University, KRG, Iraq.

ABSTRACT

This is a broad survey that investigates the use of machine learning (ML) methods for detecting distributed denial of service (DDoS) attacks. Traditional intrusion detection systems face difficulties in application-layer DDoS attacks because they target legal web traffic forms using standard transmission control protocol connections. This paper reviews different ML methods used in recent studies to tackle these issues. These studies use various data sets, such as UNSW-np-15, CICDDoS2019, and the novel dataset LATAM-DDoS-Internet of Things., which prove the efficacy of the proposed models in terms of accuracy and performance metrics. The second group of studies shows more advanced designs, such as protocol-based deep intrusion detection and autoencoder-multi-layer perceptron. These use deep learning to find features and group attacks. All of these approaches present favorable outcomes when it comes to distinguishing normal, DoS, and DDoS traffic with a high level of accuracy. Furthermore, the review discusses works that emphasize the early detection of noise-robust models and distributed frameworks. Different techniques, such as snake optimizer with ensemble learning, metastability theory, and spark-based anomaly detection, highlight the trend of predicting DDoS attacks, whereas hyperband-tuned deep neural networks and evolutionary support vector machine models show higher accuracy in cloud systems as well as software-defined networking environments. Hence, this review gives a general observation of how DDoS attacks develop on their way and proves that ML techniques help to strengthen network security.

Index Terms: Distributed Denial of Service Attacks, Machine Learning, Internet of Things, Deep Learning, Anomaly Detection

1. INTRODUCTION

Distributed denial of service (DDoS) attacks pose a significant threat in the current era of interdependent systems and digital dependencies, where cyber challenges are already numerous. It is understandable that nefarious actors remain resolute in exploiting network infrastructure vulnerabilities, necessitating the need for smarter and more adaptive defense mechanisms. This urgent need has fueled intensive research into DDoS attack detection using Machine learning (ML) methodologies, resulting in an active and rapidly evolving field of study teeming with innovative solutions. We aim to investigate the intricate web of studies dealing with ML and DDoS attack detection through this in-depth analysis. This review aims to give This review seeks to provide a comprehensive overview of cutting-edge methodologies, challenges, and advancements in this crucial field, utilizing 19 diverse references that each contribute to the overall discussion the literature review uses a wide range of DDoS

Access this article online

DOI: 10.21928/uhdjst.v8n2y2024.pp38-49 **E-ISSN:** 2521-4217 **P-ISSN:** 2521-4209

Corresponding author's e-mail: omar.mohammed@spu.edu.iq

Received: 28-07-2024 Accepted: 12-09-2024 Published: 02-10-2024

detection and ML algorithms, from classical classifiers, such as Gaussian Naive Bayes, which have been improved through iterative feature selection schemes, to current DMQ ML model the latter, which relies on quantum computing capabilities, significantly alters the dimensionality reduction and encoding paradigm to achieve an unparalleled level of efficiency in identifying DDoS attacks. Identifying the Recognizing the crucial role of software-defined networking (SDN) infrastructures, some references explore optimized models for DDoS detection in SDN environments. have achieved outstanding developments in accuracy and effectiveness by combining mininets, Ryu controllers, and one-dimensional-convolutional neural networks with innovative hyperparameter tuning techniques.

Besides traditional network systems, the review focuses on DDoS attack identification in emerging domains of 5G networks and the Internet of Things (IoT). Among notable techniques, the use of equilibrium optimization algorithms and ensemble learning tactics has emerged as an adaptable approach in response to continually changing cybersecurity challenges. A novel approach to studying the details of application-layer DDoS attacks presents a hybrid ML solution combining a Radial Basis Function neural network and a cuckoo search algorithm. This method has the potential to distinguish between legitimate and attack traffic, filling a significant loophole in current detection mechanisms. The review looks into DDoS attack prediction models that use the UNWS-np-15 dataset and the Random Forest and XGBoost classification algorithms. These models highlighted the power of ML in foreseeing and thwarting DDoS threats beforehand. When protocols-based deep intrusion detection architectures and hybrid approaches, such as autoencoder-multi-layer perceptron (AE-MLP) and evolutionary support vector machine (SVM) [1] models are used in software-defined networks, it makes things more complicated and flexible for using ML to better detect DDoS attacks. This review, after integrating these disparate views, aims to do more than summarize what is already known about the current body of knowledge; it will also reveal potential paths DDoS detection employing ML may take in the future. In doing so, it seeks to add its voice to the ongoing conversation about cybersecurity, which calls for a collaborative and dynamic approach toward mitigating an increasingly changing threat environment.

DDoS attacks form a significant threat in today's interconnected world and call for efficient and highly intelligent detection using ML. This review analyses a broad range of methods including basic classifiers all the methods up to modern quantum and various hybrid methods and discusses key advancements and future challenges in different types of networks, including SDN, 5G, and IoT. Its purpose is to present a literature review of the DDoS detection field's current state and possible further development.

2. LITERATURE REVIEW

DDoS attacks pose a major threat to network security in recent times. As a result, researchers have experimented with various methods, particularly ML approaches, to identify and neutralize these attacks. In this literature review, 19 of the most critical references are critically reviewed, providing a comprehensive analysis of how various methodologies can be used to detect DDoS attacks. Naiem *et al.* proposed a new framework that revives the Gaussian Naive Bayes classifier for DDoS attack detection in cloud computing environments during their research [2]. Their solution seems to be a thoughtfully designed combination of sequential feature selection and data preprocessing with specific targets, which greatly reduces the inadequacies observed by GNB. What distinguishes their approach is their tactical selection of attributes and highly independent characteristics, utilizing techniques such as PCC, MI, and Chi-square. They also handle data skews or sample zero frequencies effectively so that GNB would prove to be effective even under worst-case scenarios. Therefore, the study presents a potential solution to enhance the defense against DDoS in cloud computing destined for achieving consistency and availability of crucial services [2]. Analyzing the results, it is possible to observe the improvement of the identified GNB's accuracy and precision, which indicate the effectiveness of the system for the case of DDoS detection in the cloud environment.

Luo *et al.* authors created a novel model, DEQSVC, which leverages the dynamics of quantum computing to mitigate DDoS. DEQSVC tackles two key challenges: overloading of data and intricate patterns of an attack. First, DEQSVC eliminates a number of features and, therefore, minimizes the amount of data to be processed by the Quantum Support Vector Classifier. This not only leads to an increase in efficiency but also gives the true potential of the QSV in terms of identifying hidden patterns of attacks. 2) DEQSVC utilizes quantum encoding which encodes data in quantum states, and this would help QSV in recognizing even complicated attack patterns that are even impossible for quantum algorithms to determine. "It would be great to decipher digital hazards as easily as the protagonist of Superman with X-ray vision" [3]. The results are impressive. DEQSVC shows a notable increase in DDoS detection

accuracy compared to standard approaches. Its capacity to deal with both large and small attacks is why it's a useful tool in your cybersecurity armory [3].

Through an optimized AI mode, researchers Chen *et al.* offer hope to SDN environments plagued by DDoS attacks. This warrior is a hybrid of deep learning and SDN-specific features, reducing false positives and improving detection accuracy. Think about an alert AI protector monitoring the network traffic with its LSTM sniffing out irregularities like a bloodhound smelling something. The result is a DDoS-battling machine that operates your SDN with the efficiency of a well-oiled engine. Plunge into the "3 Optimized Artificial Intelligent Model for DDoS Detection in SDN Environment" PDF located in your ML folder and strengthen your network with this state-of-the-art protection [5].

In their work, Aljebreen *et al.* suggest using MEOADL-ADC as a precise method for distinguishing DDoS attacks in 5G networks. This method uses three strong techniques: important data points identified from the dataset using a method known as the Modified Equilibrium Optimization Algorithm (MEOA); deep learning with LSTM that can distinguish between attack patterns and normal traffic; and last but not least TSA used in hyperparameter optimization. With this integrated approach, MEOADL-ADC has a high accuracy of 97% by comparing with the data obtained from prototypes. 60%, which is above any of the existing state-of-the-art solutions and can present rather a good solution for network security for future generations of infrastructure networks [6].

Aljebreen *et al.* also have tackled the fact that IoT devices are becoming targeted by DDoS attacks in another work using the proposed technique of DDAD-SOEL. This method effectively applies the best aspect of Snake Optimizer in feature selection as well as strength on LSTM, DBN, and BiLSTM deep learning model through ensemble learning for achieving an enhanced attack detection result. Finally, the Adadelta optimizer further fine-tuned the hyperparameters of the model and hence the proposed DDAD SOEL has outperformed the other methods based on accuracy, precision, recall, and F1 score altogether in securing interconnected systems [7]. Sharif *et al.* address the growing problem of toolkits that facilitate DDoS attacks. His wonderful method combines a technique for selecting data features that speed up the process with an unusually detailed ML model, yielding notable results such as 99.9% accuracy, 96% precision, 98% recall, and a 97% F1 score. Diverse accessible toolkits efficiently detect network abuse, thereby providing a crucial defense against attacks [8].

Josue *et al.* His paper reveals a new dataset that addresses the vulnerability of IoT devices to denial of service (DoS) attacks. It shows how hackers can gain easy access and compromise these types of networks or services, thereby affecting the entire connection both at home and in businesses globally. IoT LATAM-DDoS combines real traffic attacks on physical devices with user data for normal users; it is also a critical ground for training robust anomaly detection systems. As it covers a vast field of different attack types and various physical devices, its gap in current resources is vital for researchers and developers to improve defense strategies, test existing ones out there, or even benchmark other approaches toward securing this rapidly developing world of connected things as shown in Figures 1 and 2 [4].

El Sayed *et al.* address DDoS threats through SDNs. He picks up important characteristics from network flows, chooses the most informative ones with Chi-square, and reuses KNN to identify normal traffic versus attack patterns. 21 As a result, this efficient and accurate solution, which boasts high detection rates with minimal false alarms, becomes an attractive method of securing the SDNs against the formation of newer DDoS malware.

Researchers Beitollani *et al.* tackle the challenge of application-layer DDoS attacks with a powerful one-two punch: Researchers Beitollani *et al.* use the Radial Basis Function (RBF) network to accurately identify attacks, and extend the Cuckoo Search Algorithm to optimize the RBF's network design. Let's assume we have a neural network with three layers. The traffic features enter this brain and undergo transformation by the neurons in these layers, resulting in either a normal output or an indication of an attack. The bright brood parasitism of cuckoo father birds motivates the CSA method, which optimizes the hidden layer's "decision-making machinery" (positioning and neuro width). In the end, it improves the accuracy of detecting DDoS attacks for a network equipped with an optimized RBF that requires fewer training sessions and less resource confit ensures resistance against a variety of attack patterns, making it a valuable tool for safeguarding the constantly expanding realm of online services [10].

Ismail *et al.* create a strong model that gains not only the ongoing DDoS attacks but forecasts them for an organization to prepare defensive measures early. The proposed multi-stage approach looks at network traffic traits, determines the most significant features, and uses ML models to correctly

classify attacks while anticipating future ones. The system's proactive protection, high accuracy, and adaptability make it a valuable asset in addressing DDoS hazards. Individuals can "instead imagine a flowchart where traffic features come in, are filtered by the process using these crucial indicators, and feed into intelligent models that not only trigger alarms for ongoing attacks but also start alarm bells when danger is approaching." Its comprehensive ML strategy creates a formidable barrier against persistent DDoS attacks [11]. Zeeshan *et al.* describe a new deep learning-based method called protocol-based deep intrusion detection (PBDiD) that can stop DoS and DDoS attacks in internal IoT networks. Their strategy uses an LSTM network to analyze network traffic, identifying suspicious anomalies that indicate attacks. Contrasting PB-DID with traditional ML techniques, the authors showcase its superb effectiveness in identifying DoS and DDoS attacks [12].

Wei *et al.* propose a new hybrid deep learning model, AE-MLP, in their paper that is capable of addressing and classifying different types of DDoS attacks successfully. AE-MLP is a combination of AE and MLP to contain the DDoS attack since they have the best characteristics for tackling them. The AE-MLP approach starts from dimensionality reduction of the data, elimination of noise, and identification of important DDoS patterns. Finally, MLP categorizes features following a compression process into the class of attacks. Dimensionality reduction, feature extraction and capacity to incapsulate noise make AE-MLP more effective than other methods. Using the statistics of the CIC-DDoS2019 dataset entails appropriateness to achieve corresponding F1-scores of 98% from 99%. 0.1–2% for detection only 2% for detection and classification [13].

Jingbo Zhang *et al.* propose to solve the problem of predicting the ACK flood attacks in WSN by using the Recursive Neural Network. The RNN temporal dependencies are adapted to control network traffic to employ pre-emptive measures that will prevent traffic congestion and service disruption. This method can be a good candidate for preventing various forms of network-based attacks on IoT systems because the method can be adjusted for different traffic conditions [14]. Maranhao *et al.* continue the research on the identification of DDoS attacks in noisy traffic flows. At the same time, posing an MLP immune to noise, the authors offer a solution capable of handling real-world network challenges. This peculiar MLP design, combined with, let's say it, proper data pre-processing and training, provides very good results. The model is highly accurate in detecting and distinguishing the DDoS attacks even when there is so much noise, and second, it is more superior to the other methods as far as this aspect is concerned. This is how it is possible to protect different network environments including enterprise centers, cloud offerings, or even IoT ecosystems that are vulnerable to DDoS attacks [15]. Ahmed *et al.* meet the urgent requirement of providing a DDoS solution in corporate networks at the moment of an attack. This SAD-F is derived from Apache Spark's real-time analytics speed where large network data streams take seconds to be analyzed and filtered for attributes that scream DDoS attack. In fact, the intelligent algorithm of the SAD-F which is statistical thresholding or ML depending on the type can identify dubious actions much better and more accurately. This entails quicker response and management of the DDoS threat reduction process necessary to safeguard an enterprise's networks from possible interruption. SAD-F is an extensible approach that can guarantee its effectiveness in enhancing different networks, including clouds or fragile IoT networks [16].

In the Bhardwaj study, the authors analyze the increasing problems of DDoS attacks on cloud platforms. For performing the analysis of massive amounts of data on the cloud network [17], the new method employs the proficiency of a suitably designed stacked sparse autoencoder (SSAE) incorporated with the hyperparameters. The SSAE works, such as a detective who sifts the data, extracts certain significant features, and emphasizes the trends that are typical of DDoS attacks. Hyperband tuning is like an army general who fine-tunes a team, especially the SSAE team to the best it can offer. They are combined in harmony, making them a dynamic duo that makes it possible to detect attacks at a very high success rate, especially in crowded traffic situations. This suggests that the cloud services contain a solid shield that protects them from interferences hence assuring them to deliver their services effectively [17]. Rahal also proposes an efficient and extensible distributed system for DDoS prediction, and in general, for botnet detection, that uses ML for the processing of the data coming from the analysis of the traffic of the networks [18]. These three man-oeuvres function as a single unit in giving high accuracy in identifying and forecasting invasions data manipulation, ML algorithms, and real-time surveillance. Since it is decentralized, it can easily cope with large data traffic and therefore can be used in large networks. The real-time monitoring system as informs of mitigation actions that need to be undertaken in realtime. The presented architecture is rather promising for networks' protection in different environments, such as enterprise networks, cloud solutions, and the IoT context. This distributed architecture naturally scales well, is able to operate in real time, and integrates with existing network

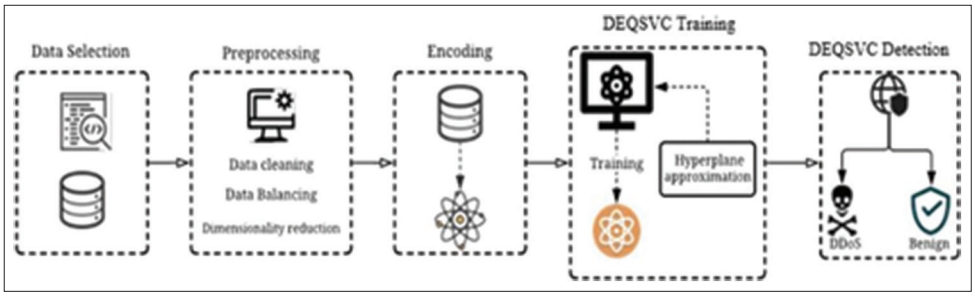

Fig. 1. Testbed configuration for the DoS and DDoS attacks launch during the LATAM-DDoS-IoT dataset creation [4].

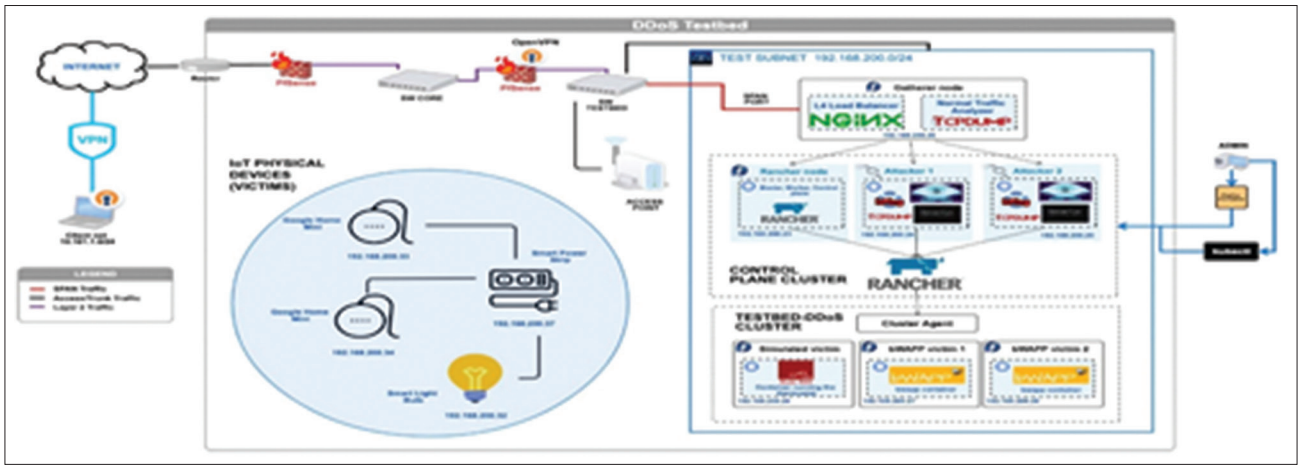

Fig. 2. DEQSVC detection approach [4].

architecture and this transforms into an immensely valuable tool for mitigating against DDoS and botnet intrusions and other evolving cyber threats [18]. For instance, Sahoo put forward an ESVM model to deal with the evolving threat of DDoS attacks in SDNs while the ESVM model is made up of components as follows [19]: Unlike other DDOS detection methods that are outdone since they do not adapt to new attack techniques by learning from them, ESVM employs an evolutionary algorithm in the creation of an SVM classifier, thus making it more of a dynamic classifier; an ever-evolving one as it seeks to learn from the newly invented DDOS attacks. Similarly, the dynamic nature of adaptation means that ESVM continues to be extremely effective in identifying DDoS attacks even though the attackers become more intelligent and complex. Besides flexibility, the proposed ESVM has a high precision level that is higher than traditional SVM and given DDoS detection methods. Being capable of handling networks of considerable size and fitting in well with the SDN controllers as was seen above, it is an effective tool for the protection of enterprise networks, cloud solutions, and IoT [1],[21],[22], [23]. Gu *et al.* explain a new approach to DDoS detection that involves both the labeled and unlabeled data handling limitations of traditional methods due to reliance on only label data. Their unsupervised research model can handle both labeled and unlabeled data, making it suitable for application in real-life settings. As a highly effective and versatile solution, SSKMeans proves useful in protecting networks against DDoS attacks across different scenarios [20].

In this connection, a number of scholars have suggested various ML techniques for identifying DDoS attacks [24]. The CIC IDS 2017 is used in Nalayini and Katiravan [25] to detect DDoS attacks. In this work, we apply data preprocessing and K-fold cross-validation to evaluate several models. The study found that the Random Forest algorithm is way better and more efficient than other models in identifying DDoS attacks within a short period. Such conclusion results from assessment measures such as recall, accuracy, precision, and FAR (False Alarm Rate). As Lunkad and Singh [26], another work performs a study that provides information on different DDoS attack motivations and ways of operation. The details of the gradual change in the types of DDoS attacks and the measures applied in their prevention are presented in this text. Furthermore, it assesses several means for identifying

TABLE 1: Discusses ML and various methodologies

References	Focus	Methodologies	Advantages	Limitations	Discussion
[2]	Cloud Computing	Machine Learning (GNB)	The framework improves Gaussian Naïve Bayes (GNB) classifier accuracy, precision, and recall by up to 2.07%. It solves the zero-frequency problem and employs iterative feature selection, making GNB more competitive and suitable to KNN, RF, DT, and SVM classifiers	GNB's assumption of feature independence makes it lag behind SVM despite improvements. Feature selection increases complexity and yields moderate recall benefits. Due to its preprocessing requirements, GNB may not be generalizable, creating a performance gap	The suggested framework is a Gaussian Naive Bayes classifier coupled with sequential feature selection and data preprocessing. Strategizing the choice of attributes and the use of techniques such as PCC, MI, and Chi-square enhances the efficiency and effectiveness of cloud DDoS detection
[3]	Quantum Computing	Quantum Computing, Dimensionaliy Reduction	DEQSVC detects DDoS with 99.49% accuracy using quantum ML. It outperforms benchmark algorithms and typical QSVMs in accuracy, recall, and precision with enhanced dimensionality reduction and resilient feature encoding	Although successful, DEQSVC's dependency on quantum computing platforms, such as IBM's may restrict its accessibility and scalability. The difficulty of quantum data encoding and model training may potentially hinder real-world applications	DEQSVC uses a combination of quantum computing and ML to address DDoS attacks, where dimensionality reduction and quantum encoding are available for efficient attack pattern identification. The obtained results demonstrate higher accuracy compared to conventional algorithms
[4]	IoT Devices Vulnerability	Dataset Creation, Anomaly Detection	Real attack and legitimate traffic make the LATAM-DDoS-IoT dataset a reliable data source for IoT anomaly identification. The dataset's 99.967% DDoS attack detection accuracy proves its efficacy. The smart IDS generated from this dataset detects over 90% of assaults without misclassifying them in virtual and physical contexts	While accurate, the IDS's dependence on certain datasets may restrict its use. The system solely records TCP traffic, and testing was done in a mixed virtual environment. To increase real-world applicability, UDP traffic and completely physical SDN systems must be prioritized	IoT LATAM-DDoS cross-feeds real traffic attacks on physical concrete appliances with user data to construct a dataset for fine-tuning anomaly detectors to help guard IOT devices against DoS attacks
[5]	SDN Environments	Deep Learning, LSTM	This method uses SDN and a 1D-CNN model optimized using NSGA-II to identify DDoS assaults with 99.99% accuracy. This technique dynamically modifies network regulations in real time for powerful protection. SMOTE at the protocol level improves dataset, model training, and complicated attack pattern detection	The simulation environment may not completely replicate real-world network complexity and dynamics, limiting the model's deployment efficacy. Simulated datasets may not completely reflect the range and complexity of developing DDoS assaults, limiting generalizability	The optimized AI model, which combines deep learning with specific SDN features and LSTM for network traffic observation, increases the accuracy of DDoS detection in the SDN environment
[6]	5G Networks	Feature Selection, Deep Learning (LSTM), Hyperparameter Optimization	Advanced feature selection, LSTM-based classification, and TSA-based hyperparameter tweaking provide a strong 5G DDoS attack detection system with MEOADL-ADC. Optimizing feature selection and model parameters yields 97.60% accuracy, making this technique viable for 5G network security	The model's benchmark datasets may restrict its adaptation to 5G network attack patterns, yet it is successful. Outlier elimination and other enhancements show that the technique may still struggle to perform well in dynamic contexts	MEOADL-ADC's overall workflow is an integration of MEOA for feature selection, LSTM-based deep learning, and TSA for optimizing hyperparameters for efficient DDoS attack classification in 5G networks

(*Contd...*)

TABLE 1: *(Continued)*

References	Focus	Methodologies	Advantages	Limitations	Discussion
[7]	IoT Devices	Snake Optimizer, Ensemble Learning (LSTM, DBN, BiLSTM)	The DDAD-SOEL method detects IoT DDoS assaults with 99.81% accuracy using the Snake Optimizer (SO) for feature selection and an ensemble of sophisticated deep learning models (LSTM, BiLSTM, DBN). This method protects sensitive IoT installations from DDoS attacks and optimizes model performance	The method's computationally demanding deep learning models may be difficult to deploy on resource-limited IoT devices. The approach is proven on benchmark datasets, but its performance in different, real-world IoT contexts may need more testing and lightweight models for wider application	DDAD-SOEL employs Snake Optimizer to choose features and deep learning models for the identification of DDoS attacks in IoT devices. Thus, the proposed method for predicting customer dynamics outperforms the existing approaches in terms of accuracy, precision, recall, and F1 score
[8]	Diverse Toolkits	Feature Selection, ML	The suggested ML approach identifies DDoS assaults with 99.9% accuracy, decreasing the feature set from 78 to 6, improving speed and efficiency. Its high accuracy, recall, and F1 score show that the model can effectively categorize DDoS attack tools, helping cybersecurity operations mitigate these attacks	The model's narrow feature set may miss minor attack patterns that develop, limiting its adaptation to new, sophisticated DDoS tools despite its high accuracy. While the model performs well in controlled conditions, its real-world efficacy against various and new DDoS attack vectors is yet untested	Different DDoS tools successfully identify network misuse through a procedure that chooses the data features and combines it with a comprehensive ML model, yielding high rates of accuracy, precision, recall, and F1
[9]	SDNs	Feature Selection (Chi-square), KNN	The research uses IG and RF feature selection approaches to improve SDN DDoS attack detection accuracy and reduce false alarms. LSTM and Autoencoder in the deep learning model identify attacks efficiently without affecting network speed or latency. Testing on several datasets shows that concentrating on key characteristics improves model efficiency	The study's high-dimensional dataset may make training difficult and time-consuming. The feature selection approaches assist, but the model may struggle with scalability and adaptation to new DDoS assaults. Further testing on live SDN networks is required to determine the model's real-world applicability	The solution optimizes the extraction of characteristic flows from networks, uses Chi-Square for feature selection, and uses KNN for normal traffic differentiation from actual attacks, providing a reliable method of protecting SDNs from DDoS attacks
[10]	Application-Layer DDoS Attacks	Radial Basis Function (RBF) Network, Cuckoo Search Algorithm	A new ML method for identifying App-DDoS assaults uses Radial Basis Function (RBF) neural networks with the Cuckoo Search Algorithm (CSA). This hybrid technique beats k-NN, Bagging, SVM, MLP, and RNN with 96.9% detection accuracy. Genetic Algorithm (GA) feature selection optimizes the model, improving error rate and accuracy	Due to integrating RBF, CSA, and GA algorithms, the study's technique may be complicated and computationally intensive. Although the approach is more accurate, its efficacy in many real-world settings and against developing assault techniques is questionable. The method's scalability and applicability to datasets other than NSL-KDD need more testing	We use the RBF network to accurately classify attacks and improve the cuckoo search algorithm to make the RBF network's configuration work best for finding common application-layer DDoS attacks

(*Contd*...)

TABLE 1: *(Continued)*

References	Focus	Methodologies	Advantages	Limitations	Discussion
[11]	DDoS Attack Pre-diction	Feature Selection, Multi-stage Approach	The article uses the newest UNSW-NB15 dataset to identify DDoS attacks effectively. It performs well with 89% and 90% accuracy using Random Forest and XGBoost algorithms. This is better than earlier models' lesser accuracy. Python data wrangling and a methodical manner strengthen the detection framework	The study's use of Random Forest and XGBoost may restrict its research of other promising techniques. Although intriguing, the article does not address the computational efficiency of these strategies. Supervised learning may neglect unsupervised learning approaches, which may discover new or emerging assault patterns	The following multi-stage strategy investigates network traffic characteristics, identifies the most important factors, and relies on ML algorithms to correctly identify current and future DDoS attacks
[12]	Internal IoT Networks	Deep Learning (LSTM), Anomaly Detection	Combining UNSW-NB15 and Bot-IoT characteristics gives the PB-DID architecture 96.3% classification accuracy. The selection of equal packets from each category solves data imbalance and overfitting. Deep learning and a smaller feature set improve non-anomalous, DoS, and DDoS traffic detection	This article employs just two benchmark datasets, which may restrict its generalizability. Despite its effectiveness, feature reduction may miss certain complex attack patterns. To guarantee detection system coverage and reliability, future work must include more datasets and attack types	PB-DiD uses the LSTM network to analyze network traffic and detect suspicious anomalies, which proved to be much more effective than traditional ML algorithms in identifying DoS and DDoS attacks
[13]	Various DDoS Attacks	Hybrid Deep Learning (AEMLP)	The AE-MLP model identifies and classifies DDoS assaults with over 98% precision, recall, F1-score, and accuracy. To automate feature selection and decrease processing costs, the model uses Autoencoder (AE) for feature extraction and Multi-layer Perceptron (MLP) for classification. This hybrid strategy is resilient enough to handle large-scale DDoS assaults, outperforming several other approaches	The model's efficacy is exclusively evaluated on the CICDDoS2019 dataset, which may restrict its applicability to other attacks or situations. Further validation with other incursion kinds and datasets is required to confirm the model's applicability across domains and real-world settings	AE-MLP uses autoencoder and multilayer perceptron networks to detect and classify various forms of DDoS attacks, demonstrating its strengths in dimensionality reduction and noise immunity
[14]	Wireless Sensor Networks	RNN, Proactive Defense	The paper analyzes transmission characteristics and network security to accurately identify DDoS assaults in Wireless Sensor Networks (WSNs). The method recommends 23 ms between transfers to reduce network overload and counteract DDoS assaults	The results may not apply to other DDoS attacks or real-world WSN settings due to the experimental emphasis on DDoS-PSH-ACK. The approach's efficiency in managing different network circumstances and attack vectors is also unknown	The discussion above emphasizes how crucial it is to take temporal dependencies into account when building defenses against various network-based attacks on wireless sensor networks, and it suggests using an RNN-based solution to predict ACK flood attacks

(*Contd...*)

TABLE 1: *(Continued)*

References	Focus	Methodologies	Advantages	Limitations	Discussion
[15]	Noisy Network Traffic	MLP, Data Prepro Cessing	Noise-robust MLP architecture filters out common characteristics from damaged datasets to identify DDoS assaults, improving performance. Comparatively, the strategy improves accuracy, detection rate, and false alarm rates	The noise-robust MLP may only work well with damaged data and may not work with all DDoS assaults or datasets. Using Higher Order Singular Value Decomposition (HOSVD) for feature filtering may add complexity or computational cost	The MLP design's immunity to noise and the preprocessing used in this paper ensure accurate identification of DDoS attacks when the network environment is noisy compared to other approaches
[16]	Corporate Networks	Real-time Analytics (Apache Spark), Anomaly Detection	Apache Spark parallel data processing makes the SAD-F framework scalable, real-time, and efficient for DDoS detection. It handles huge network traffic with 92% accuracy using the KNN model in a high-end testbed	SAD-F framework processing speeds vary greatly by testbed configuration, with lower-end installations taking longer. Memory usage during data gathering is considerable, and CPU and cluster size may restrict the framework's usefulness	The SAD-F framework, developed on Apache Spark, performs real-time analysis to discover signs of DDoS attacks in corporate networks; it enables a fast reaction and, thus, mitigates threats
[17]	Cloud Platforms	Stacked Sparse Autoencoder (SSAE), Hyperparameter Tuning	A stacked sparse Auto Encoder (AE) and Deep Neural Network (DNN) increase cloud DDoS attack detection in the suggested architecture. It handles high-dimensional, unbalanced, and noisy data with 98.92% accuracy on CICIDS2017. The strategy exceeds current approaches in accuracy, recall, and F1-score	Compared to NSL-KDD, the model performs similarly on CICIDS2017. The method has good accuracy, but real-time detection and computational simplicity need improvements. Managing large amounts of data in real-time is difficult	By fine-tuning the SSAE algorithm and altering the hyperparameter tunings, we can successfully apply the proposed method across various cloud platforms, ensuring its high portability and flexibility
[18]	Network Traffic Patterns	Distributed Architecture, ML	The study describes a two-tier distributed architecture for early DDoS prediction and bot identification. It detects bots early, preventing assaults. The system clusters network traffic to reduce data volume without affecting detection efficiency and achieves 99.9% detection accuracy	Early signal prediction may be inaccurate or late, resulting in missed assaults. The architecture's performance depends on network device clustering and early signal quality, which may vary by network environment and dataset	ML uses network traffic patterns to build a distributed architecture that can accurately detect DDoS attacks in any environment
[1]	SDNs	Evolutionary support vector machine (ESVM)	A multi-layer SVM with KPCA and GA is used to create a new SDN DDoS detection system. This method reduces dimensionality and optimizes SVM parameters to boost detection accuracy to 98.907%. The model is more efficient using the updated N-RBF kernel function, which decreases noise and training time	Multi-controller environments may challenge the concept, while single-controller environments work well. KPCA outperforms PCA in this case, but it may not work for other attackers or datasets. More effort is required to identify complicated attacks and multi-controller systems	ESVM employs a short-term evolution strategy to optimize the SVM classifier in real-time with better precision than basic SVM in the face of new and evolving DDoS attack patterns

(*Contd...*)

TABLE 1: *(Continued)*

References	Focus	Methodologies	Advantages	Limitations	Discussion
[20]	DDoS detection	Unsupervised learning (SSK Means)	The research offers a semi-supervised weighted k-means detection technique (SKM-HFS) that overcomes supervised and unsupervised DDoS detection constraints. A Hadoop-based hybrid feature selection approach with an upgraded density-based algorithm increases clustering accuracy and outlier handling. Experimental findings reveal that SKM-HFS outperforms previous approaches in TOPSIS assessment and detection	The approach is tested on certain datasets, but bigger and more varied datasets are required to validate its generality. While the technique increases detection, its parallel processing and real-world scalability need improvement	As mentioned before, SSK Means is an unsupervised research model that can simultaneously use labeled and unlabeled data; therefore, it turns out useful in defending against DDoS attacks across multiple situations

ML: Machine learning, DDoS: Distributed denial of service, 1D-CNN: One-dimensional-convolutional neural networks

such unauthorized access violations. Two approaches to identifying DDoS attacks are described in the work of [27]. Subsequently, a mathematical model is used to analyze the relationship between the time taken by the requests to reach the network and the performance of the network. Besides, the paper employs logistic regression and naive Bayes techniques for constructing the ML model aimed at DDoS attack detection through throughput analysis. Dell offers an elaborate system for the detection of DDoS attacks. The authors of [28] propose a separate algorithm aimed at the classification of DDoS attacks and achieve it by using the CCIDS2017 dataset. The future work of the proposed methodology is that the SVM classification algorithm is used to get a precision rate of 99%. 68%. Others include the size of the packets, the length of the packets, the time each flow is on the network, and the forward and backward packets among other characteristics of the packet. This shows how effective the method is in identifying the DDOS attacks as shown in the video. In particular, the study focuses on the CCIDS2017 dataset to detect DDoS attacks as demonstrated by Nath Rimal and Praveen [29].

To lessen the dimensions for the feature vector and cut down the time of complexity, we also employed PCA and considerably compressed the neural network model. In the selection of the output dimension, the use of PCA turns out to be more flexible than when LDA and other linear techniques of dimensionality reduction are used [30]. As for the packets dataset, the parameters are diverse including the transmission control protocol (TCP) flag, flow duration, header length, and length of the packet. By a SVM classification algorithm trained on this dataset, the proposed method is very effective at seeing DDOS traffic 99. 68% of the time. This establishes its efficiency in establishing the differences between an attack and a normal flow of traffic. The research indicated in Sudheer *et al.* [31] uses different types of ML models for the evaluation of the input information for the purpose of detecting DDoS attacks. To increase this accuracy, the authors utilize PCA and a random forest classifier for ranking the features based on their importance. The accuracy of the Decision Tree model is higher than the accuracy of the rest of the classifiers that were tested, and therefore the Decision Tree model can be considered as a very promising and valuable instrument for the detection of DDoS attacks [32]. Furthermore, prevention, as it is pointed out in the case of DDoS assaults, is the best way. The authors recommend packet filtering as a way of filtering out the bad packets in other to minimize DDoS attacks. It demonstrates the need for proactive defensive measures possible through an analysis of various approaches such as ingress/egress packet filtering, router-based packet filtering, and some statistical approaches like Packets Core.

3. DISCUSSION

Table 1 discusses ML and various methodologies used to combat DDoS attacks in multiple technological areas. Ranging from cloud computing and SDN environments to 5G networks and IoT devices, the table displays 19 entries.

4. CONCLUSION

In the end, this extensive literature review critically appraises 19 core studies that discuss the serious dangers posed by DDoS attacks. It also reviews various methodologies, with a primary focus on ML methods. The review includes new app the review includes some new methods, such as a revisited Gaussian Naive Bayes classifier for DDoS detection in cloud computing settings, a DEQSVC framework based on quantum computers, and a better AI model for finding DDoS attacks in SDN settings, promising technique to categorize DDoS attacks in 5G networks, showing unprecedented accuracy. Furthermore, the DDAD-SOEL approach is designed to counteract IoT device attacks caused by DDoS using Snake Optimizer and multiple deep learning models ahead of other methods in terms of precision, accuracy, as well as F1 score. In addition, the literature review stresses considering DDoS attacks in certain scenarios, such as SDNs, IoT devices, and clouds. The provided solutions have significant achievements, namely improved accuracy and precision, as well as suitability in the protection of infrastructure items. These innovations add significant value to the field, providing a wide variety of techniques that strengthen defensive mechanisms and reduce challenges caused by DDoS attacks. All in all, the results reflected ML and alternative methodologies needed to protect network security through reliable delivery of critical services due to expanding cyber threats.

REFERENCES

[1] K. S. Sahoo, B. K. Tripathy, K. Naik, S. Ramasubbareddy, B. Balusamy, M. Khari and D. Burgos. "An evolutionary SVM model for DDoS attack detection in software defined networks". *IEEE Access*, vol. 8, pp. 132502-132513, 2020.

[2] S. Naiem, A. E. Khedr, M. I. Marie and A. M. Idrees. "Enhancing the efficiency of gaussian naive bayes machine learning classifier in the detection of DDoS in cloud computing". *IEEE Access*, vol. 11, pp. 124597-124608, 2023.

[3] A. Alomari and S. A. Kumar. "Deqsvc: Dimensionality reduction and encoding technique for quantum support vector classifier approach to detect DDoS attacks". *IEEE Access*, vol. 11, pp. 110570-110581, 2023.

[4] J. G. Almaraz-Rivera, J. A. Perez-Diaz, J. A. Cantoral-Ceballos, J. F. Botero and L. A. Trejo. "Toward the protection of iot networks: Introducing the latam-DDoS-iot dataset". *IEEE Access*, vol. 10, pp. 106909-106920, 2022.

[5] Y. Al-Dunainawi, B. R. Al-Kaseem and H. S. Al-Raweshidy. "Optimized artificial intelligence model for DDoS detection in sdn environment". *IEEE Access*, vol. 1, pp. 106733-106748, 2023.

[6] M. Aljebreen, F. S. Alrayes, M. Maray, S. S. Aljameel, A. S. Salama and A. Motwakel. "Modified equilibrium optimization algorithm with deep learning-based DDoS attack classification in 5g networks". *IEEE Access*, vol. 11, pp. 108561-108570, 2023.

[7] M. Aljebreen, H. A. Mengash, M. A. Arasi, S. S. Aljameel, A. S. Salama and M. A. Hamza. "Enhancing DDoS attack detection using snake optimizer with ensemble learning on internet of things environment". *IEEE Access*, vol. 11, pp. 104745, 2023.

[8] D. M. Sharif, H. Beitollahi and M. Fazeli. "Detection of application-layer DDoS attacks produced by various freely accessible toolkits using machine learning". *IEEE Access*, vol. 11, pp. 51810-51819, 2023.

[9] M. S. El Sayed, N. A. Le-Khac, M. A. Azer and A. D. Jurcut. "A flow-based anomaly detection approach with feature selection method against DDoS attacks in sdns". *IEEE Transactions on Cognitive Communications and Networking*, vol. 8, no. 4, pp. 1862-1880, 2022.

[10] H. Beitollahi, D. M. Sharif and M. Fazeli. "Application layer DDoS attack detection using cuckoo search algorithm-trained radial basis function". *IEEE Access*, vol. 10, pp. 63844-63854, 2022.

[11] Ismail, M. I. Mohmand, H. Hussain, A. A. Khan, U. Ullah, M. Zakarya, A. Ahmed, M. Raza, I. U. Rahman and M. Haleem. "A machine learning-based classification and prediction technique for DDoS attacks". *IEEE Access*, vol. 10, pp. 21443-21454, 2022.

[12] M. Zeeshan, Q. Riaz, M. A. Bilal, M. K. Shahzad, H. Jabeen, S. A. Haider and A. Rahim. "Protocol based deep intrusion detection for dos and DDoS attacks using unsw-nb15 and bot-iot data-sets". *IEEE Access*, vol. 10, pp. 2269-2283, 2021.

[13] Y. Wei, J. Jang-Jaccard, F. Sabrina, A. Singh, W. Xu and S. Camtepe. "Ae-mlp: A hybrid deep learning approach for DDoS detection and classification". *IEEE Access*, vol. 9, pp. 146810-146821, 2021.

[14] M. A. Al-Naeem. "Prediction of re-occurrences of spoofed ack packets sent to deflate a target wireless sensor network node by DDoS". *IEEE Access*, vol. 9, pp. 87070-87078, 2021.

[15] J. P. A. Maranhão, J. P. C. da Costa, E. P. de Freitas, E. Javidi and R. T. de Sousa. "Noise-robust multilayer perceptron architecture for distributed denial of service attack detection". *IEEE Communications Letters*, vol. 25, no. 2, pp. 402-406, 2020.

[16] A. Ahmed, S. Hameed, M. Rafi and Q. K. A. Mirza. "An intelligent and time-efficient DDoS identification framework for real-time enterprise networks: SAD-F: Spark based anomaly detection framework". *IEEE Access*, vol. 8, pp. 219483-219502, 2020.

[17] A. Bhardwaj, V. Mangat and R. Vig. "Hyperband tuned deep neural network with well posed stacked sparse autoencoder for detection of DDoS attacks in cloud". *IEEE Access*, vol. 8, pp. 181916-181929, 2020.

[18] M. Rahal, A. Santos and M. Nogueira. "A distributed architecture for DDoS prediction and bot detection". *IEEE Access*, vol. 8, pp. 159756-159772, 2020.

[19] K. S. Sahoo, B. K. Tripathy, K. Naik, S. Ramasubbareddy, B. Balusamy, M. Khari and D. Burgos. "An evolutionary SVM model for DDoS attack detection in software defined networks". *IEEE access*, vol. 8, pp. 132502-132513, 2020.

[20] Y. Gu, K. Li, Z. Guo and Y. Wang. "Semi-supervised k-means DDoS detection method using hybrid feature selection algorithm". *IEEE Access*, vol. 7, pp. 64351-64365, 2019.

[21] R. A. Hamaamin, S. H. Wady and A. W. Kareem Sangawi. "The effect of feature extraction on Covid-19 classification". *Science Journal of University of Zakho*, vol. 12, no. 2, pp. 227-236, 2024.

[22] O. M. Amin Ali, S. Wahhab Kareem and A. S. Mohammed. "Evaluation of Electrocardiogram Signals Classification using CNN, SVM, and LSTM Algorithm: A Review". 2022 8th *International Engineering Conference on Sustainable Technology and*

Development (IEC), Erbil, Iraq, 2022, pp. 185-191.

[23] R. A. Hamaamin, O. M. A. Ali and S. W. Kareem. “Biometric systems: A comprehensive review”. *Basrah Journal of Science*, vol. 24, no. 2, pp. 146-167, 2024.

[24] A. Saeed and N. G. M. Jameel. “Intelligent feature selection using particle swarm optimization algorithm with a decision tree for DDoS attack detection”. *International Journal of Advances in Intelligent Informatics*, vol. 7, no. 1, pp. 37-48, 2021.

[25] C. M. Nalayini and J. Katiravan. “Detection of DDoS attack using machine learning algorithms”. *SSRN Journal*, vol. 9, no. 7, p. 4173187, 2022.

[26] D. Lunkad and S. Govind. “DDOS attack detection using machine learning for network performance improvement.” *International Journal of Creative Research Thoughts*, vol. 8, pp. 2320-2882, 2020.

[27] K. Kumari and M. Mrunalini. “Detecting denial of service attacks using machine learning algorithms”. *Journal of Big Data*, vol. 9, no. 1, p. 56, 2022.

[28] J. Pei, Y. Chen and W. Ji. “A DDoS attack detection method based on machine learning”. *Journal of Physics: Conference Series*, vol. 1237, p. 032040, 2019.

[29] P. S. Saini, S. Behal, and S. Bhatia. "Detection machine learning algorithms." *In* 2020 7*th International Conference Sustainable Global Development (INDIACom)*, pp. 16-21. IEEE, 2020.

[30] Q. Li, M. Linhai, Z. Yuan and Y. Jinyao. DDoS attacks detection using machine learning algorithms. In: “*Digital TV and Multimedia Communication: 15th International Forum, IFTC 2018, Shanghai, China, September 20-21, 2018, Revised Selected Papers 15*”. Springer, Singapore, pp. 205-216, 2019.

[31] Z. H. Sahosh, A. Faheem, M. B. Tuba, Md. I. Ahmed, and S. A. Tasnim. "A comparative review on DDoS attack detection using machine learning techniques." *Malaysian Journal of Science and Advanced Technology*, Vol. 4 no. 2, pp. 75-83, 2024.

[32] B. Fakiha. “Detecting distributed denial of services using machine language learning techniques”. Xinan Jiaotong Daxue Xuebao/Journal of Southwest Jiaotong University, vol. 57, no. 5, pp. 675-688, 2022.