International Journal on Robotics, Automation and Sciences

From Signatures to AI: A Comprehensive Review of DDoS Detection Strategies in IoT & SDN

Shehroze Ahmed Khan*, Syed Ihtesham Hussain and Jawaid Iqbal

***Abstract* – In the ever-evolving landscape of the Internet of Things (IoT) and Software-Defined Networks (SDN), the rapid growth of interconnected devices has enhanced ease and efficiency. However, this evolution has also paved the way for the ominous cyber-attack: Distributed Denial of Service (DDoS). These attacks, which make systems unavailable for legitimate users, threaten the data integrity, confidentiality, and availability in IoT and SDN infrastructure. This paper delves into the critical issue of DDoS attacks within the IoT and SDN environments, offering a comprehensive exploration of detection mechanisms by categorizing them into traditional (signature-based) and anomaly-based approaches i.e., Machine Learning (ML), Deep Learning (DL), and statistical techniques. Our key findings reveal that while signature-based methods effectively identify known attack patterns, they fall short against novel threats. In contrast, AI-based approaches, particularly ML and DL, demonstrate superior performance in detecting previously unseen attacks. However, their efficiency is highly dependent on the quality of training data and model robustness. Our comparative analysis indicates that ML and DL methods achieve higher detection rates and lower false positives in experimental settings, underscoring the importance of high-quality datasets and resilient models. By highlighting the strengths and limitations of both approaches, this study provides valuable insights for researchers and cybersecurity experts. The need for an effective and diversified DDoS detection mechanism in the developing IoT and SDN domains is evident. While conventional methods remain relevant, AI-based strategies offer a dynamic avenue for enhancing security.**

Keywords*— *IOT, SDN, ML, DDOS Attacks, AI Detection Approach, Traditional Approaches.

I. Introduction

The 21st century connects the world digitally. Such enormous growth in information access opens an easy gateway to intruders. To cope with malicious intentions, cyber-security emerges to safeguard the Integrity, Confidentiality, and Availability of belongings of the governments, organizations, or individual's digital assets by preventing Cyber-attacks [1].

Cyber-attack is a deliberate attempt by cybercriminals also known as hackers, to penetrate the digital system intended to obtain sensitive, confidential information or to get control or to corrupt the system by taking advantage of the system's loop-holes and then launching various kinds of network attacks accordingly. These attacks are not only confined to individual or small and big organizations' digital assets but also a concern at the government level [2]. Generally, cyber security against cybercrimes splits into five stages which are commonly referred to as Identity, Protect, Detect, Respond, and Recover [2]. Figure 1 represents the commonly known stages of

.*corresponding author email: shehroze.khan@ riphah.edu.pk ORCID: 0009-0003-2588-499X
Shehroze Ahmed Khan is with Faculty of Computing, Riphah International University, Islamabad, Pakistan (e-mail: shehroze.khan@ riphah.edu.pk).
Syed Ihtesham Hussain is with Faculty of Computing, Riphah International University, Islamabad, Pakistan (e-mail: ihtesham.hussain@ riphah.edu.pk).
Jawaid Iqbal is with Faculty of Computing, Riphah International University, Islamabad, Pakistan (e-mail: jawaid.iqbal@ riphah.edu.pk).

International Journal on Robotics, Automation and Sciences (2025) 7, 1:19-26
https://doi.org/10.33093/ijoras.2025.7.1.3
Manuscript received: 24 Oct 2024 | Revised: 14 Dec 2024 | Accepted: 30 Dec 2024 | Published: 31 Mar 2025

Published by MMU PRESS. URL: http://journals.mmupress.com/ijoras

cyber security. The intentions of cybercriminals can vary from personal fun to exploitative purposes [3].

Cyber-attack is a deliberate attempt by cybercriminals According to [4], these attacks can be confined into two categories "Active" and "Passive" attacks. A type of active attack is the DDoS attacks, which can prohibit authorized users from accessing network services. The servers can be the target of a DDoS attack by flooding the network with a massive volume of traffic, which can exhaust the network's resources [5]. Additionally, there are many devices that can be connected to the Internet as a result of the IoT age. As a result, attackers can utilize numerous DDoS attack types by utilizing a large number of bots from various locations. DDoS attacks [6] have the ability to overload several SDN levels, including the channels for communication between the controller and application layer or between the controller and open flow switches. If a DDoS attack overwhelms SDN, which has a single point of failure, the entire network will crash at once. As DDoS attacks in IoT and SDN environment becomes frequent, it urges the need for an effective and efficient detection system to mitigate its attacks [7]. A detection system in IoT environment is hardware or it can be software that observes the abnormal behavior in traffic flow and analyzes the detection phase, where regular packets are separated from irregular packets. Beside IDS is utilized to check the audit log for illegal activities in the network [8]. Hybrid approach for the detection of anomalies is proposed using data mining techniques to avoid the adversary attacks [9]. Under the anomaly approach, Artificial intelligence is widely used, using its Machine learning and Deep learning techniques for DDoS detection [10,11].

FIGURE 1. Cyber Security Framework [2]

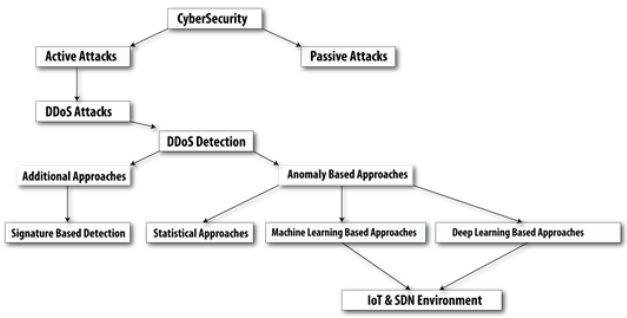

FIGURE 2. Research Hierarchy

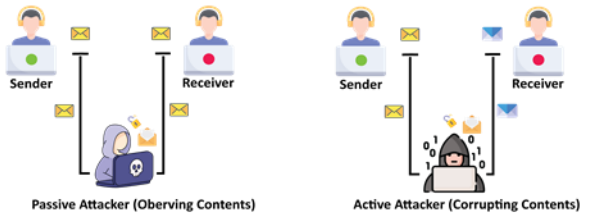

FIGURE 3. Passive Attacks Vs Active Attacks

This study serves as a roadmap for practitioners and researchers, providing insights into the growing threat landscape of DDoS attacks within IoT and SDN. It blends the collective wisdom of traditional and AI-based detection approaches while focusing on the significant role, AI (ML and DL) technologies play in strengthening the security of IoT and SDN infrastructure. Figure 2 illustrates the research roadmap to understand the flow of this study.

II. Passive Attacks Vs Active Attacks

In the case of passive attacks in wireless sensor networks adversary only listen the traffic flow without the victim's notice, the intruder enters the system to observe and steal the resources for various purposes compromising its confidentiality without corrupting its contents [12]. However, the active attack, [13] is another category of a cyber-attack where an intruder penetrates the system aiming to get control or to modify and corrupt the resources harming its integrity and availability. In a COVID-19 pandemic, mostly communication is on digital platforms that leads to security breaches [14]. Figure 3 depicts the difference b/w an active and passive attack.

III. DDoS Attacks

Distributed Denial of Service (DDoS) is one of the devastated forms of active attacks, in which the cyber-criminal by deploying various compromised devices ranging from 12 to 100,000 from multiple geographical locations attacks the victim by sending a flux of artificial traffic aiming to either make interruptions or block the whole system or even to seize on all the available resources causing its unavailability for the authorized users. Beside optimized artificial intelligence model is have proposed for the DDoS detection in SDN environment [15]. The recent studies reveal the prophecy of Cisco that DDoS attacks are becoming quick in succession, jumped from a figure of 7.9m in 2018 to more than 15 million in 2023 [16]. On Feb 2020 this variant victimized Amazon Web Services (AWS) for three days with a gigantic volume that reached 2.3 Tbps [15]. Based on its nature, DDoS attacks can be split two groups. The first one is known as bandwidth attack, [17] that targets the system's network bandwidth with the help of Zombies/Bots, aiming to overload the system's network by sending a flux of packets at once, which results in reducing the processing power and reaching the system's maximum memory capacity making it ineffective to serve the authorized users. and the second one is source depletion attack [18], here its attack makes the system unavailable by consuming its resources either by distorting the network protocols or sending abnormal packets [19]. Figure 4 represent this DDoS attack.

IV. DDoS And the Detection Mechanism

The rapid frequency of DDoS attacks urges the need for an efficient detection mechanism and to deal with this challenge, many detection methodologies have been proposed with different success ratios. On the basis of their technical nature of working, the DDoS detection mechanism can be split into Traditional approaches and Anomaly detection [20]. Figure 5 shows the DDoS detection mechanism's categories.

V. Traditional Approaches

These approaches are more focused on observing the network traffic volume and whenever the traffic volume exceeds a certain threshold, it creates an alert for DDoS attack.

A. Signature Based Detection

The most ordinary detection mechanism where already captured attack pattern plays the fundamental role. The signature detection mechanism can only detect the known attack after comparing its pattern with the pre-stored pattern in the database and would fail to detect, if there exists a minimal change in pattern. The mechanism is efficient in detecting the known attacks and requires high processing power but the attack pattern needs to be updated regularly [2]. DDoS attack detection based on signature mechanism further splits into "Traffic Analysis Pattern" and "Correlation of IP address" [20].

- Traffic Pattern Analysis is based on the idea that malicious packets behave in a similar manner to genuine ones, yet differently. For instance, in a botnet attack, all the bots are normally under the authority of a single bot master. The behavior is caused by requests being sent to several botnet members, which is why the same patterns are observed. With this technique, incoming traffic patterns are compared to already-created authentic traffic profiles. These profiles should not deviate in any way since malicious traffic will. When the terminal providing the traffic is secure, traffic features can be recorded to create a profile of valid traffic [21].
- Correlation of IP, based on Detecting falsified IP addresses is crucial for localizing DDoS attacks because attackers often fake packet origins. This method involves comparing IP addresses between the target server and the attacker's spoofed server. When disparities emerge, it triggers a DDoS alert, allowing for targeted traffic filtering and mitigation [20]

B. Anomaly Detection

This mechanism [2] has its foundation in monitoring legitimate traffic and captures their regular pattern over a certain time and whenever traffic shows irregular or abnormal behavior it suggests an attack, which makes it proficient in detecting the unknown and zero-day attacks. Based on its nature, the DDoS detection method further splits into a Statistical approach, Machine learning and Deep learning [20].

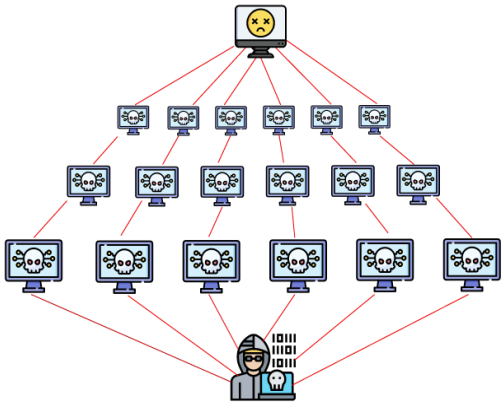

FIGURE 4. General scenario for DDoS Attack [19]

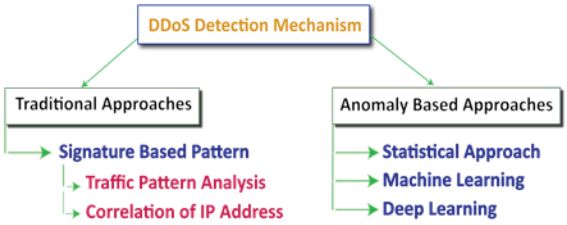

FIGURE 5. Categories of DDoS Detection Mechanism [20]

- Statistical Approach creates a threshold after monitoring the statistical features of the legitimate traffic and if the traffic exceeds the threshold it is marked as malicious traffic. This mechanism uses a sophisticated statistical algorithm to differentiate the irregular behavior from the regular pattern of the already built network flow and can detect the attack without prior knowledge but using only the statistical features which makes it more effective in detecting the malicious activities [2].
- Machine learning (ML) algorithms are divided into three categories supervised, unsupervised and reinforcement learning [21]. [22] Each input data is connected to a class, or label, in supervised learning algorithms. The computer uses the training sample to predict the type of input data during testing. Due to the fact that the class of the training sample is known during the learning phase, this is called supervised learning. We don't have any labeled responses when the cases are unsupervised While using the trial-and-error method, the machine is continuously trained in the reinforcement learning method. In order to make the best decisions possible, it draws on prior knowledge and works to acquire new information. OneR, LR, NB, BN, K-NN, DT, RF, and SVM are common algorithms used for supervised learning [23] while for unsupervised learning, algorithms like EM and K-means are common [24].
- Artificial intelligence (AI) uses deep learning, a form of machine learning (ML), to learn from both supervised and unstructured data. Due to the usage of multilayer networks, deep learning is often referred to as a deep neural network or deep neural learning. Furthermore machine learning classifier are utilized for early detection

of DDoS attack in IoT environment [25]. Neurons [26], which represent the mathematical calculations of the learning process, connect the layers. Preprocessed data are used as input by DL algorithms, which then extract and classify features and determine whether the samples are benign or malignant. Five categories are covered under the taxonomy: Based on standard DL technique parameters, supervised instance learning, supervised sequence learning, semi-supervised instance learning, hybrid learning, and other learning methods of DL models are used to detect DDoS attacks [27].

In Table 1, two main categories of detection techniques are analyzed. An unidentified attack or even a version of a known attack cannot be detected using the signature-based detection method. By using these techniques, any modifications to the attack signature patterns that already exist are not caught. Numerous false alarms are set off in this case. The attack signatures' database must be routinely updated as a result. However, maintaining an attack signature can be costly and occasionally challenging. The primary benefit of anomaly-based detection over signature-based detection is that it has the ability to localize new assaults whose signatures deviate from typical traffic patterns. However, due to the large amount of resources required for monitoring, its detection speed is actually quite slow.

VI. DDoS IN IoT

The DDoS detection in the SDN is improved using the deep learning algorithms [28]. Internet of Things is a gigantic network of interconnected devices with the capability of interacting, collaborating, sharing, and receiving services, information, and data without being dependent on human aid.

TABLE 1. Overview of the DDoS Detection Approaches and their constraints [27].

Approaches	*Working*	*Constraints*
Signature Based	Attacks are identified using captured signatures of well-known attacks within the database	• Lacks detection precision for different types of known assaults in the database. • Attacks that are unknown or zero day cannot be found. • Increased false negative rates are brought on by misrepresenting signature patterns. • Requires that the database's attack signatures be updated often.
Anomaly Based	Creates a threshold of typical traffic behavior based on data gathered over a given time period.	• The Speed of detection is not high. • Attack patterns using encryption have not been found. • Occasionally produce high false alert rates.

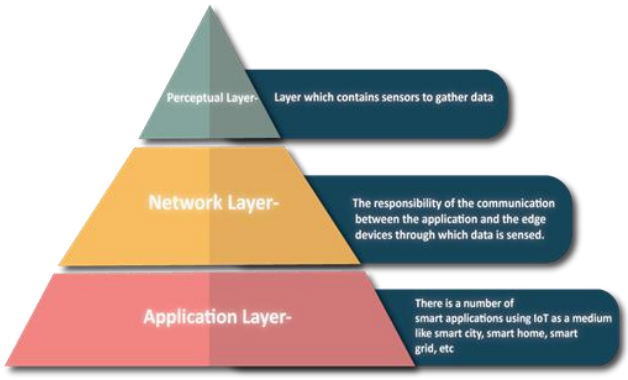

FIGURE 6. Basic Layered Approach of IoT [31]

IoT [29] has grown to be the biggest network with millions of devices communicating with one another to facilitate and ease human tasks. A recent survey found that there are 22 million Amazon Echo's and 310.4 million dollars' worth of wearable technology had been sold till 2017 and the number is doubling with each passing year. In the entire IoT working span, many operations are performed at various levels to accomplish the desired goal of any smart application [30]. Data collection [31] via various sensing devices, including sensors, RFID readers, and smart controllers, is the primary focus of the first layer. To ensure compatibility with the various protocols used inside the network, the collected data must follow established. formats. In addition, the 2nd layer known as the network layer controls the connection between edge devices and applications, enabling data transmission across wireless networks like Bluetooth, Wi-Fi, and Zigbee. Last but not least, the outermost application layer functions as the user interface for a variety of IoT-based smart applications, including apps for smart grids, homes, and cities. These layers work together to create the architecture for effective Internet of Things-based systems, enabling seamless data transfer from sensors to applications across a variety of areas [32]. Three layers, which stand for different functionalities, make up the fundamental model presented in Figure 6. Although it has a fairly simple definition, when it comes to security and privacy concerns, it becomes considerably more intricate and significant. a result of unstable networking protocols being utilized, and there is substantially less human interference and more exposure to different cyber-attacks.

VII. DDoS IN SDN

A new network paradigm called the Software Defined Network (SDN) emerged as a result of many issues with current networks, including vertical integration, coupling between the data and controller planes, difficulty modifying (or inserting) applications into the network, and decentralization [33]. The flexibility of SDN [34] to decouple the data and controller planes gives developers more freedom and makes it easier to maintain applications in these environments. It was able to isolate the network infrastructure from its applications in order to decouple the control plane and allow for logical centralization. As a result, software can be used to build services that are implemented by hardware (such as IDS, Firewall, and Routers) [35]. Because the network controller and the

switches have well-defined programmable interfaces through APIs, which enable communication between them, this centralization and decoupling of SDN is possible [33]. However, SDN [36] use has the potential to be innovative, but it also presents some new security challenges for networks. These issues may jeopardize a secure communication network's fundamental characteristic including its confidentiality, integrity, information availability, and authentication [37].

VIII. Analysis of ML DDoS Detection Approaches in IoT & SDN

In [38] to enhance the detection and mitigation of DDoS attack using ensemble online machine learning model in the SDN environment is utilized. Moreover using SVM to identify assaults in a network powered by SDN. This method includes gathering network packets on a regular basis and extracting 24 features from them. Then, these features are categorized using SVM to look for anomalies. The method's effectiveness was evaluated against that of the J48 and Naive Bayes (NB) classification algorithms using the NSL-KDD dataset. The technique has a 99.4 percent detection accuracy compared to the J48 and NB algorithms' respective values of 99.75 percent and 95.87 percent. It can be demonstrated that the suggested method falls short in terms of accuracy while the J48 classification method continues to perform better. Additionally, the approach has a considerable computational overhead.

In [39] work, Decision Trees (DT) were used by the researchers to identify Distributed Denial of Service (DDoS) assaults in an environment with multiple layers of the Internet of Things (IoT). IoT gateways, cloud servers, SDN switches, and IoT devices made up this environment. Eight smart poles with different capabilities were deployed in a campus-wide wireless sensor network. To communicate sensor data, these poles used Wi-Fi, Bluetooth, ZigBee, and LoRa. A Raspberry Pi 3 served as a heterogeneous gateway for data transfer on each pole. Sensor data packets were gathered and made ready to be processed by the IoT gateway, and DT classifiers were trained to recognize DDoS attacks based on packet properties. These classifiers identified whether packets were normal or abnormal, accurately identifying different attack types. In order to lessen the effects of DDoS assaults, the SDN controller and an SDN switch were utilized to blacklist compromised devices and regulate network traffic bandwidth when attacks were detected.

In [40] multiple methods have explored against mitigation of DDoS attack in the IoT environment to protect the sensitive data during transmission using public network. However a threat identification and controlling architecture for IoT networks based on machine learning. The retrieved properties from the BoT-IoT dataset were categorized in this work using a multi-class classifier developed using DT, RF, k-NN, multi-layer perception (MLP), RNN, and LSTM. With a looking-back methodology, this classifier also localizes the assault subcategories. The results of the evaluation show that the accuracy of looking-back-enabled RF is highest, whereas that of k-NN under identical circumstances is lowest.

The [41] introduced a hybrid feature selection methodology to the Extreme Gradient Boosting (XGBoost), RF, DT, and k-NN classifiers. Chi-square, Extra Tree, and ANOVA are the hybrid feature selection techniques. The CICDDoS2019 dataset was used to verify this method's efficacy. The evaluation's findings demonstrate the higher performance of XGBoost with ANOVA, which has an accuracy of 98.35 %. With only 15 features and an 82.5 % feature reduction ratio, this performance was accomplished. When all the features were taken into account, XGBoost's accuracy fell to 96.7 %.

Table 2 gives an overview of the studies and progress made in using machine learning models for assault detection. Based on the methodology used, the dataset, and the application domain, these researches were contrasted.

IX. Analysis of DL DDoS Detection Approaches in IoT & SDN

Various mitigation strategies have proposed for DDoS attack in the SDN environment to enhance the security and privacy of data plan and control plan [42]. However, different approaches to attack detection in an IoT network were looked at separately. While the second method makes use of an LSTM deep learning model, the first method utilizes a hybrid intrusion detection system. The CICDDoS2019 dataset served as a demonstration of how applicable these methods are. For DDoS and DoS attacks, the combined accuracy of the two approaches was 91.9 %. A few instances of false alarms were noted in this investigation.

The [43] worked for identifying assaults in an IoT environment, a customized deep learning solution has been presented. In this study, multiclass attack prediction was carried out using an embedding layer and a FNN method. A binary classification model was also created using FNN technology.

TABLE 2. An overview of studies on the use of ML models for detecting DDoS attacks

Adopted Approaches	Overview	Dataset	Environment	Takeaway
SVM [38]	Gather network packets on a regular basis. Take 24 features out of each packet. Use SVM to classify the features	NSL-KDD	IoT-SDN	Achieves 99.4% detection accuracy. Considerable computational overhead.
DT [39]	Using an IoT gateway, captured sensor data packets. A DT classifier is trained using data.	Created	Multi-layer IoT	With 97.39% accuracy, ICMP, SYN, and UDP floods are identified. F1- score has been obtained above 97%.
DT, RF, K-NN and XGBoost [41]	Apply the feature selection method to four classifiers to evaluate the decision precision	CICDoS2019	IoT	With an accuracy of 98.35% XGBoost with ANOVA performs better.

The method's success is demonstrated by the evaluation findings. Each classifier outperformed the other. Particularly, the multi-class classifier achieved approximately 99.79% accuracy while the binary classifier demonstrated detection accuracy close to 99.99%. Only a few assault classes were apparently found in this investigation. Therefore, it is not always possible to identify alternative attack types.

Work [5] explains how an RNN combined with an autoencoder (AE) can increase the SDN's DDoS attack detection accuracy. In comparison to the NB, RF, DT, SVM, and linear regression classifiers, this scheme's effectiveness was assessed. When compared to previous methods, the scheme significantly improves accuracy when tested on the CICDDoS2019 dataset. The method reports a 99% accuracy rate. The study, however, did not include reporting performance indicators such model training time or samples identified, despite the fact that the computational overhead was slightly decreased. Based on the [44] dataset, the application domain, and the deep learning model employed, these researches are contrasted. The proposed framework is tested using the CICDDoS2019 dataset to identify reflection attacks and exploitation attacks in TCP, UDP, and ICMP. The experimental findings show that, in comparison to current methods, the suggested framework can effectively detect and mitigate DDoS attacks while making efficient use of CPU resources and doing so faster.

Table 3 shows the DL models that are used for detecting DDoS attacks. Table 4 presents a comparison of ML & DL methods. This comparison is based on the features of each method, their strengths, and constraints.

TABLE 3. An overview of studies on the use of DL models for detecting DDoS attacks

Adopted Approaches	Overview	Dataset	Environment	Takeaway
LSTM [42]	Examine the application of LSTM and Hybrid intrusion detection system.	CICDDoS2019	IoT	The Combined accuracy of the two methods is 91.9%. Considerable computational overhead.
FNN [43]	For multiclass attack prediction, combine an embedding layer and an FNN model.	Created	IoT	It is shared that only a few attack classes have been found, thus it is not obvious that more attack classes will also be identified.
AE, RNN, [5]	For Increased accuracy, combine AE with RNN	CICDDoS2019	SDN	The method records a 99% accuracy rate. Minimizes the computational overhead.

TABLE 4. An overview of comparison on the use of ML & DL models for detecting DDoS attacks

Approaches	Overview	Strengths	Takeaway
Machine Learning	By studying the characteristics of the network traffic, algorithms can be used to distinguish malicious data from other types of network traffic.	Quickly recognizes traffic patterns. Excellent detection precision.	Problem with Feature engineering. Long period of training. Better accuracy requires a larger dataset.
Deep Learning	Uses its feature extraction and classification module, which benefits from both supervised and unsupervised learning.	Being able to identify high-dimensional features. Flexible response to new issues. Super capacity to learn layer features. Having the capacity to directly process raw data.	Issue with generalization. Leads to overfitting occasionally. Overhead in computation. Better accuracy requires a larger dataset.

X. CONCLUSION

In a rapidly digital era, where IoT and SDN form the backbone of the interconnected world, the growing threat of DDoS attacks is a great concern. The deliberate, malicious attempts to overwhelm & incapacitate computer systems or networks by flooding them with massive traffic or requests, disrupting the normal operations of IoT and SDN infrastructure, causing severe impact on their performance or making them non-functional. The damaging effects of DDoS provoke the urgent necessity for strong and effective methods to detect & mitigate these attacks.

This paper analysis commenced by categorizing the detection mechanism into two paradigms; the traditional signature-based method & anomaly-based approaches, fueled by ML, DL, and statistical techniques. Based on this classification, this work highlighted the strengths and constraints of each, mentioning how the signature-based technique is effective in identifying known attack patterns but ineffective in the case of novel attacks, while anomaly-based approaches show their superiority by detecting unseen attacks.

In conclusion, this study investigated AI-driven DDoS detection techniques adapted for IoT and SDN settings. This paper carried out a thorough comparison analysis and offered insights into their advantages and performance indicators. The foundation of contribution in this analysis, which is important for researchers, and cybersecurity experts. The need for an effective and diversified DDoS detection mechanism in the developing IoT and SDN domains is presented in this study. While the conventional approaches are still effective, AI-based strategies open up a new dynamic area for improving security.

ACKNOWLEDGMENT

We thank the anonymous reviewers for the careful review of our manuscript.

FUNDING STATEMENT

There are no funding agencies supporting the research work.

AUTHOR CONTRIBUTIONS

Shehroze Ahmed Khan: Conceptualization, Data Curation, Methodology, Validation, Writing – Original Draft Preparation;

Syed Ihtesham Hussain: Investigation, Writing – Review & Editing;

Jawaid Iqbal: Project Administration, Visualization, Supervision, Writing – Review & Editing.

CONFLICT OF INTERESTS

No conflict of interests were disclosed.

ETHICS STATEMENTS

Our research work follows The Committee of Publication Ethics (COPE) guideline. https://publicationethics.org.

REFERENCES

[1] J. Kaur and K.R. Ramkumar, "The recent trends in cyber security: A review," *Journal of King Saud University-Computer and Information Sciences*, vol. 34, no. 8, pp. 5766-5781, 2022. DOI: https://doi.org/10.1016/j.jksuci.2021.01.018

[2] K. Sudar and V. Muneeswaran, "Analysis of cyberattacks and its detection mechanisms," *Fifth International Conference on Research in Computational Intelligence and Communication Networks*, pp. 12-16, 2020. DOI: https://doi.org/10.1109/ICRCICN50933.2020.9296178

[3] J. Curtis and G. Oxburgh, "Understanding cybercrime in real world policing and law enforcement," *The Police Journal*, vol. 4, no. 96, pp. 573-592, 2023. DOI: https://doi.org/10.1177/0032258X221107584

[4] M.V. Pawar and J. Anuradha, "Network security and types of attacks in network," *Procedia Computer Science*, vol. 48, pp. 503-506, 2015. DOI: https://doi.org/10.1016/j.procs.2015.04.126

[5] M.S. Elsayed, N.A. Le-Khac, S. Dev and A.D. Jurcut, "DDoSNet: A deep-learning model for detecting network attacks," *IEEE 21st International Symposium on A World of Wireless, Mobile and Multimedia Networks*, pp. 391-396, 2020. DOI: https://doi.org/10.1109/WoWMoM49955.2020.00072

[6] A.B. Dehkordi, M.R. Soltanaghaei, and F.Z. Boroujeni, "The DDoS attacks detection through machine learning and statistical methods in SDN," *Journal of Supercomputing*, vol. 77, no. 3, pp. 2383-2415, 2021. DOI: https://doi.org/10.1007/s11227-020-03323-w

[7] K.B. Adedeji, A.M. Abu-Mahfouz, and A.M. Kurien, "DDoS attack and detection methods in internet-enabled networks: Concept, research perspectives, and challenges," *Journal of Sensor and Actuator Networks*, vol. 12, no. 4, pp. 51, 2023. DOI: https://doi.org/10.3390/jsan12040051

[8] V. Choudhary and S. Tanwar, "Generation & evaluation of datasets for anomaly-based intrusion detection systems in IoT environments," *Multimedia Tools and Applications*, pp. 1-25, 2024. DOI: https://doi.org/10.1007/s11042-024-19066-2

[9] B. Agarwal and N. Mittal, "Hybrid approach for detection of anomaly network traffic using data mining techniques," *Procedia Technology*, vol. 6, pp. 996-1003, 2012. DOI: https://doi.org/10.1016/j.protcy.2012.10.121

[10] A.R. Wani, Q.P. Rana, U. Saxena and N. Pandey, "Analysis and detection of DDoS attacks on cloud computing environment using machine learning techniques," *Amity International Conference on Artificial Intelligence*, pp. 870-875, 2019. DOI: https://doi.org/10.1109/AICAI.2019.8701238

[11] Z. He, T. Zhang and R.B. Lee, "Machine learning based DDoS attack detection from source side in cloud," *IEEE 4th International Conference on Cyber Security and Cloud Computing*, pp. 114-120, 2017. DOI: https://doi.org/10.1109/CSCloud.2017.58

[12] D. Kapetanovic, G. Zheng and F. Rusek, "Physical layer security for massive MIMO: An overview on passive eavesdropping and active attacks," *IEEE Communications Magazine*, vol. 53, no. 6, pp. 21-27, 2015. DOI: https://doi.org/10.1109/MCOM.2015.7120012

[13] M. Keerthika and D. Shanmugapriya, "Wireless sensor networks: Active and passive attacks-vulnerabilities and countermeasures," *Global Transitions Proceedings*, vol. 2, no. 2, pp. 362-367, 2021. DOI: https://doi.org/10.1016/j.gltp.2021.08.045

[14] J. Ahmed and Q. Tushar, "COVID-19 pandemic: A new era of cyber security threat and holistic approach to overcome," *IEEE Asia-Pacific Conference on Computer Science and Data Engineering*, pp. 1-5, 2020. DOI: https://doi.org/10.1109/CSDE50874.2020.9411533

[15] 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.11, pp. 106733-106748, 2023. DOI: https://doi.org/10.1109/ACCESS.2023.3319214

[16] A. Singh and B.B. Gupta, "Distributed Denial-of-Service (DDoS) attacks and defense mechanisms in various web-enabled computing platforms: issues, challenges, and future research directions," *International Journal on Semantic Web and Information Systems*, vol. 18, no. 1, pp. 1-43, 2022. DOI: https://doi.org/10.4018/IJSWIS.297143

[17] R. Vishwakarma and A.K. Jain, "A survey of DDoS attacking techniques and defence mechanisms in the IoT network," *Telecommunication Systems*, vol.73, no.1, pp.3-25, 2020. DOI: https://doi.org/10.1007/s11235-019-00599-z

[18] W. Guo, J. Xu, Y. Pei, L. Yin, C. Jiang and N. Ge, "A distributed collaborative entrance defense framework against DDoS attacks on satellite internet," *IEEE Internet of Things Journal*, vol. 9, no. 17, pp. 15497-15510, 2022. DOI: https://doi.org/10.1109/JIOT.2022.3176121

[19] A. Gaurav, B. B. Gupta, W. Alhalabi, A. Visvizi and Y. Asiri, "A comprehensive survey on DDoS attacks on various intelligent systems and its defense techniques," *International Journal of Intelligent Systems*, vol. 37, no. 12, pp. 11407-11431, 2022. DOI: https://doi.org/10.1002/int.23048

[20] S. Potluri, M. Mangla, S. Satpathy and S. N. Mohanty, "Detection and prevention mechanisms for DDoS attack in cloud computing environment," *11th International Conference on Computing, Communication and Networking-Technologies*, pp.1-6, 2022. DOI: https://doi.org/10.1109/ICCCNT49239.2020.9225396

[21] Y.F. Hsu, A. Ryusei and M. Matsuoko, "Real network DDoS Pattern Analysis and Detection," *IEEE 46th Annual Computers, Software, and Applications Conference*, pp. 1489-1494, 2022. DOI: https://doi.org/10.1109/COMPSAC54236.2022.00236

[22] M.Z. Shafiq, L. Ji, A.X. Liu, J. Pang and J. Wang, "Large-scale measurement and characterization of cellular machine-to-machine traffic," *IEEE/ACM Transactions on Networking*, vol. 21, no. 6, pp. 1960-1973, 2013. DOI: https://doi.org/10.1109/TNET.2013.2256431

[23] A.L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, pp. 1153-1176, 2015. DOI: https://doi.org/10.1109/COMST.2015.2494502

[24] 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. DOI: https://doi.org/10.1109/ACCESS.2020.3009733

[25] V. Gaur and R. Kumar, "Analysis of machine learning classifiers for early detection of DDoS attacks on IoT devices,"

Arabian Journal for Science and Engineering, vol.47, pp.1353-1374, 2022.
DOI: https://doi.org/10.1007/s13369-021-05947-3

[26] T.K. Moon, "The expectation-maximization algorithm," *IEEE Signal Processing Magazine*, vol. 13, no. 6, pp. 47-60, 1996.
DOI: https://doi.org/10.1109/79.543975

[27] A. Aldweesh, A. Derhab and A.Z. Emam, "Deep learning approaches for anomaly-based intrusion detection systems: A survey, taxonomy, and open issues," *Knowledge-Based Systems*, vol. 189, pp. 105124, 2020.
DOI: https://doi.org/10.1016/j.knosys.2019.105124

[28] Z. Fatehi and A. Montazerolghaem, "DDoS Detection in SDN using Deep Learning," *8th International Conference on Smart Cities, Internet of Things and Applications*, pp. 201-206, 2024.
DOI: https://doi.org/10.1109/SCIoT62588.2024.10570129

[29] M. Mittal, K. Kumar and S. Behal, "Deep learning approaches for detecting DDoS attacks: A systematic review," *Soft Computing*, vol. 27, pp. 13039-13075, 2023.
DOI: https://doi.org/10.1007/s00500-021-06608-1

[30] K. Chen, S. Zhang, Z. Li, Y. Zhang, Q. Deng, S. Ray and Y. Jin, "Internet-of-things security and vulnerabilities: Taxonomy, challenges, and practice," *Journal of Hardware and Systems Security*, vol. 2, pp. 97-110, 2018.
DOI: https://doi.org/10.1007/s41635-017-0029-7

[31] J. C. Reed and N. Dunaway, "Cyberbiosecurity implications for the laboratory of the future," *Frontiers in Bioengineering and Biotechnology*, vol. 7, no. 182, 2019.
DOI: https://doi.org/10.3389/fbioe.2019.00182

[32] J. Gubbi, R. Buyya, S. Marusic and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Generation Computer Systems*, vol. 29, no. 7, pp. 1645-1660, 2013.
DOI: https://doi.org/10.1016/j.future.2013.01.010

[33] J. H. Lee and H. Kim, "Security and privacy challenges in the Internet of Things [Security and privacy matters]," *IEEE Consumer Electronics Magazine*, vol. 6, no. 3, pp. 134-136, 2017.
DOI: https://doi.org/10.1109/MCE.2017.2685019

[34] D. Kreutz, F.M.V. Ramos, P.E. Verissimo, C.E. Rothenberg, S. Azodolmolky and S. Uhlig, "Software-defined networking: A comprehensive survey," *Proceedings of the IEEE*, vol. 103, no. 1, pp. 14-76, 2014.
DOI: https://doi.org/10.1109/JPROC.2014.2371999

[35] B. Wang, Y. Zheng, W. Lou and Y. T. Hou, "DDoS attack protection in the era of cloud computing and software-defined networking," *Computer Networks*, vol. 81, pp. 308-319, 2015.
DOI: https://doi.org/10.1016/j.comnet.2015.02.026

[36] S. Sezer, S. Scott-Hayward, P.K. Chouhan, B. Fraser, D. Lake, J. Finnegan, N. Viljoen, M. Miller and N. Rao, "Are we ready for SDN? Implementation challenges for software-defined networks," *IEEE Communications Magazine*, vol. 51, no. 7, pp. 36-43, 2013.
DOI: https://doi.org/10.1109/MCOM.2013.6553676

[37] S. Scott-Hayward, G. O'Callaghan and S. Sezer, "SDN security: A survey," *IEEE SDN for Future Networks and Services*, pp. 1-7, 2013.
DOI: https://doi.org/10.1109/SDN4FNS.2013.6702553

[38] A.A. Alashhab, M.S. Zahid, B. Isyaku, A.A. Elnour, W. Nagmeldin, A. Abdelmaboud, T.A.A. Abdullah and U. D. Maiwada, "Enhancing DDoS attack detection and mitigation in SDN using an ensemble online machine learning model," *IEEE Access*, vol. 12, pp. 51630-51649, 2024.
DOI: https://doi.org/10.1109/ACCESS.2024.3384398

[39] Y.W. Chen, J.P. Sheu, Y.C. Kuo and N.V. Cuong, "Design and implementation of IoT DDoS attacks detection system based on machine learning," *European Conference on Networks and Communications*, pp. 122-127, 2020.
DOI: https://doi.org/10.1109/EuCNC48522.2020.9200909

[40] P.M. Prajapati, P.P. Gandhi and S. Degadwala, "Exploring methods of mitigation against DDoS attack in an IoT network," *International Conference on Inventive Computation Technologies*, pp.1373-1377, 2024.
DOI: https://doi.org/10.1109/ICICT60155.2024.10544424

[41] V. Gaur and R. Kumar, "Analysis of machine learning classifiers for early detection of DDoS attacks on IoT devices," *Arabian Journal for Science and Engineering*, vol. 47, pp. 1353-1374, 2022.
DOI: https://doi.org/10.1007/s13369-021-05947-3

[42] S. Karnani and H.K. Shakya, "Mitigation strategies for Distributed Denial of Dervice (DDoS) in SDN: A survey and taxonomy," *Information Security Journal: A Global Perspective*, vol. 32, no. 6, pp. 444-468, 2023.
DOI: https://doi.org/10.1080/19393555.2022.2111004

[43] M. Ge, N.F. Syed, X. Fu, Z. Baig and A. Robles-Kelly, "Towards a deep learning-driven intrusion detection approach for Internet of Things," *Computer Networks*, vol. 186, pp. 107784, 2021.
DOI: https://doi.org/10.1016/j.comnet.2020.107784

[44] M. Cherian and S. L. Varma, "Secure SDN–IoT framework for DDoS attack detection using deep learning and counter-based approach," *Journal of Network and Systems Management*, vol. 31, no. 54, 2023.
DOI: https://doi.org/10.1007/s10922-023-09749-w