 http://dx.doi.org/10.14500/aro.12210

Enhancing Network Security: A Review of Machine Learning Techniques for Detecting TCP SYN Flood Attacks

Soran A. Hamad† and Kayhan Z. Ghafoor

Department of Information and Communication Technology Engineering, Erbil Polytechnic University, Erbil, Kurdistan Region – F.R. Iraq

***Abstract*—Distributed denial of service (DDoS) attacks are a significant danger to network security, with SYN flood assaults being particularly known for exploiting the transmission control protocol (TCP) handshake to deplete server resources. This review paper analyzes the current research on classifying DDoS attacks using machine learning (ML) approaches, with a focus on SYN flood scenarios. Traditional algorithms such as XGBoost, Random Forest, and k-Nearest Neighbors are examined alongside modern deep learning methods such as convolutional neural networks and long short-term memory networks. Deep learning, noted for its capacity to automatically learn complex properties from data, is particularly effective in dynamic contexts like the internet of things. The review analyzes the usefulness of various strategies, obstacles in feature engineering and model training, and their implications for real-time detection. This study presents a comprehensive overview of the accomplishments in employing ML and deep learning for TCP SYN flood attack classification and exposes gaps in the field that indicate options for further research.**

***Index Terms*—Anomaly detection, Distributed denial of service, Deep learning, Machine learning, Network security, Transmission control protocol SYN flood.**

I. Introduction

A distributed denial of service (DDoS) attack is a coordinated cyber offensive aiming at overwhelming a targeted server, network, or service with excessive traffic, thereby disrupting its normal operation. The attack method begins with the attacker identifying a target, which may be a business's online service, a vital infrastructure system, or a governmental website. To execute the attack, the attacker joins a botnet – a collection of compromised devices such as PCs, servers, or internet of things (IoT) devices that are infected with malware and controlled remotely (Echeverría, Pinilla and Mora 2024; Das, et al., 2022; Kanimozhi and Radhika, 2022). A common example of a DDoS attack is the SYN flood attack, which leverages a weakness in the transmission control protocol (TCP) handshake process.

In this attack, the attacker inundates the target server with a high volume of SYN requests, which are part of the TCP handshake to initiate a connection that can never be completed (Bhutani and Dash, 2024; Bhutani and Dash, 2024; Ravi and Shalinie, 2021). The server, after getting a flood of half-open connections, which utilize the server's resources, eventually becomes overwhelmed, unable to process legitimate users' requests, leading to service disruption. This causes the server to run out of resources and be unable to serve legitimate traffic.

SYN flood makes the attack capable of causing heavy operational costs with a number of highly visible attacks in history, including one where the Mirai Botnet was used to flood Dyn which has led to twitter, Netflix, and similar platforms being brought to their knees due to the SYN flood of over 600,000 devices p2p botnets tracking devices as illustrated in Fig. 1 (Hossain and Islam, 2024).

Think of it like a large birthday party you're organizing. You invite all your buddies to come over and they reply yes or no. Most of the time, a friend will text back, "Yes, I'm coming!" and you respond, "Wonderful, see you there!" Now, suppose there's a renegade youngster on the block hellbent on destroying your celebration. He continues to email you fake responses: "Yes, I'm coming!" but never shows up. He does it so many times that you lose track and can't remember who is coming. This manner seems tough to you to prepare the party, and some of your actual pals can get forgotten while you're busy managing all the bogus responses (Bhayo, et al., 2023; Sreeram and Vuppala, 2019).

Hence, in a similar fashion in the realm of computers, there is something called a TCP SYN flood assault. When computers wish to connect with each other, they send messages, such as sending parties or event invitations. When one computer sends a "Hello" message (a.k.a. a SYN message) to another computer, the second computer will answer with a "Hello back" (a SYN-ACK message). Then, the first computer says, "Thanks!" (ACK message), then they start conversing.

ARO-The Scientific Journal of Koya University
Vol. XIV, No. 1 (2026), Article ID: ARO.12210, 14 pages
DOI: 10.14500/aro.12210
Received: 17 April 2025; Accepted: 20 November 2025
Regular review paper; Published: 11 February 2026
†Corresponding author's e-mail: soran.hamad@epu.edu.iq

But a malicious computer (the attacker) can just submit plenty of affected "Hello" messages without finishing the discussion. This makes the good computer (the target) pause waiting for the "Thanks!" message that never comes which demonstrated in Fig. 2. A good computer waits so long for these bogus replies that it cannot communicate with true, crucial messages, just like you couldn't realistically arrange your party (Hwang, 2020; Nath Rimal and Praveen, 2020; Novaes, 2020; Sahi, et al., 2017).

DDoS attacks yield particularly serious repercussions in contemporary technological contexts such as IoT and IoV (internet of vehicles) (Syafiuddin, Mandala and Cahyani, 2023; Patel, et al., 2024; Singh, Jeong and Park, 2016) Zamrai, Yusof and Azizan, 2024). Average length: In the IoT ecosystem, there are millions of interconnected devices, ranging from smart home appliances to industrial sensors, which are usually installed with inadequate security.

Furthermore, in Fig. 3 when infected with malware, such devices can be incorporated into a botnet (Zamrai, et al., 2024; Hoque, Kashyap and Bhattacharyya, 2017). This massive amount of compromised IoT devices can be exploited by attackers to carry out huge-scale DDoS attacks. IoT devices such as the cameras or routers were hijacked and targeted to shut down key internet services in the 2016 Mirai botnet assault by producing huge volumes of traffic (Sharma and Kumar, 2017). This expanding use of IoT devices poses a severe concern in terms of security flaws that can be utilized to raise the magnitude of DDoS attacks.

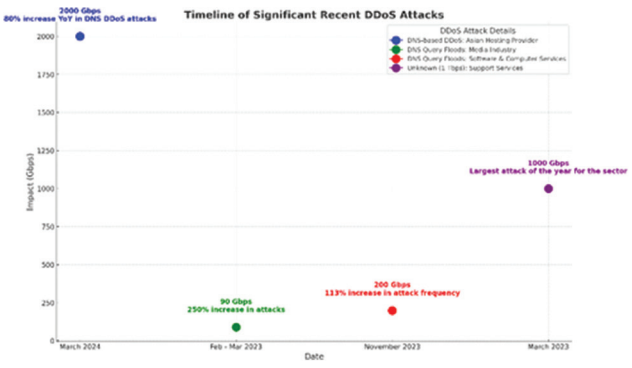

Fig. 1. Recent Distributed denial of service attack.

In the same manner, for the internet of vehicles (IoV) in which connected cars and smart transportation systems evolve, DDoS attacks can lead to disastrous consequences. Real-time traffic data, remote diagnostics, and other IoT features are enabling vehicles to become increasingly interconnected (Sambangi and Gondi, 2020a; Saif, Widyawan and Ferdiana, 2024; Saiyed and Al-Anbagi, 2024).

An effective DDoS attack on internet of vehicles infrastructure can damage communication channels between vehicles and traffic management services, which can result in disorderly traffic, compromised safety and even vehicle failure. These attacks may focus on vital building blocks of the smart transportation networks and result in huge interruptions and threats to public safety (Bamasag, et al., 2022; Dasari and Kaluri, 2024).

DDoS attacks can occur not only in classical network and server environments but also in diverse technology ecosystems featuring high degrees of interconnectedness and real-time dependence. It is why artificial intelligence (AI) and machine learning (ML) is increasingly integrated with cybersecurity defenses to help mitigate such attacks. AI-powered solutions improve the detection and response mechanisms to DDoS attacks by analyzing network traffic in real time, identifying patterns, and differentiating between normal and malicious traffic. ML algorithms can adapt to changing attack strategies by learning from historical data to improve detection accuracy and by automating responses (Zeeshan, et al., 2022).

Such technologies are crucial to protecting IoT networks, IoV systems, and other digital infrastructures against an ever-evolving threat landscape. New DDoS attacks show that they are becoming highly sophisticated.

For instance, Amazon Web Services in 2023 capped at 2.3 terabits per second (Tbsp.) (Dash, et al., 2024; Jaraba, et al., 2024), demonstrating advanced amplification techniques that can even submerge large-scale cloud service providers. The Mirai botnet attack is still the biggest case about how insecure IoT devices in homes, offices, and potentially even

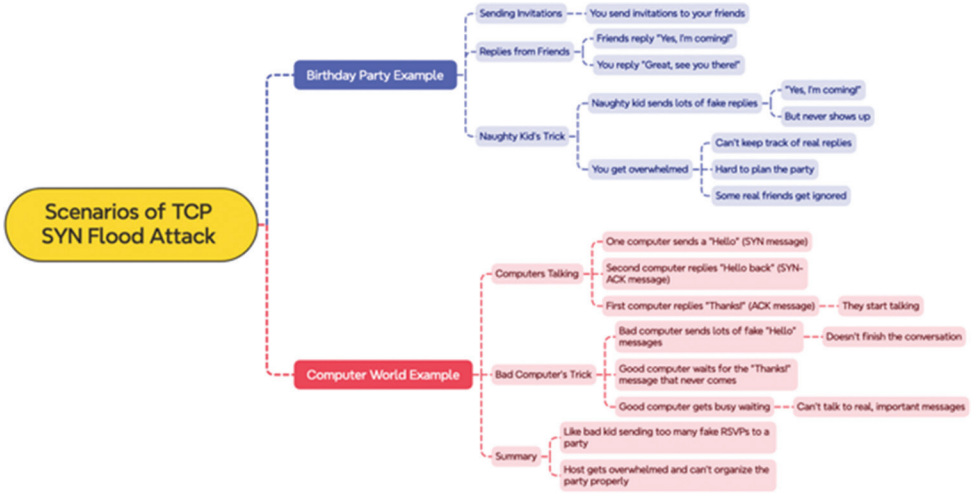

Fig. 2. Transmission control protocol SYN flood scenarios.

http://dx.doi.org/10.14500/aro.12210

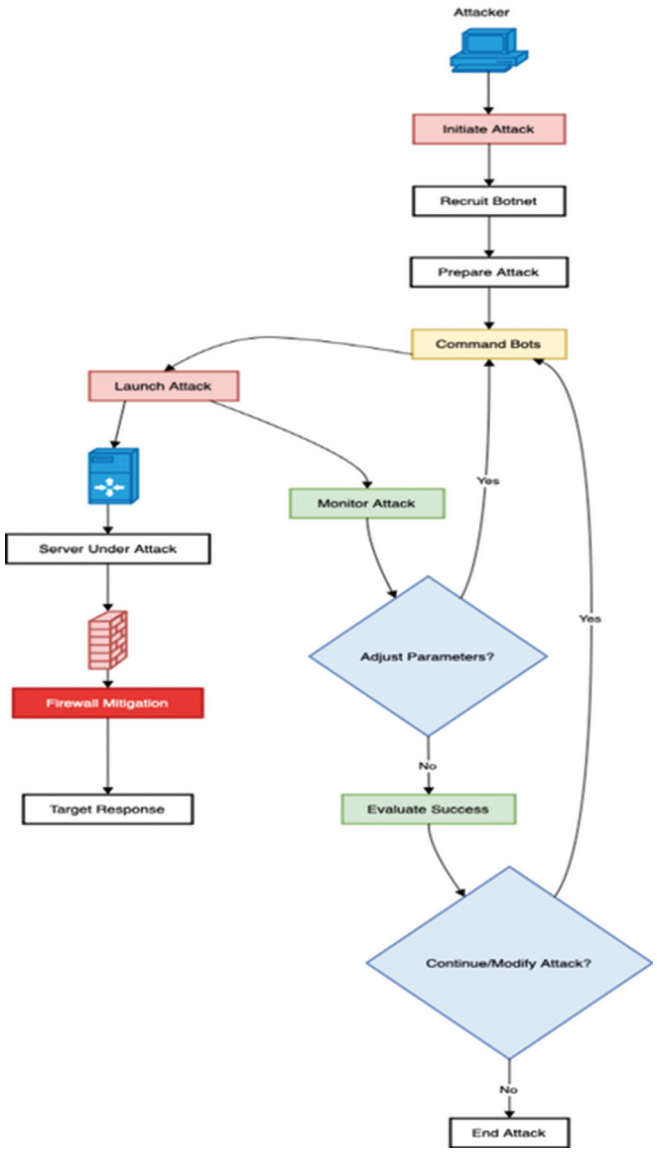

Fig. 3. Distributed denial of service attack workflow.

factories can be used to disrupt a large part of the internet (Hussain, et al., 2016; Ghafoor, 2022).

In the context of IoT and cloud environments, the studies indicate that SYN flood detection presents specific challenges, including limited power and resources in IoT devices and the large scale of cloud networks. In these scenarios, lightweight ML models are typically at the network edge to reduce latency and achieve better detection efficiency (Kreutz, et al., 2014; Pai and Bha, 2014; Meng, et al., 2017; Hsu, et al., 2021; Wang and Li, 2024).

ML's ability to learn and adjust in these environments allows for scalable and efficient detection systems that are especially useful in distributed networks, where traffic its real-time analysis is critical for preventing their attacks from consuming server resources and compromising the availability of the service. In most classes, researchers focus on the respective algorithm solutions to detect network attacks using proposed models even to real-time network traffic data (Bhayo, et al., 2023; Syafiuddin, Mandala and Cahyani, 2023). This emphasis on quick turnaround is especially important for mission-critical services, where interruption may incur significant business or operational impacts. Patterns can vary significantly, and attack vectors are often distributed.

With growing IoT and cloud infrastructures, detection techniques are advancing toward a strong defense with minimal resource usage. Another common theme is real-time mitigation, with several papers focusing on techniques for timely detection and response to SYN floods during their occurrence as described in Table I. Its real-time analysis is critical for preventing their attacks from consuming server resources and compromising the availability of the service. In most classes, researchers focus on the respective algorithm solutions to detect network attacks using proposed models even to real-time network traffic data (Zubaydi, Anbar and Wey, 2017; Haider, 2020; Dimolianis, Pavlidis and Maglaris, 2021a). This emphasis on quick turnaround is especially important for mission-critical services, where interruption may incur significant business or operational impacts.

II. State of the Art

There are many studies for detecting and mitigating DDoS attacks using ML techniques, specifically TCP SYN flood attacks, which are very threatening to network infrastructure. While working on ICMPv6-based DDoS attack detection using a modified flower pollination algorithm, innovative but only on ICMPv6 vectors, and workaround similar anomaly detection techniques may probably become efficient in TCP SYN flood detection as well (Feng, et al., 2023; Shao, et al., 2023; Saif, Widyawan and Ferdiana, 2024).

An additional systematic study was conducted on ML techniques for their implementation in Software Defined Few-shot learning that has been successfully applied to classifying attack traffic in IoT systems, which is important where there is only limited labeled data available to the user (i.e., TCP SYN flood) and its performance tends to degrade with larger datasets also (Liu, et al., 2023). Certain techniques have demonstrated suitability for network attacks prediction, such as ensemble classification, which has been performed for the prediction of botnet impact on IoT networks, with strong results at the cost of higher complexity and computational demand and combining multiple classifiers can improve TCP SYN flood detection (Bovenzi, et al., 2024).

In addition, DDoS attack classification based on both hierarchical ML and hyperparameter optimization performs well in managing wide-ranging attack patterns, but demand considerable computational resources (Gaurav, et al., 2021; Zhou, et al., 2022; Hossain and Islam, 2024), hence making this approach compatible with TCP SYN flood detection. Moreover, in Table II, the combination of analytics and ML in big data helps to analyze a large amount of network data and improves DDoS detection accuracy, and this is an advantage that applies to TCP SYN flood detection as well (Hassan and Daneshwar, 2022; Javadpour and Wang,

TABLE I
Related Survey of TCP Sync Flood

References	Focus on TCP SYN flood attacks	Machine learning for detection	SDN integration	IoT and cloud environments	Real-time mitigation	High-speed network adaptation
Aighuraibawi et al., 2023	√	√	X	√	√	X
Ali et al., 2023	√	√	√	√	X	√
Bhayo et al., 2023	√	√	√	X	√	X
Bovenzi et al., 2024	√	√	X	X	√	√
Chandana Swathi et al., 2024	√	√	√	√	X	X
Dasari and Kaluri, 2024	√	X	X	√	√	√
Dash et al., 2024	√	√	X	√	X	√
Doshi, Apthorpe and Feamster, 2018	√	√	√	X	√	X
Feng et al., 2023	√	√	X	√	√	X
Gaurav et al., 2021	√	√	√	X	√	X
Hasan et al., 2023	√	√	X	√	√	X
Hossain and Islam, 2024	√	√	X	√	X	X
Ismail et al., 2022	√	√	√	X	√	√
Jaraba et al., 2024	√	√	X	√	X	√
Javanmardi et al., 2024	√	√	√	√	X	X
Kim, Hakak and Ghorbani, 2024	√	√	√	X	√	X
Kumari and Jain, 2023	√	√	X	√	X	X
Nadeem et al., 2022	√	√	X	√	√	√
Nath Rimal and Praveen, 2020	√	√	√	X	√	X
Naveen and Manu, 2019	√	√	√	√	√	X

TCP: Transmission control protocol, SDN: Software-defined networking, IoT: Internet of things

2022). DDoS vulnerabilities have been studied for smart grid applications, providing a wealth of information about potential attack vectors, though with a narrower focus which may still apply to TCP SYN floods (Sambangi and Gondi, 2020b; Bensaid, et al., 2024). Hybrid feature selection and ensemble classifiers achieve a balance between robustness and implementation complexity, which greatly increases TCP SYN flood detection performance by exploiting the combination of detection methods and appropriate feature selection (Bhutani and Dash, 2024).

While this framework needs to be modified, it reveals a solid detection method for TCP SYN floods among many others. Most of the reviewed papers prove that ML Classification and Prediction methods provide a solution that encompasses a wide range of DDoS attacks which can be easily tweaked to detect TCP SYN floods, but they typically have no real-time capability (Rawashdeh, Alkasassbeh and Al-Hawawreh, 2018). Reviews of existing DDoS solutions under software-defined networking (SDN) environments also provide meaningful insights for TCP SYN flood detection in SDN, even though these papers do not reflect novel methodologies (Jaafar, Abdullah and Ismail, 2019). Hence, the innovative IDS solution for DDoS UDP flooding attacks in IoT-Fog networks considered mobility and impersonation (two aspects that could be adapted over TCP SYN flood attacks (Cui, et al., 2019; Dasari and Devarakonda, 2022; Wang, Lu and Qin, 2022; Kumari and Jain, 2023)).

Integrating the reviewed papers above Paragraphs present a summary of significant results from various researchers and discuss their methodologies, strengths, and weaknesses and link with detection of TCP SYN flood attacks. For traffic classification with regularization techniques especially TCP SYN flood (Hong et al., 2017; Özçam, Kilinc and Zaim, 2021; Ramadhani et al., 2025), DDoS vulnerabilities have been studied for smart grid applications, providing a wealth of information about potential attack vectors and defense strategies that can inform TCP SYN flood mitigation as well. Moreover, a comprehensive approach for accurately detecting TCP SYN flood attacks is offered because support vector machines (SVMs) can deal with high-dimensional spaces and distinct class segregation but only learn something for complexes patterns. For a scenario like big-data and complex pattern, you require advanced deep-learning techniques like Neural Networks which have a substantial computational cost. Even more, just applying the hybrid of different models can further improve the detection as we can use the benefits of another algorithm.

Hence, we started with Random Forest approach to see how good it was against other models as a threshold detection mechanism, and we tweaked XGBoost hyperparameters to better our detection at some computational complexity cost and deep diving. Relatedly, the reviewed studies provide a holistic snapshot of the landscape of ML today mechanisms of DDoS detection and mitigation, almost all provide unique applications. All these contributions together lead to improved knowledge and solutions to fighting against DDoS attacks, particularly SYN flood attacks from anywhere in network ecosystem.

TABLE II
Overview of Related Papers in TCP Sync Flood Detection

References	Objective	Methodology	Strength	Weakness	Key focus
Aighuraibawi, et al. (2023)	Detect ICMPv6-based DDoS attacks using a modified flower pollination algorithm	Modified flower pollination algorithm for anomaly detection	Innovative approach using nature-inspired algorithms	Limited scope to ICMPv6; might not handle all attack vectors	Anomaly detection in network traffic
Ali, et al. (2023)	Review ML techniques for DDoS detection in SDN	Systematic review of existing literature	Comprehensive overview of various techniques	Lack of original experimentation	Systematic review of ML in SDN
Bhayo, et al. (2023)	Develop a ML -based framework for DDoS detection in SD-IoT networks	Framework development with ML techniques	Focus on IoT-specific network environments	May require adaptation for other network types	DDoS detection in IoT environments
Bovenzi, et al. (2024)	Classify attack traffic in IoT environments using few-shot learning	Few-shot learning for classification	Use of few-shot learning for limited data	Performance may vary with larger datasets	Classification of attack traffic in IoT
Chandana Swathi, Kishor Kumar and Siva Kumar (2024)	Predict botnet impact on IoT networks using ensemble classification	Ensemble classification techniques	Strong performance with ensemble methods	Potential complexity and computational cost	Botnet detection and impact prediction
Dasari and Kaluri (2024)	Classify DDoS attacks using hierarchical ML and hyperparameter optimization	Hierarchical ML and optimization techniques	Effective use of hierarchical methods	Computationally intensive	DDoS attack classification with optimization
Dash, et al. (2024)	Enhance DDoS detection in IoT using PCA	Principal Component Analysis (PCA) for feature reduction	Use of dimensionality reduction to improve detection	PCA may lose important features	Feature reduction and detection enhancement
Doshi, Apthorpe and Feamster (2018)	Detect DDoS attacks in IoT devices using ML	ML techniques for detection	Practical application to consumer IoT	Limited to consumer devices	DDoS detection in consumer IoT
Feng, et al. (2023)	Collaborative DDoS detection using reinforcement learning	Reinforcement learning at the edge	Innovative use of reinforcement learning	Complexity in implementation	Stealthy DDoS detection in IoT
Gaurav, et al. (2021)	Detect DDoS attacks using big data and ML	Big data analytics combined with ML	Utilizes big data for improved accuracy	Potential challenges with real-time processing	Big data and ML for DDoS detection
Hasan, et al. (2023)	Analyze DDoS vulnerabilities in smart grid applications	Analysis of vulnerabilities and recent developments	In-depth analysis of smart grid security	Narrow focus on smart grid applications	DDoS vulnerabilities in smart grids
Hossain and Islam (2024)	Enhance DDoS detection with hybrid feature selection and ensemble classifiers	Hybrid feature selection and ensemble-based classifiers	Combines multiple techniques for robustness	Implementation complexity	Hybrid feature selection and ensemble classifiers
Ismail, et al. (2022)	Classify and predict DDoS attacks using ML	ML classification and prediction	Comprehensive classification and prediction	May not address real-time detection	Classification and prediction of DDoS attacks
Jaraba, et al. (2024)	Explore solutions for DDoS attacks in SDN environments	Review of current solutions for SDN	Provides an overview of current solutions	Limited to existing solutions	DDoS solutions in SDN environments
Javanmardi, et al. (2024)	IDS for DDoS UDP flooding in IoT-Fog networks	Mobility and impersonation-aware IDS	Innovative approach considering mobility	Specific to UDP flooding attacks	IDS for IoT-Fog networks and UDP flooding
Kim, Hakak and Ghorbani (2024)	Detect false authentications due to DDoS in EV charging infrastructure	Detection techniques for false authentications	Focused approach on a specific infrastructure	Narrow application scope	Detection of false authentications in EV infrastructure
Kumari and Jain (2023)	Study DDoS attacks over IoT networks and countermeasures	Comprehensive study and review of countermeasures	Broad review of countermeasures	Limited to review and not original research	DDoS attacks and countermeasures in IoT
Nadeem, et al. (2022)	Detect DDoS attacks in SDN using ML	ML techniques for SDN	Application of ML in SDN	Specific to SDN networks	DDoS detection in SDN environments
Nath Rimal and Praveen (2020)	Discuss various aspects of DDoS attacks and their detection	Overview and discussion of DDoS attacks	Broad overview of issues	Lack of novel contributions	General overview of DDoS attacks
Naveen and Manu (2019)	Detect DDoS attacks using ML techniques	Application of ML to detect DDoS	Practical application of ML techniques	Potential data limitations	ML for DDoS attack detection
Zhou, et al. (2022)	Explainable meta-learning for DDoS detection	Meta-learning with explainability focus	Focus on explainability and meta-learning	Complexity in model interpretation	Explainable meta-learning for DDoS detection

DDoS: Distributed denial of service, TCP: Transmission control protocol, SDN: Software-defined networking, IoT: Internet of things, ML: Machine learning

III. Leveraging ML Techniques for TCP SYN Flood Attack Detection

Because ML techniques are effective in analyzing large amounts of network data and finding malicious patterns, they have been widely used in the detection of DDoS attacks such as SYN flood attacks (Sahi, et al., 2017; Magnani, Doriguzzi-Corin and Siracusa, 2023). Broadly, these techniques can be grouped into supervised learning, unsupervised learning, deep learning and hybrid models, and nature inspired and optimization methods, of which each has its own strengths and application.

Different supervised learning techniques, including SVM, Decision Trees, and Random Forests, are successful at DDoS detection. Such algorithms learn how to classify new data as normal or malicious based on known attack patterns available in labeled data (Tuyen, et al., 2022). In particular, SVMs are very well suited for problems of binary classification, whereas Decision Trees are fairly easy to implement and provide interpretability. As they are an ensemble method, Random Forests leverage multiple decision trees to improve the robustness of the analysis when there is high dimensional data to be analyzed in network traffic.

In situations where the patterns of attacks are known, and the datasets are labeled supervised learning models are preferred to be used and thus provide high accuracy in spotting known threats (Javanmardi, et al., 2024). For detection of novel or unknown attacks, clustering, such as (K) means, and anomaly detection are two unsupervised learning techniques. These methods do not require any labeled data, which are useful in cases that we cannot obtain labeled training dataset. Similar data points get grouped together by clustering algorithms, whereas anomaly detection techniques try to identify data points that differ very much from the norm and may be an attack (Jr, Tavares and Nogueira, 2023).

Interestingly, though these approaches have lower accuracy than supervised methods, they are also typically less interpretable, making them better suited to environments where attack patterns are themselves not well understood or quickly evolving.

IV. ML For Real-Time Mitigation in SDN and IOT Networks

All the recent survey papers on TCP SYN flood detection together present the enhancement which ML applications have brought into concurrently with a special emphasis on niche areas such as SDN and IoT and cloud environments (Tuan, et al., 2020; Sharma, et al., 2020). These studies show that TCP SYN flood attack is still relevant among the other DDoS attack types, which misuse the holes in TCP three-way handshake to exhaust network resources and inundate services with half-open connections.

Every paper reveals that ML is a potential solution for detection, to improve the detection rate the papers use several ML models including SVM, Decision Trees, and ensemble methods (Bovenzi, et al., 2024; Chandana Swathi, Kishor Kumar and Siva Kumar, 2024). Here, sync is particularly suitable to be applied in situations where new attack pattern or types of attack are not yet known but the attacks detected are known a prior and there is labeled data available for classification of SYN flood traffic only, but deep learning models on the other hand are adept at managing large scale data efficiently and can be seamlessly integrated into the network's control plane. This enables the possibility to monitor and respond to SYN Flood attacks in a much broader and efficiently since the SDN controller can use the ML algorithms to adapt the traffic flow effectively, for example, a paper can show how an ML model was implemented as a lightweight model to improve the detection attacks and mitigate threats in an IoT setting (Dimolianis, et al., 2022; Patel, Anagha and Santhosh Kumar, 2024). One interesting fact of these surveys is that most of them are conducted on the SDN technology that offers centralized control and dynamic traffic management. SDN provides tools for centralized management of the network, for real-time, control and optimization of the flows MDL models can detect and counteract SYN flood attacks with precision. SDN also provided the capability to filter or reroute the traffic based on an analysis of the current situation that is more advantageous than flooding the data center with numerous shuttling requests. Through integration with these capabilities of SDN, these studies seek to use enhanced time and accuracy of attack detection so that service interruption is reduced (Alasadi, et al., 2024; Aggarwal et al., 2025).

V. ML Applications in TCP SYN Flood Detection

It found that ML has been applied preferably in IoT and SDN scenarios as both settings have their own set of challenges and benefits (Chicco and Jurman, 2020; Swami, Dave and Ranga, 2021; Dash, et al., 2024). Being a complex field, IoT networks comprise a wide range of devices with limited resources.

The developed ML model must be lightweight and efficient for real-time detection without overwhelming the system. The usage of surveillance techniques such as anomaly detection and clustering is used to alert traffic patterns and findings that can make SYN flood attacks unfathomable, even for devices with constrained resources. In contrast, SDN has a central controller architecture which is suitable for ML (Pari, et al., 2023).

VI. Lessons Learned

ML has been incorporated in the DDoS detection systems and the results that have been obtained include the following advantages and disadvantages. One important lesson that can be learnt from such cases as the department of energy DDoS attack is that interruptions can be experienced even if full outages are not present, and they will severely affect operations. This points to the fact that early detection and quick action are mandatory for organizations and particularly in businesses with significant infrastructure. Furthermore, systems should be constantly patched and updated to avoid the weaknesses to be exploited in DDoS attacks (Bawany, Shamsi and Salah, 2017). However, the quality and representativeness of training data also greatly define the performance of the ML models (Ismail, et al., 2022; Sahosh, et al., 2024).

An important strong point of ML systems is that they learn patterns as per the training data and when the training data are not rich or diverse, the model will not be able to identify an attack that is out of the trained-on data set. This is even more challenging when it comes to DDoS because the attacker is always looking for new ways to subvert the defense.

For instance, a model trained on data from the attack vector such as SYN flood will underperform when handling multi-

vector attack that for instance includes UDP amplification or DNS reflection (Hossain and Islam, 2024). In addition, there could be more serious consequences in the case that the training set provided is inadequate in that overfitting of the mode could occur whereby it is over tuned to specific traffic patterns that are present in the training set but will not hold true for unseen traffic patterns (Sudar and Deepalakshmi, 2020b; Kim, Hakak and Ghorbani, 2024).

Furthermore, an inadequate training set could lead to overfitting, where the model is too finely tuned to the specific patterns in the training data, resulting in poor generalization to unseen traffic patterns. However, one main issue is that ML models require updates periodically and training to improve the model's accuracy. Static models closely reflect older attack approaches but do not address evolving network defense threats due to emergent attack types. A model trained using data from 2 years ago will not detect a low-and-slow DDoS attack which occurs when the perpetrator uses a small number of packets with a low rate and over a very extended period (Nath Rimal and Praveen, 2020; Deb, Rodrigo and Kumar, 2024).

A second lesson is that ML models will need to be incorporated into open frameworks to provide security (Jr, Tavares and Nogueira, 2023). ML models can be used to automate much of the detection process, but network traffic is too complex and too unpredictable to rely exclusively on automation or the human mind alone. Powerful, purely automated systems might not be able to fully understand the context that rests behind some traffic patterns.

VII. Survey and Comparative Analysis

The present section is devoted specifically to the rather recent DDoS SYN flood attacks and uses ML approaches to improve identification and counteraction. Available from industry reports and other threat intelligence sources, the study identified common trends that were highlighted in the preliminary findings, including the increase in scale and sophistication of attacks such as DNS amplification and HTTP/2 Continuation Floods.

Consequently, strengths and challenges in current detection methods using supervised learning, deep learning, and other hybrid approaches are evaluated that mentioned in Fig. 4.

The chronology of notable recent attacks serves background information that explains the development of

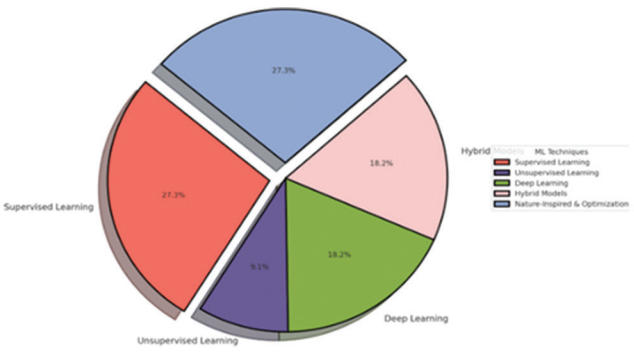

Fig. 4. SYNK flood detection algorithms.

DDoS threats and the necessity of progressive and intelligent protection tools. Linear models are predominant in DDoS detection research, particularly supervised learning, which would be highly suitable for well-labeled datasets since they achieve high proximity accuracy and low interpretability.

The chart reflects the dominance of supervised learning in DDoS detection research, likely due to its balance of accuracy and interpretability when working with well-labeled datasets. Deep learning also has a noteworthy part here due to handling complex data and feature extraction of relevant characteristics, which means deep learning is appropriate for more complex detections. H_1 arising from the lower counts of unsupervised learning and hybrid models indicates that these techniques are utilized in more specific scenarios, particularly with limited labeled data and application of the approach across several attack types. Nature-inspired and optimization techniques are applied selectively to more focused, novel applications, thereby illustrating their utilization in enhancing and fine-tuning detectors, as shown in Fig. 5.

The chosen results demonstrate that although supervised methods are preferred due to their applicability and efficiency, there is a trend toward using more sophisticated techniques, such as deep learning and solving nature-inspired algorithms for enhanced and sophisticated detection tasks.

VIII. Recent DDOS Attack Trends (2023–2024)

According to the latest reports from cybersecurity firms such as Cloudflare, Netscout, and Akamai (Sahosh, et al. 2024; Tang, et al., 2023), here are some key trends:

A. Increase in Sophisticated DDoS Attacks

The scale and complexity of DDoS attacks have increased, with multi-vector attacks combining multiple protocols (e.g., SYN flood, UDP amplification, and HTTP floods) becoming more common.

B. DNS and HTTP/2 Attacks

DNS amplification remains one of the most popular vectors, whereas HTTP/2 vulnerabilities have been exploited in recent high-profile attacks, with large-scale campaigns observed in 2023 and 2024.

C. Targeted Industries

The gaming, financial services, and telecommunications sectors have been among the most targeted industries in 2024. Attackers often use DDoS attacks as a precursor to more sophisticated intrusions.

D. Geopolitical Motivations

DDoS attacks have increasingly been linked to geopolitical tensions, with state-sponsored actors targeting critical infrastructure and government websites.

E. ML in Detection

ML techniques are being increasingly adopted for anomaly detection and threat prediction in real-time, improving the speed and accuracy of DDoS mitigation efforts.

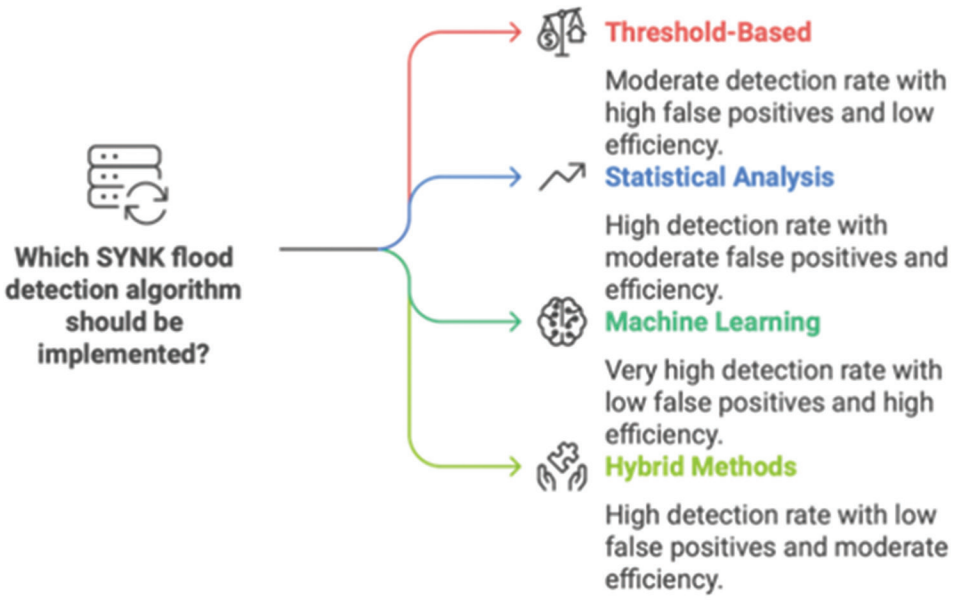

Fig. 5. Distribution of machine learning techniques in distributed denial of service attack detection.

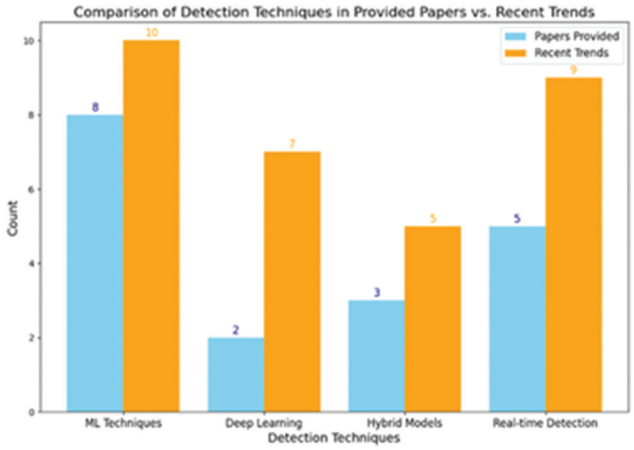

Fig. 6. Machine learning models.

IX. Comparison With Reviewed Survey Papers

A. Detection Techniques

Emphasizing nature-inspired and ML-based detection techniques. These methods align with the current trend of using advanced algorithms for real-time anomaly detection, as seen in recent reports (Deshmukh and Devadkar, 2015; Hong, et al., 2017). However, recent reports suggest an increase in the complexity of attacks, which may require more robust and hybrid approaches, as shown in both Figs. 6 and 7. Furthermore, many studies provide a comprehensive review of ML techniques for DDoS detection, especially in SDN (Subashini, et al., 2022; Liu, et al., 2023; Bhutani and Dash, 2024). This is consistent with recent trends where SDN environments are increasingly being targeted, and ML is crucial for adaptive defense mechanisms.

B. Attack Vectors and Types

Individual classes of attacks such as the SYN flood attack and the UDP flooding attack. When such attacks still hold relevance, newer trends show that multi vector attack are now prevalent, and this implies that newer methodologies should consider this added advancement (Doshi, Apthorpe and Feamster, 2018).

C. Industry Focus

Exploration of the vulnerabilities of DDoS Tcp-sync flood attack on some of the limited structures such as smart grids and EV charging. New trends support their focal threats but suggest that these sectors may experience novel attacks over time (Mohammadi, Javidan and Conti, 2017).

D. ML Models

However, they also provided their work on ML models for the classification and prediction of DDoS attacks. Despite a rising trend in the approach of deep learning models in recent years, especially in high volume and complex attack cases, the researchers might give more emphasis on deep learning and compounding models in the future (Yang, et al., 2023; Hamad, 2022).

X. Research Challenges

Several challenges that impact the accuracy, speed, and reliability of real-time mitigation efforts in TCP SYN flood detection. One prominent challenge of real-time detection systems is managing high traffic volumes. In attacks such as TCP SYN flood, distinguishing legitimate spikes in traffic from malicious floods is difficult, especially when high-volume traffic floods detection systems. In addition, we need scalable techniques for feature extraction like streaming data preprocessing to identify, for example, SYN packet rates, and connection attempts as specific TCP SYN indicators. By integrating these techniques with high through put anomaly detection models, and prompt, accurate detection is achieved

http://dx.doi.org/10.14500/aro.12210

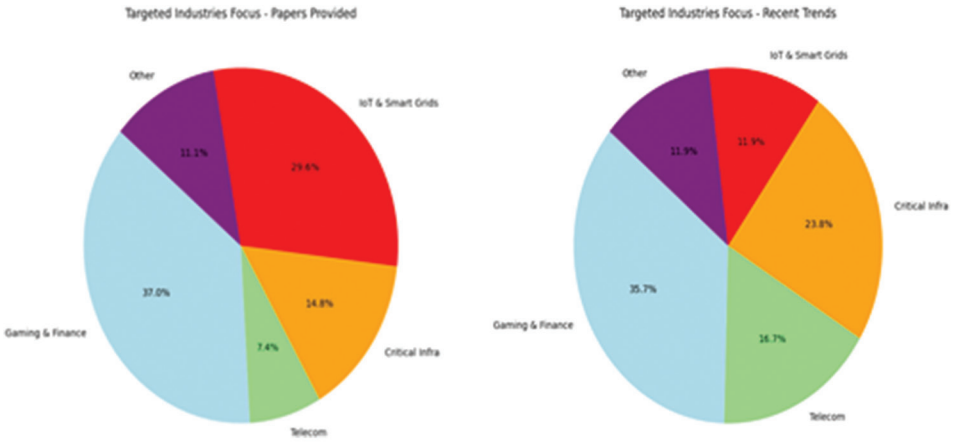

Fig. 7. Targeted industries.

without overloading the system (Bhutani and Dash, 2024; Sharma, et al., 2019).

A challenge here is that increasingly, attackers use multi-vector tactics – which combine TCP SYN flooding with other attacks, such as amplification or botnet-based DDoS – to evolve their attack patterns. For this, we require adaptive ML models that dynamically adapt to new data, thereby capable of real-time adaptation with changes in attack patterns. Reinforcement learning or hybrid models, combining ML and rule-based systems, increase resilience by giving the model the ability to recognize and respond to variations of emerging SYN flood attacks.

Detection and response delay is a vital issue, especially in the latency when beneath SYN flood attacks can fill the server with load and cause the service outages. This is solved by edge computing and automation deciding detection, allowing for decreased response times as the data are processed closer to the source.

On the parallel, automated responses such as IP blacklisting or SYN rate limiting further reduce latency and protect server resources from active attacks, but at the cost of still high levels of risk of false positives: Real-time systems erroneously identify legitimate traffic surges as SYN floods and disrupt business. Reducing false positives involves multi-layer verification mechanisms that take into consideration contextual factors, for example, known peak times. These explainable AI models form another layer of human oversight between service quality and the action taken by the model to ensure that legitimate users remain a priority (Kellerer, et al., 2021; Xiao, et al., 2022; Cai, et al., 2023; Singh, et al., 2023).

Multistep mitigation introduces additional complexity for more complex attacks since it requires perfect coordination without making the system overloaded or prone to configuration errors. Orchestrating mitigation steps such as IP filtering and session revalidation with orchestration tools allow these defenses to work without causing unintended service disruption while they are coordinated. Limited memory and processing power in IoT environments also in high-speed networks, giants in data volumes need to be processed, without trade off on speed and accuracy as scalable.

Detection systems can both maintain speed and accuracy through distributed processing frameworks (e.g., Apache Kafka) and load balanced processing. In high-speed networks, effective monitoring of network traffic can also be provided by methods of parallelized data processing, such as SYN flood detection on arrival of the traffic in heavy traffic loads.

Building trust in automated systems like that is difficult without ensuring interpretability of ML models that can produce false positives or mislead their users by action. Detection decisions occur in explainable AI approaches (such as SHAP or LIME) which provide insight as to why a certain packet is marked suspicious (Doshi, Apthorpe and Feamster, 2018; Rimal and Praveen, 2020; Bensaid, et al., 2023). This transparency also helps operators to review decisions, permitting confidence that, for example, automated responses, such as IP blocking, relate to justified and appropriate situations. Human-in-the-loop frameworks offer benefits considering the verification of important decisions, particularly where the false positives would damage the experience for users.

XI. Certain Challenges in Data Quality and Preprocessing in SYN Flood Detection are Mentioned Below

Talking about core challenges which demonstrated in Fig. 8 here along with data quality and preprocessing in the context of SYN flood detection. In particular, with data completeness and integrity issues, approaches for transforming and representing data, and the fundamental importance of well-designed feature engineering in this entire field. Investigating these challenges allows us to show how researchers and practitioners can improve the performance of detection systems and produce more complete, reliable results in the identification of SYN flood attacks (Sikos, 2020; Srinivasu, et al., 2021).

XII. 1- Data Completeness and Integrity

A. Missing Data

Many datasets have missing values which should be addressed when doing all we can to avoid negatively impacting

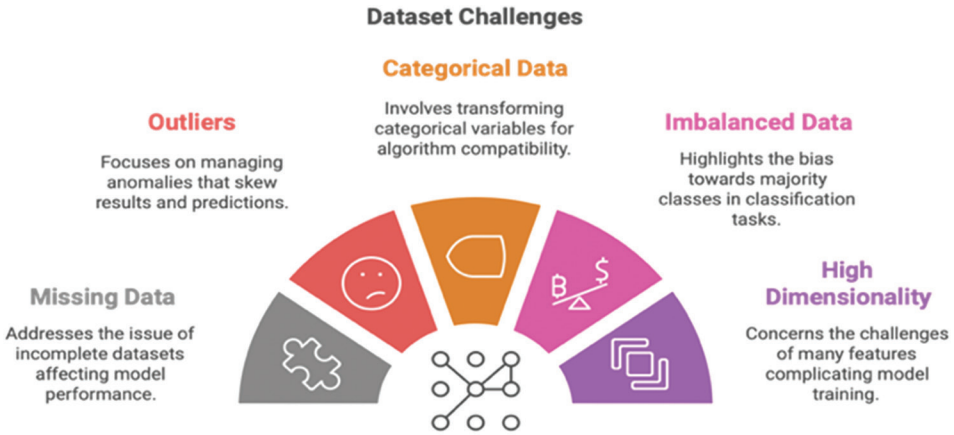

Fig. 8. Dataset challenges.

model performance. However, they may be reduced in impact by substituting with the mean or median, or by deleting incomplete records. In fact, the choice of an approach is determined by the type and severity of missing data (Mirmohseni, Tang and Javadpour, 2020; Hossain and Islam, 2024).

B. Outliers and Anomalies

Outliers (extreme values lying beyond indices of expected normal distributions) can distort statistical measures and incorrectly skew our prediction in cases such as SYN flood – detection where traffic anomalies are ubiquitous. Detecting and managing appropriate outliers is important to maintain integrity of data (robust scaling, outlier removal).

XIII. Data Representation and Transformation is

A. Categorical Data Encoding

But almost all the ML algorithms require numerical data as input, and they require categorical features to be coded in to a numerical format. Common transformations like one hot encoding/label encoding are applied, and model performance and interpretability are changed by the transformed method (Doshi, Apthorpe and Feamster, 2018; Javadpour, 2020).

B. Handling Imbalanced Data

The problem of class imbalance is also seen in SYN flood detection, where benign traffic is typically orders of magnitude greater than sampled attack. For instance, data sets with imbalanced class distribution may be learned easily, but models trained on that data may not generalize well across the minority class (attacks) and may even be overfit to the majority (healthy) class. Here, if dataset is balanced, you can try increasing accuracy over the classes by oversampling, under sampling, or generating say synthetic data by SMOTE (Naveen and Manu, 2019; Nadeem, et al., 2022).

XIV. Representative Datasets and Feature Engineering

A. Feature Engineering Technique

The feature engineering could be improved for SYN flood detection using subtle features such as SYN packet inter arrival, IP address diversity, or connection attempt sequency. More sophisticated modeling of attack characteristics improves model accuracy and resists evasion tactics (Javadpour, Wang and Rezaei, 2020; Sudar and Deepalakshmi, 2020a).

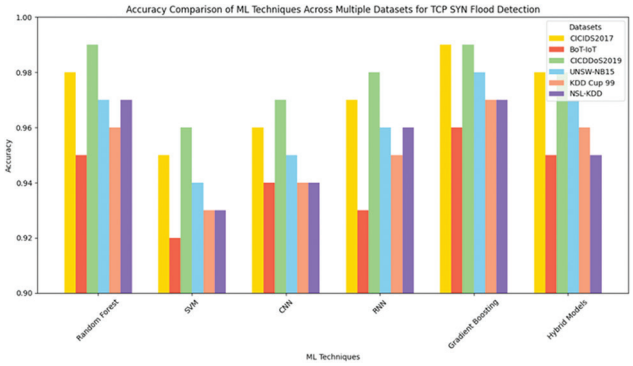

Fig. 9. Comparison of machine learning techniques over transmission control protocol Sync.

B. Creating

Another problem that still needs more work is that subjecting high quality, representative datasets that well represent realistic traffic patterns and real attack behaviors require. Vastly improving t robustness and transferability of such detection systems requires writing or using datasets that appropriately predict benign (Dimolianis, Pavlidis and Maglaris, 2021b; Aighuraibawi, et al., 2023).

XV. Comparison of Ml Techniques Over TCP SYN Flood in Various Datasets

In this survey that showed in Fig. 9, the performance of various ML models – including Random Forest, SVM, convolutional neural networks (CNN), RNN, Gradient Boosting, and Hybrid Models – across six well-known datasets:

In addition, the argument about these: CICDDoS2017, BoT-IoT, CICDDoS2019, UNSW-NB15, KDD Cup 99, and NSL-KDD. In Fig. 9 that illustrates, dataset characteristics

affect the effectiveness of the model in detection of the TCP SYN flood. For instance, the CICDDoS2019 dataset is specifically tailored to DDoS attack patterns; and while being less comprehensive, yet randomly very effective in achieving high accuracy on a variety of models (Random Forest and Gradient Boosting in particular), it stacks specifically on DDoS-related features. However, datasets such as UNSW-NB15 and KDD Cup 99, containing larger variety of attack types, demonstrated high variability of accuracy across the models, suggesting that DDoS traffic detection is an intractable task, given the dataset is not properly tailored to it.

However, datasets such as BoT-IoT and NSL-KDD were also able to perform well on some models, but they relied on the model's ability to generalize over different attack features.

XVI. Cross-Validation Accuracy

The above chart shows a comparison of accuracies realized by distinct models of ML in TCP SYN flood attacks' detection. The horizontal axis measures the ML models whereas the vertical axis is the accuracy level which determines the ability by percentage of the particular model to classify well.

The findings also emphatically reveal that Random Forest gives better results than all the other models with average accuracy of 99.99% ensuring the high efficiency of the chosen model to detect SYN flood attacks. This fairly accurate result implies adept handling of relationships within a dataset, which translates well to this network intrusion detection. Moreover, Decision Tree and Gradient Boosting achieve the accuracies of 99.84% and 99.95%, respectively. These outcomes stress the high stability and efficiency of growing tree models, in particular, gradient boosting, those are based on the principle of the ensemble of models. L: K-Nearest Neighbors another impressive model also agreed with the conclusion attaining an accuracy of 99.22% suggesting that it can also be used to classify the network traffic, though it falls a bit behind the ensemble models.

On the other hand, the accuracy of logistic regression has dropped to 94.81%. These poor results again indicate the problem with linear models, in which logistic regression may not capture all the intricacies of the patterns necessary for correct SYN flood detection when compared to the better models. Likewise, the MLP classifier (Neural Network), though quite satisfactory in commission rate of 2.16%, was slightly below par in accuracy standing at 97.84% and far below the tree-based models. This could be since hyperparameters of neural network's need to be tuned to near optimum to match the features of models such as Random Forest and Gradient Boosting.

Moreover, the other method is SVM which also has a satisfactory accuracy of 98.92% but worse than the ensemble models and had better performance compared with logistic regression and MLP classifier. Although SVM has proven itself to be a high dimensional data learner, it was less effective than Random Forest and Gradient Boosting in this case.

XVII. Conclusion

TCP SYN flood has emerged as a major problem in contemporary networks due to its ability to severely and quickly overwhelm the resources, therefore, the need to develop better ways of detecting and preventing it. These attacks happen at the initial TCP handshake stage to overwhelm the server resources to the extent of straining most of the available networks and computations. Protecting against this form of attack is important in securing networks and network infrastructure as threats evolve and advance in their sophistication and magnitude and as novel network environments continue to arise.

In this paper, an overview of different types of ML algorithms used in identifying TCP SYN flood attacks has been provided, ranging from conventional supervised models, self-organized deep learning frameworks, and combinations of these. In the light of detecting the TCP SYN flood, the review discusses the strength and weakness of each of the mentioned techniques. In the cases of supervised models, algorithms such as SVM and random forests are accurate to detect previously identified attack signatures and the best suited in well-understood environments where the attacking signatures are already defined. Neural networks, specifically CNN, have the potential of improving their performance when applied to massive high-dimensional data and applying deep learning models in the context of the network traffic is valuable due to the dynamic settings in which the TCP SYN flood features may change or evolve.

Nevertheless, various issues are still apparent in TCP SYN flood detection even with improved techniques proposed. Real-time detection is still a problem since making a distinction between the authentic traffic and the malicious traffic is tough due to network congestion. However, there are also important limitations and future work regarding the presented work: specifically, the concerns about the scalability and interpretability of the grouped models. Other ways of improving these models include minimizing the false positives and optimizing response mechanisms that guarantee these models provide useful information without compromising on the legitimate traffic on the network.

References

Aggarwal, S., Behera, B., Singh, M.K., and Sharma, A.K., 2025. Optimizing DDoS Attack Detection Using Machine Learning. In: *2025 2nd International Conference on Computational Intelligence, Communication Technology and Networking (CICTN)*, pp.245-250.

Aighuraibawi, A.H.B., Manickam, S., Abdullah, R., Alyasseri, Z.A.A., Jasim, H.M., and Sani, N.S., 2023. Modified Flower Pollination Algorithm for ICMPv6-Based DDoS Attacks Anomaly Detection. In: *Procedia Computer Science*. Elsevier B.V., Netherlands, pp.776-781.

Alasadi, S.A., Manaa, M.E., Hussain, S.M., and Al-Khamees, H.A.A., 2024. DDoS attacks detection based on machine learning algorithms in IoT environments. *Inteligencia Artificial Revista Iberoamericana de Inteligencia*

Artificia, 27, pp.152-165.

Ali, T.E., Chong, Y.W. and Manickam, S., 2023. Machine learning techniques to detect a DDoS attack in SDN: A systematic review. *Applied Sciences,* 13(5), p.3183.

Bamasag, O., Alsaeedi, A., Munshi, A., Alghazzawi, D., Alshehri, S., and Jamjoom, A., 2022. Real-time DDoS flood attack monitoring and detection (RT-AMD) model for cloud computing. *PeerJ Computer Science*, 7, p.e814.

Bawany, N.Z., Shamsi, J.A., and Salah, K., 2017. DDoS attack detection and mitigation using SDN: Methods, practices, and solutions. *Arabian Journal for Science and Engineering*, 42, pp.425-441.

Bensaid, R., Labraoui, N., Abba Ari, A.A., Maglaras, L., Saidi, H., Abdu Lwahhab, A.M., and Benfriha, S., 2024. Toward a real-time TCP SYN flood DDoS mitigation using adaptive neuro-fuzzy classifier and SDN assistance in fog computing. *Security and Communication Networks*, 2024(1), p.6651584.

Bhayo, J., Shah, S.A., Hameed, S., Ahmed, A., Nasir, J., and Draheim, D., 2023. Towards a machine learning-based framework for DDOS attack detection in software-defined IoT (SD-IoT) networks. *Engineering Applications of Artificial Intelligence*, 123, p.106432.

Bhutani, P., and Dash, C.S., 2024. Deep learning approaches for SYN flood detection in internet service providers network. *International Journal of Innovative Research in Engineering and Management*, 11(4), pp.86-94.

Bovenzi, G., Di Monda, D., Montieri, A., Persico, V., and Pescapè, A., 2024. Classifying attack traffic in IoT environments via few-shot learning. *Journal of Information Security and Applications*, 83, p.103762.

Cai, T., Jia, T., Adepu, S., Li, Y., and Yang, Z., 2023. ADAM: An adaptive DDoS attack mitigation scheme in software-defined cyber-physical system. *IEEE Transactions on Industrial Informatics*, 19(6), pp.7802-7813.

Chandana Swathi, G., Kishor Kumar, G., and Siva Kumar, A.P., 2024. Ensemble classification to predict botnet and its impact on IoT networks. *Measurement: Sensors*, 33, p.101130.

Chicco, D., and Jurman, G., 2020. The advantages of the Matthews correlation coefficient (MCC) over F1 score and accuracy in binary classification evaluation. *BMC Genomics*, 21, p.6.

Cui, J., Wang, M., Luo, Y., and Zhong, H., 2019. DDoS detection and defense mechanism based on cognitive-inspired computing in SDN. *Future Generation Computer Systems*, 97, pp.275-283.

Das, T., Hamdan, O.A., Sengupta, S., and Arslan, E., 2022. Flood control: TCP-SYN Flood Detection for Software-Defined Networks using OpenFlow Port Statistics. In: *2022 IEEE International Conference on Cyber Security and Resilience (CSR)*. pp.1-8.

Dasari, K.B., and Devarakonda, N., 2022. Detection of DDoS attacks using machine learning classification algorithms. *International Journal of Computer Network and Information Security*, 6, pp.89-97.

Dasari, S., and Kaluri, R., 2024. An effective classification of DDoS attacks in a distributed network by adopting hierarchical machine learning and hyperparameters optimization techniques. *IEEE Access*, 12, pp.10834-10845.

Dash, S.K., Dash, S., Mahapatra, S., Mohanty, S.N., Khan, M.I., Medani, M., Abdullaev, S., and Gupta, M., 2024. Enhancing DDoS attack detection in IoT using PCA. *Egyptian Informatics Journal*, 25, p.100450.

Deb, D., Rodrigo, H., and Kumar, S., 2024. Performance Analysis of Machine Learning Algorithms on Imbalanced DDoS Attack Dataset. In: *2024 IEEE World AI IoT Congress (AIIoT)*. pp.349-355.

Deshmukh, R.V., and Devadkar, K.K., 2015. Understanding DDoS attack & its effect in cloud environment. *Procedia Computer Science*, 49, pp.202-210.

Dimolianis, M., Kalogeras, D.K., Kostopoulos, N., and Maglaris, V., 2022. DDoS Attack Detection via Privacy-aware Federated Learning and Collaborative Mitigation in Multi-domain Cyber Infrastructures. In: *2022 IEEE 11th International Conference on Cloud Networking (CloudNet)*. pp.118-125.

Dimolianis, M., Pavlidis, A., and Maglaris, V., 2021a. Signature-based traffic classification and mitigation for DDoS attacks using programmable network data planes. *IEEE Access*, 9, pp.113061-113076.

Dimolianis, M., Pavlidis, A., and Maglaris, V., 2021b. SYN Flood Attack Detection and Mitigation using Machine Learning Traffic Classification and Programmable Data Plane Filtering. In: *2021 24th Conference on Innovation in Clouds, Internet and Networks and Workshops, ICIN 2021*. Institute of Electrical and Electronics Engineers Inc., pp.126-133.

Doshi, R., Apthorpe, N., and Feamster, N., 2018. Machine Learning DDoS Detection for Consumer Internet of Things Devices. In: *Proceedings - 2018 IEEE Symposium on Security and Privacy Workshops, SPW 2018*. Institute of Electrical and Electronics Engineers Inc. pp.29-35.

Echeverría, A.D., Pinilla, M.A., and Mora, H.R.C., 2024. Securing the IoT: An In-Depth Analysis of Ubuntu Core Hardening Measures Using CIS LTS Guide. In: *2024 4th Interdisciplinary Conference on Electrics and Computer (INTCEC)*. pp.1-8.

Feng, Y., Zhang, W., Yin, S., Tang, H., Xiang, Y., and Zhang, Y., 2023. A collaborative stealthy DDoS detection method based on reinforcement learning at the edge of internet of things. *IEEE Internet of Things Journal*, 10(20), pp.17934-17948.

Gaurav, A., Zhou, Z., Tai Chui, K., Colace, F., Chaurasia, P., and Hsu, C.H., 2021. *A Novel Approach for DDoS Attack Detection Using Big Data and Machine Learning*. In: CEUR Workshop Proceedings.

Ghafoor, K.Z., 2022. Social bot detection using machine learning algorithms: A survey and research challenges. *Polytechnic Journal*, 12(2), pp.219-228.

Haider, S., 2020. A deep CNN ensemble framework for efficient DDoS attack detection in software defined networks. *IEEE Access*, 8, pp.53972-53983.

Hamad, Z.O., 2022. Review of feature selection methods using optimization algorithm (Review paper for optimization algorithm). *Polytechnic Journal*, 12(2), pp.203-214.

Hassan, S.K.H., and Daneshwar, M.A., 2022. Anomaly-based network intrusion detection system using deep intelligent technique. *Polytechnic Journal*, 12(2), pp.100-113.

Hasan, M.K., Habib, A.A., Islam, S., Safie, N., Abdullah, S.N.H.S. and Pandey, B., 2023. DDoS: Distributed denial of service attack in communication standard vulnerabilities in smart grid applications and cyber security with recent developments. *Energy Reports,* 9, pp.1318-1326.

Hong, K., Kim, Y., Choi, H., and Park, J., 2017. SDN-assisted slow HTTP DDoS attack defense method. *IEEE Communications Letters*, 22, 688-691.

Hoque, N., Kashyap, H., and Bhattacharyya, D.K., 2017. Real-time DDoS attack detection using FPGA. *Computer Communications*, 110, pp.48-58.

Hossain, M.A., and Islam, M.S., 2024. Enhancing DDoS attack detection with hybrid feature selection and ensemble-based classifier: A promising solution for robust cybersecurity. *Measurement: Sensors*, 32, 101037.

Hsu, F.H., Lee, C.H., Wang, C.Y., Hung, R.Y., and Zhuang, Y., 2021. DDoS flood and destination service changing sensor. *Sensors (Basel)*, 21, p.1980.

Hussain, K., Syed Jawad, H., Veena, D., Muhammad, N., and Muhammad Awai, A., 2016. An adaptive SYN flooding attack mitigation in DDOS environment. *International Journal of Computer Science and Network Security*, 16, pp.27-33.

Hwang, R.H., 2020. An unsupervised deep learning model for early network traffic anomaly detection. *IEEE Access*, 8, pp.30387-30399.

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

Jaafar, G.A., Abdullah, S.M., and Ismail, S., 2019. Review of recent detection methods for HTTP DDoS attack. *Journal of Computer Networks and Communications*, 2019, p.1283472.

Jaraba, F., Mahajan, G., Jani, J., Ipu, R., and Butakov, S., 2024. Exploring

current solutions against DDoS attacks in SDN environment. *Procedia Computer Science*, 238, pp.127-134.

Javadpour, A., 2020. Providing a way to create balance between reliability and delays in SDN networks by using the appropriate placement of controllers. *Wireless Personal Communications*, 110, pp.1057-1071.

Javadpour, A., and Wang, G., 2022. cTMvSDN: Improving resource management using combination of Markov-process and TDMA in software-defined networking. *Journal of Supercomputing*, 78, pp.3477-3499.

Javadpour, A., Wang, G., and Rezaei, S., 2020. Resource management in a peer-to-peer cloud network for IoT. *Wireless Personal Communications*, 115, pp.2471-2488.

Javanmardi, S., Ghahramani, M., Shojafar, M., Alazab, M., and Caruso, A.M., 2024. M-RL: A mobility and impersonation-aware IDS for DDoS UDP flooding attacks in IoT-Fog networks. *Computers and Security*, 140, p.103778.

Jr, E.P.F., Tavares, A.C.J., and Nogueira, M., 2023. A Runtime DDoS Attack Detection Technique Based on Stochastic Mathematical Model. In: *2023 IEEE Latin-American Conference on Communications (LATINCOM)*. pp.1-6.

Kanimozhi, S., and Radhika, D., 2022. Detection of DDos attack using machine learning algorithms in cloud computing. *Turkish Online Journal of Qualitative Inquiry*, 13 (1), pp.2079-2088.

Kellerer, W., Schembra, G., Hwang, J., Kamiyama, N., Kang, J.M., Martini, B., Pasquini, R., Pezaros, D., Zhang, H., Zhani, M.F., and Zinner, T., 2021. Guest EDITORS Introduction: Special issue on advanced management of softwarized networks. *IEEE Transactions on Network and Service Management*, 18(1), pp.20-29.

Kim, Y., Hakak, S., and Ghorbani, A., 2024. Detecting distributed denial-of-service (DDoS) attacks that generate false authentications on Electric Vehicle (EV) charging infrastructure. *Computers and Security*, 144, p.103989.

Kreutz, D., Ramos, F.M., Verissimo, P.E., Rothenberg, C.E., Azodolmolky, S., and Uhlig, S., 2014. Software-defined networking: A comprehensive survey. *Proceedings of the IEEE*, 103, pp.14-76.

Kumari, P., and Jain, A.K., 2023. A comprehensive study of DDoS attacks over IoT network and their countermeasures. *Computers and Security*, 127, p.103096.

Liu, Z., Wang, Y., Feng, F., Liu, Y., Li, Z., and Shan, Y., 2023. A DDoS detection method based on feature engineering and machine learning in software-defined networks. *Sensors (Basel)*, 23, p.6176.

Magnani, S., Doriguzzi-Corin, R., and Siracusa, D., 2023. Enhancing Network Intrusion Detection: An Online Methodology for Performance Analysis. In: *2023 IEEE 9th International Conference on Network Softwarization (NetSoft)*. pp.510-515.

Meng, B., Andi, W., Jian, X., and Fucai, Z., 2017. DDOS Attack Detection System Based on Analysis of Users' Behaviors for Application Layer. In: *Proceedings - 2017 IEEE International Conference on Computational Science and Engineering and IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, CSE and EUC 2017*. Institute of Electrical and Electronics Engineers Inc., pp.596-599.

Mirmohseni, S.M., Tang, C., and Javadpour, A., 2020. Using Markov learning utilization model for resource allocation in cloud of thing network. *Wireless Personal Communications*, 115, pp.1-25.

Mohammadi, R., Javidan, R., and Conti, M., 2017. Slicots: An SDN-based lightweight countermeasure for TCPSYN flooding attacks. *IEEE Transactions on Network and Service Management*, 14, pp.487-497.

Nadeem, M.W., Goh, H.G., Ponnusamy, V., and Aun, Y., 2022. DDoS detection in SDN using machine learning techniques. *Computers, Materials and Continua*, 71(1), pp.771-789.

Nath Rimal, A., and Praveen, R., 2020. DDOS attack detection using machine learning. *Journal of Emerging Technologies and Innovative Research*, 7, pp.1-7.

Naveen, B., and Manu, S., 2019. Detecting DDoS attacks using machine learning techniques and contemporary intrusion detection dataset. *Automatic Control and Computer Sciences*, 53(5), pp.419-428.

Novaes, M.P., 2020. Long short-term memory and fuzzy logic for anomaly detection and mitigation in software-defined network environment. *IEEE Access*, 8, pp.83765-83781.

Özçam, B., Kilinc, H.H., and Zaim, A.H., 2021. Detecting TCP Flood DDoS Attack by Anomaly Detection based on Machine Learning Algorithms. In: *2021 6th International Conference on Computer Science and Engineering (UBMK)*. pp.512-516.

Pai, K., and Bha, A., 2014. Detection and performance evaluation of DoS/DDoS attacks using SYN flooding attacks. *International Journal of Computer Applications*, 975, pp.1-4.

Pari, S.N., Ritika, E.C., Ragul, B., and Bharath, M., 2023. AI-based Network Flooding Attack Detection in SDN using Multiple Learning Models and Controller. In: *2023 12th International Conference on Advanced Computing (ICoAC)*. pp.1-7.

Patel, M., Amritha, P.P., Sudheer, V.B., and Sethumadhavan, M., 2024. DDoS Attack detection model using machine learning algorithm in next generation firewall. *Procedia Computer Science*, 233, pp.175-183.

Patel, N.K., Anagha, N., and Santhosh Kumar, J., 2024. Effective Intrusion Detection and Prevention System of Botnet attack in Blockchain Technology using Recurrent Neural Network. In: *2024 Control Instrumentation System Conference (CISCON)*. pp.1-6.

Ramadhani, E.H., Enriko, I.K.A., Alamsyah, A.T., Nuha, M.A.U., and Sari, E.L.I.P., 2025. *Comparative Analysis of QoS between LEO Satellite and Cellular Internet Networks for IoT Smart Farming*. pp.479-489.

Ravi, N., and Shalinie, S.M., 2021. BlackNurse-SC: A novel attack on SDN controller. *IEEE Communications Letters*, 25(7), pp.2146-2150.

Rawashdeh, A., Alkasassbeh, M., and Al-Hawawreh, M., 2018. An anomaly-based approach for DDoS attack detection in cloud environment. *International Journal of Computer Applications in Technology*, 57, p.312.

Rimal, A.N. and Praveen, R., 2020. DDOS attack detection using machine learning. *Journal of Emerging Technologies and Innovative Research,* 7(6), pp.185-188.

Sahi, A., Lai, D., Li, Y., and Diykh, M., 2017. An efficient DDoS TCP flood attack detection and prevention system in a cloud environment. *IEEE Access*, 5, pp.6036-6048.

Sahosh, Z.H., Faheem, A., Tuba, M.B., Tasnim, S.A., Anika, S., and Tasnim, 2024. A Comparative review on DDoS attack detection using machine learning techniques. *Malaysian Journal of Science and Advanced Technology*, 4, pp.75-83.

Saif, S., Widyawan, W., and Ferdiana, R., 2024. IoT-DH dataset for classification, identification, and detection DDoS attack in IoT. *Data in Brief*, 54, p.110496.

Saiyed, M.F., and Al-Anbagi, I., 2024. A genetic algorithm- and t-test-based system for DDoS attack detection in IoT networks. *IEEE Access*, 12, pp.25623-25641.

Sambangi, S., and Gondi, L., 2020a. A machine learning approach for DDoS (distributed denial of service) attack detection using multiple linear regression. *Proceedings*, 63, p.51.

Sambangi, S., and Gondi, L., 2020b. A machine learning approach for DDoS (distributed denial of service) attack detection using multiple linear regression. *Proceedings*, 63, p.51.

Shao, Z., Chen, T., Cheng, G., Hu, X., Li, W., and Wu, H., 2023. AF-FDS: An accurate, fast, and fine-grained detection scheme for DDoS attacks in high-speed networks with asymmetric routing. *IEEE Transactions on Network and Service Management*, 20(4), pp.4964-4981.

Sharma, V.K., and Kumar, M., 2017. Adaptive congestion control scheme in mobile ad-hoc networks. *Peer-to-Peer Networking and Applications*, 10, pp.633-657.

Sharma, V.K., Verma, L.P., and Kumar, M., 2019. CL-ADSP: Cross-Layer adaptive data scheduling policy in mobile ad-hoc networks. *Future Generation Computer Systems*, 97, pp.530-563.

Sharma, V.K., Verma, L.P., Kumar, M., Naha, R.K., and Mahanti, A., 2020. A-CAFDSP: An adaptive-congestion aware Fibonacci sequence based data scheduling policy. *Computer and Communications*, 158, pp.141-165.

Sikos, L.F., 2020. Packet analysis for network forensics: A comprehensive survey. *Forensic Science International: Digital Investigation*, 32, p.200892.

Singh, A., Çamtepe, S.A., Jang, J.S., Wei, Y., and Sabrina, F., 2023. Classification and Explanation of Distributed Denial-of-Service (DDoS) Attack Detection using Machine Learning and Shapley Additive Explanation (SHAP) Methods. *ArXiv*, abs/2306.17190.

Singh, S., Jeong, Y.S., and Park, J.H., 2016. A survey on cloud computing security: Issues, threats, and solutions. *Journal of Network and Computer Applications*, 75, p.200-222.

Sreeram, I., and Vuppala, V.K., 2019. HTTP flood attack detection in application layer using machine learning metrics and bio inspired bat algorithm. *Applied Computing and Informatics*, 15, pp.59-66.

Srinivasu, P.N., Bhoi, A.K., Nayak, S.R., Bhutta, M.R., and Woźniak, M., 2021. Blockchain technology for secured healthcare data communication among the non-terminal nodes in IoT architecture in 5G network. *Electronics*, 10, 1437.

Subashini, V., Janaki, R., Mol, M.S., and Kokilavani, G.M., 2022. Implementation of Effective IoT Architecture for Early Flood Detection and Management System. In: *2022 International Conference on Computer, Power and Communications (ICCPC)*. pp.158-165.

Sudar, K.M., and Deepalakshmi, P., 2020a. A two level security mechanism to detect a DDoS flooding attack in software-defined networks using entropy-based and C4.5 technique. *Journal of High Speed Networks*, 26, pp.1-22.

Sudar, K.M., and Deepalakshmi, P., 2020b. Comparative study on IDS using machine learning approaches for software defined networks. *International Journal of Intelligent Enterprise*, 7, pp.15-27.

Swami, R., Dave, M., and Ranga, V., 2021. Detection and analysis of TCP-SYN DDoS attack in software-defined networking. *Wireless Personal Communications*, 84, pp.2295-2317.

Syafiuddin, N.H., Mandala, S., and Cahyani, N.D.W., 2023. Detection Syn Flood and UDP Lag Attacks Based on Machine Learning Using AdaBoost. In: *2023 International Conference on Data Science and Its Applications (ICoDSA)*. pp.36-41.

Tang, D., Zheng, Z., Wang, X., Xiao, S., and Yang, Q., 2023. PeakSAX: Real-time monitoring and mitigation system for LDoS attack in SDN. *IEEE Transactions on Network and Service Management*, 20(3), pp.3686-3698.

Tuan, N.N., Hung, P.H., Nghia, N.D., Tho, N.V, Phan, T.V., and Thanh, N.H., 2020. A DDoS attack mitigation scheme in ISP networks using machine learning based on SDN. *Electronics*, 9, 413.

Tuyen, N.D., Quan, N.S., Linh, V.B., Tuyen, V.V., and Fujita, G., 2022. A comprehensive review of cybersecurity in inverter-based smart power system amid the boom of renewable energy. *IEEE Access*, 10, pp.35846-35875.

Wang, H., and Li, Y., 2024. Overview of DDoS attack detection in software-defined networks. *IEEE Access*, 12, pp.38351-38381.

Wang, M., Lu, Y., and Qin, J., 2022. Source-based defense against DDoS attacks in SDN based on sFlow and SOM. *IEEE Access*, 10, pp.2097-2116.

Xiao, M., Cui, Y., Qian, Q., and Shen, G., 2022. KIND: A novel image-mutual-information-based decision fusion method for saturation attack detection in SD-IoT. *IEEE Internet of Things Journal*, 9(23), pp.23750-23771.

Yang, C.H., Wu, J.P., Lee, F.Y., Lin, T.Y., and Tsai, M.H., 2023. Detection and mitigation of SYN flooding attacks through SYN/ACK packets and black/white lists. *Sensors (Basel)*, 23(8), 3817.

Zamrai, M.A.H., Yusof, K.M., and Azizan, M.A., 2024. Random Forest Stratified K-Fold Cross Validation on SYN DoS Attack SD-IoV. In: *2024 7th International Conference on Communication Engineering and Technology (ICCET)*. pp.7-12.

Zeeshan, M., Riaz, Q., Bilal, M.A., Shahzad, M.K., Jabeen, H., Haider, S.A., and Rahim, A., 2022. Protocol-based deep intrusion detection for DoS and DDoS attacks using UNSW-NB15 and Bot-IoT data-sets. *IEEE Access*, 10, pp.2269-2283.

Zhou, Q., Li, R., Xu, L., Nallanathan, A., Yang, J., and Fu, A., 2022. Towards Explainable Meta-Learning for DDoS Detection. *SN Computer Science,* 5 (1), 115.

Zubaydi, H.D., Anbar, M., and Wey, C.Y., 2017. Review on Detection Techniques against DDoS Attacks on a Software-Defined Networking Controller. In: *Proceedings - 2017 Palestinian International Conference on Information and Communication Technology, PICICT 2017*. Institute of Electrical and Electronics Engineers Inc., pp.10-16.