INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT (IJSREM)
VOLUME: 08 ISSUE: 05 | MAY - 2024 SJIF RATING: 8.448 ISSN: 2582-3930

Surveying Emerging Trends in DDoS Defense

Sumith Pandey
Student, School Of CS and IT
Jain(Deemed-to-be University)
Jayanagar 9th block,
Bengaluru,India-560069.
Email:23mcar0150@jainuniversity.ac.in

Dr.Febin Prakash
Asst. Professor,
School of Computer Science and IT,
Jain (Deemed-to-be University),
Bengaluru,India - 560069
Febin.prakash@jainuniversity.ac.in

***Abstract*—**This The DDoS attack threat is evolving, and because of this, organizations are discovering and using new modern technologies to lay the ground for more effective defensive strategies. This paper is devoted to the investigation of the most efficient methods fighting DDoS – downtime of the network, and ensuring cybersecurity on different domains. First of all, the integration of Convolutional Neural Networks (CNNs) into cybersecurity is a very promising move with respect to fighting exactly the phishing and application-layer DDoS attacks in greater details than the machine learning approaches like the LSTMs and SAEs. Another aspect of building the effective opposition against the dummy data attacks on the critical infrastructures, for example on the power systems, is creating the multi-dimensional mitigation models composed of various timely detection techniques and robust network architecture. In addition, the usage of Physically Unclonable Functions (PUFs) in network architectures provides a means of authentication as well as access control that can improve the resilience of a network against DDoS attacks. PUFs enables the blockade of unwanted packets of high volume traffic, allowing granular traffic filtration and isolation. By using hardware solutions such as Distributed-Denial-of-Service (DDoS) attack prevention, SDN-biased security frame with deep learning algorithms can improve network resilience with significant detection and response to slow-rate DDoS attacks. At last EWMA, KNN, and CUSUM as statistical methods integrated with FOG computing architectures ensure real time and effective solution for the detection and mitigation of DDoS attacks in the IoT networks, making them immune to the current as well as the continuously emerging cyber threats. Through the integration of these cutting edge methods, organizations will be able to hold their ground against cyberattacks catalyzed by DDoS menace and stay ahead of dynamic threats whenever they arise.

Keywords— Cloud computing, Data threats, Data Protection, Cloud security.

INTRODUCTION

Likewise, options to counter DDoS attacks grow with the increasing awareness about DDoS mitigations globally. The most striking change which has so far taken place in this process is the growing acceptance of modern technologies such as the Convolution Neural Networks (CNNs) which have come to dominate data processing. CNNs have found their place in diverse fields extending beyond cybersecurity and are notable in their use mostly for commercial applications that block phishing and application-level DDoS attacks among others. In this world where CNNs are used to fight phishing defense, they bring the very dynamism and adaptability in detection of some complicated web traffic patterns linked to the phishing and, therefore, they help organizations in improving the security level relative to deceptive methods that thrive to penetrate their setups. Correspondingly, the application layer DDoS attacks that take advantage of web application weaknesses being identified by a CNN-based detection system it is being done through analysis of fine-grained network traffic features that are catching the attacker in the act and impede them from achieving their goals. CI development business can impose the capabilities of deep learning to remain in the lead with the dynamic DDoS threats and the cyber threats' landscape's modifying tendency in the future.[1]

The area of power systems data integrity, as representing an attack by using fake data - injection of malicious information into the control and monitoring system of critical infrastructures of energy - is significant as it ensures system
reliability and safety. Creating an effective model of mitigation towards activities of such attacks really needs

to carry multidimensional approach which involves two factors e. g. , highly advanced anomaly detection techniques and robust cryptographic protocols and resilient network architectures. The subroutine of anomaly detection of algorithms, including the use of machine learning-based models and statistic analysis methods, will be employed to find diffusion of abnormal patterns in the sensor data that can be caused by use of dummy data injections. Embedded with the machines' data algorithms, these systems can uninterruptedly track and beacon the integrity of data flow and can also promote and promote quick response and imbursement measures in times of suspicious activities. Moreover, the incorporation of cryptographical methods, for example, digital signatures and message authentication codes, increase data security and integrity level, which makes it hard for data to be edited or spoofs by impersonators. To this end, the redundancy, segmentation, and robust access control methods much like these are utilized for fortifying the entire system and protecting it from unlawful intrusions. This, in turn, limits the impact of successful attacks. The exploitation of the additive nature of these approaches may result in a sophisticated power system defense paradigm against the exponentially increasing dummy data assault, thus, securing the key energy infrastructure fundamentals of the service provision.[2]

Building a network microstructure on the basis of Physically Unclonable Functions (PUFs) for DDoS risk prevention brings an additional mean of cybersecurity strengthening. PUFs are based on the intrinsic physical properties of electronic components which leads to acquiring the unique identifiers and makes them vulnerable to the cloning or replicating. Through the implementation of PUF-based authentication measures at the infrastructure network, organizations can build up resilience to DDoS attacks. PUFs are implemented in devices' memory with robust device authentication that is keyless and utilizes pre-shared secrets to shield them from risks associated with theft or compromise. The implementation of such identifiers is therefore essential in regard of building trust relationships among network elements and it enables for granular access control and traffic filtration so as to isolate and mitigate DDoS attack traffic. Adversary of PUF-based structures normally face difficulty to launch spoofing, replay, and similar forms of attack because of the physical uniqueness of PUFs. By their distributed system of authentication, these nodes do not reduce reliance on infrastructure in the center, therefore mitigating the problems of single point of failure, which in turns helps in strengthening the robustness of the network. In general, PUF-based network structures offer a very strong method for authentication, access control, and DDoS attack resistance, thus, it is a good strategy for companies pursuing better cybersecurity.[3]

The SDN framework-based security plan with automatic detection and capabilities for response in a timely manner for slow-rate DDoS attacks opens new perspectives to deal with cyberattacks in real time. Using the central control and programmability of SDN helps speeding up a real-time monitoring and mitigation mechanisms that when detecting anomalies indicative of a slow-rate DDoS attacks, the traffic forwarding policies can dynamically be changed ,and the suspicious traffic paths directed to the center for futher processing and filtering too. SDN is the enabler of dynamic rate limiting and traffic shaping policies that are necessary in order to achieve service delivery optimization in addition to limiting the possible side effects of DDoS attacks. On the other hand, the centralized management capabilities which enhance the rate of response and enable organizations to wind through the ever-changing methods of attack, help them stay informed of the adversaries and instruct a coordinated threat response. These SDN-based security frameworks contribute to the incident response workflows streamlining and overall security increase, allowing organizations to have an upper hand in fending off the sluggish DDoS attacks by adopting strategies that protect critical network resources from being compromised.[4]

An anomaly mitigation system for IoT networks can be designed using some of the statistics technique such as, Exponentially Weighted Moving Average (EWMA), K-Nearest Neighbors (KNN), and Cumulative Sum (CUSUM) which offers a holistic view of detecting and mitigating Distributed Denial of Service (DDoS) in these complex environments. The proliferation of IoT devices led to the increased trend to protect these interlinked networks from the bad actions. This system applies statistical methods to create the pattern behavior of the IoT devices and the moments those anomalies occur are the moments that attackers attack the system. EWMA (Exponentially Weighted Moving Average) traces variations over time, getting out the creepy changes showing gradual disturbances signaling ongoing attacks, while KNN (K-Nearest Neighbors) classifying instances as normal or anomalous enables proactively seek and response. Also, CUMSUM method provides detection of changes in statistical nature of streamed data, thus enable identifying intrusion events at an early stage. Through implementing such approaches organizations get ability to bolster their defense against DDoS attacks so that IoT infrastructures do not fail from endangering threats that arise continuously.[5]

I. LITERATURE REVIEW

The paper is coming with a groundbreaking solution to the plague of phishing and application layer DDoS attacks. The solution comprises of the exploitation of convolutional neural networks (CNNs), which have proved problem-solving and cybersecurity adjudication competence. For long, traditional techniques such as LSTM and SAE have instilled the deep cement known as the data processing pipeline within AI systems but the emergence of CNNs has poised a full proof solution which goes beyond the tracking of complex patterns in phishing emails and network traffic associated with client-server DDoS attacks. Using multiple convolutions, poolings, and nonlinear activations, CNNs are practiced to automatically remove unnecessary information and extract the needed features, for accurate detection of malicious behaviours which reveal through hidden subtle anomalies. Consequently, results of empirical implementation have shown that the proposed CNN model has overcome the shortcomings of the two simpler models, i. e. the neural network with LSTM and hierarchical architecture based on SAE, obtaining higher accuracy rates. In addition, CNNs are scalable, interpretable, and responsive to emergence of the other attack vectors, and the possibility to apply them in cybersecurity increases the chances for organizations to outsmart attackers in the challenging, dynamic setting of the cyber environment.[1]

Usually, in the current mitigating strategy, a reactive filtering system is implemented which, even though a bit efficient, has caveats in blocking the tailored Distributed Denial of Service (DDoS) attacks. The disadvantages of this architecture are recognized, therefore; the proposal output to measures against the DDoS using PUF to attain high efficiency in countering malicious activities by accurate filtering the traffic while maintaining the traffic flow during a DDoS attack. PUFs exploit natural physical disparities of digital assets for numerous purposes, such as random number generation, cryptographic operations, and unique identifiers. These unique identifiers in turn empower responsive defense strategies that specifically mitigate threats by identifying genuine requests from malicious ones in real-time. Contrary to the traditional passive approaches with long latencies that do not scale well, the PUF-based framework with its dynamic and proactive mitigation mechanisms blocks DDoS attacks at the entry points before they acknowledge them. Empirical assessments of the proposed structures have better results than reactive filtering, what reinforces the option of introducing it into the cybersecurity system to harden infrastructures against the DDoS attacks sophistication.[3]

Organizations that make use of Software-Defined Networking (SDN)-based automation systems encounter DDoS mitigation effectiveness that is as great as indicated by the studies. The ability of SDN to use the centralized control and programmability is enabling a change in the defense mechanisms of the frameworks, which become dynamic and proactive with the power to identify abnormal connections and block them in real-time. It has been documented how effectiveness varies from 91% by various studies. According to the source the SDN can decrease the number of established connections by from 66% to 100% highlighting the effectiveness of the SDN-based methods to reduce the DDoS impact on organizational networking. These SDN-based frameworks allow for automatic detection and mitigation hands down, efforts which in turn result in reduced response times and robust defense of organizations against DDoS threats. Also, SDN can be updated quickly and adjusted to combat any changing threat vectors. Therefore, they secure valuable network assets constantly. These findings emphasize the substantial role of SDN infratructures as a key component of modern cybersecurity tools, bringing organizations the needed layer of proactive action against the fast-changing DDoS threat landscape.[4]

The leading mitigation strategies for IoT networks in the context of fog computing include the use of statistic methods like EWMA, KNN, and CUSUM, being integrated within the fog computing architecture. So this way takes the fog nodes advantage that are located in distributed computing of network edge for doing real-time analysis and mitigation of security threats that minimizes the network latency and bandwidth consumption. The proposed model which links EWMA, KNN, and CUSUM with fog computing has obtained a remarkable accuracy of 99%. 00% and have a low false positive rate, thus, showing that they are highly accurate in detecting and responding to malicious acts and incidents and cause a low risk of erroneous alerts. Through blending statistical approaches with fog computing architectures, organizations are able to create IoT security defenses which are robust as well as agile. This integration gives out the possibility to spread the distributed threat detection and mitigation capabilities throughout the network, providing fog nodes with local processing data to identify and respond to security threats in real-time. This approach helps to lower latency by reducing the bandwidth requirements, and at the same time improves the overall security of IoT networks shielding such environments from disruptions or communication failures.[5]

The present DDoS attack mitigation strategies based on conventional techniques of detection are inadequate as

they may not prove to be so efficient in detecting and mitigating more creative attacks. Nevertheless, a Spatio-Temporal Graph Convolutional Network (ST-GCN) strategy which comes embedded into the SDN architecture brings a new perspective to the DDoS detection. It increases detection rate by almost 10% and enables CPU overhead as well as southbound interface load reduction that is significant. With the aid of the intrinsic spatial and temporal dependencies of network traffic data, the ST-GCN approach improves the capability of SDN-based systems to detect and mitigate DDoS attacks in real-time leading to a more adaptive solution for network administrators in guarding networks against the fast-moving DDoS atttacks.[6]

II. *CURRENT LANDSCAPE OF DDOS ATTACKS*

A. Types and Characteristics of DDoS Attacks:

1) Volumetric Attacks: These attacks focus on inundating a target network or a system with a tremendous traffic volume, exhausting system resources in response and shutting out any legitimate users. Typical, for example, may be: UDP flood attacks, ICMP flood attacks, and DNS amplification attacks.

2) Protocol Attacks: The range of protocol assaults varies from clogging of the system or exhausting of the resources to paralyzing the communication. Illustrations involve SYN flood attacks, Ping of death attacks and Smurf attacks.

3) Application Layer Attacks: They happen at application layer level of the OSI model in attempt to make use of vulnerabilities in web applications or services. There are different types of DDoS attack such as HTTP flood, Slowloris and Layer 7 DDoS Attacks.

4) Reflection and Amplification Attacks: Reflection and amplifying attacks put the use of third party servers or services at advantage as they intensify the volume of attack traffic that is targeted at the target. Common attacks include the DNS reflecting attack and the NTP amplifying attack.

5) Zero-Day Attacks: The zero-day DDoS attacks take advantage of previously found vulnerabilities in software or hardware that were not patched. Furthermore, the absence of verified fixes or mitigations also makes them more difficult to protect against.

B. Impact of DDoS Attacks on Organizations:

1) Disruption of Services: DDoS attacks are capable of disrupting the availability of important services thereby, causing downtime, the waste of resources and revenues for commercial companies. This perturbation extends beyond customers' trust and detrimentally affects sentiments about the brand.

2) Financial Losses: It is the financial impact of a DDoS attack that can be extreme in nature, including costs involved which are both to mitigate the attack and restoring services, and possible regulatory fines or legal liabilities.

3) Operational Challenges: DDoS attacks are able to bring many operational problems to the organisations, for example, the workload for the IT staff should increase, the resource limits may be gone and the business continuity can be affected.

4) Reputational Damage: Such DDoS attacks that become public can hurt an organization's credibility resulting in loss of customer trust and eventually investors' confidence. Brand loyalty can be affected to a long term extent, thus market competitiveness can as well.

5) Security Risks: DDoS attacks have the effect of just being a veil over more complex cyber threats such as data breaches or malware injections, which in turn places organizations in multiple security risks.

C. Evolution of DDoS Attack Techniques:

1) Increased Complexity: DDoS attack methodology has become more professional and complex with the advent of multi-vector attacks, encryption, and evasion techniques that beat the outdated mitigation methods.

2) Botnet Infrastructure: The growth of botnets, composed of compromised devices and system components, has helped execution of massive DDoS attacks that result in capacity and bandwidth agreement with the will of the attacker.

3) Use of IoT Devices: The growth in Internet of Things(IoT) empowered devices has significantly increased the attack surface for DDoS attacks. The hackers now use the vulnerabilities in the poorly protected IoT devices to build huge botnets.

4) Shift towards Application Layer Attacks: Despite the fact that volumetric attacks still dominate, we can see a decline in the number of these attacks and an increase in application layer attacks aiming to exploit specific vulnerabilities in a web application or service, which makes them more difficult to detect and mitigate.

5) Advanced Evasion Techniques: Attackers use crafty evasion tactics to go undetected and exhaust the resources of their target systems, such as IP spoofing, encryption, and traffic cloaking.

III. OVERVIEW OF MITIGATION STRATEGIES

A. Network-Level Mitigation Techniques:

1) Traffic Filtering and Rate Limiting: Traffic filtering is identification and filtering of malicious traffic at entry points of the network that is based on either predefined rules or signatures. Rate limit avoids network congestion by curbing the flow of incoming traffic and regulates DDoS attacks. These techniques are often applied via firewalls, routers and specialized DDoS mitigation devices.

2) Black Hole Routing: Black hole routing, also called null routing, operates by redirecting questionable or hostile traffic through the null interface or black hole destinations that result in dropping the traffic and preventing it from reaching the target. Black hole routing can successfully repulse DDoS attacks; however, it also can lead to unintended disruption of normal traffic.

3) Anycast Deployment: Anycast deployment is the process of having multiple network nodes with the same IP address and routing the incoming traffic to the nearest available node, based on the proximity algorithm. The benefits of anycast deployment can be improved through distribution of traffic over several geographically dispersed nodes which help increase the resilience and scalability, leading to lowering of the likelihood of individual nodes suffering from DDoS attacks.

B. Application-Level Mitigation Techniques:

1) Web Application Firewalls (WAF): WAFs are aimed to patrol web applications from the usual security concerns such as DDoS attacks by applying and analyzing the traffic in HTTP/HTTPS conntection based on defined security policies. Not only WAFs make possible the detection and filtration of malicious requests, but they also prevent SQL injection attacks, XSS attacks, and application layer DDoS attacks from reaching the web application server.

2) Intrusion Detection and Prevention Systems (IDPS): A perfect IDPS captures suspicious or bad network traffic even during DDoS attacks and works alone or by alerting the network administrators in response to the noticed threats. IDPS use a blend of signature detection, anomaly detection and behavioral analysis methods, which help to detect and eliminate the DDoS in real time.

3) Content Delivery Networks (CDNs): CDNs have a network of physically distributed geographical server locations that cache and distribute web content. This enables faster delivery of content to the end-users, and reduces implications of DDoS attacks on origin servers. CDNs function as an attack distributer and mitigator in DDoS attacks by the virtue of distributing traffic across multiple servers and also making use of specialized anti-DDoS capabilities such as scrubbing centers and traffic filtering

C. Hybrid and Cloud-Based Mitigation Solutions:

1) Hybrid On-Premises and Cloud-Based Solutions: With hybrid DDoS mitigation method, a company's local infrastructure or devices are integrated with cloud DDoS defense services so that all directions of an attack are contained and deterred. This solution allows organizations to scale both resources and network infrastructures as the attack volumes rise, thereby being able to benefit from the expansive pool of expertise and devices of the cloud-based DDoS protection vendors.

2) DDoS Protection Services from Cloud Providers: Cloud based DDoS protection services provided by cloud providers based on the global network infrastructure and advanced anti-DDoS techniques turn out to be the most effective solution against DDoS attacks. There are also those services, which mostly comprise of features like traffic scrubbing, rate limiting, DNS protection and can be deployed in an instant with no need for initial investment in hardware or software prior to that.

IV. EXCEPTION METHODOLOGIES

Integrating Convolutional Neural Networks (CNN) approach into the purposed solution is a big step forward in the research of machine learning solutions. CNNs have a great advantage in discovering spatial dependencies by using convolutional or other similar filters that are usually applied for imaging, natural language processing and even cybersecurity. Through incorporating the CNNs in the model, it attains the ability to automatically extrapolate the meaningful features out of fraught data representations, resulting into accurate and robust detection of the anomalies as well as malicious patterns inside the network traffic. Besides that, the suggested methods are remarkable for their new high accuracy level superseding the Long Short-Term Memory (LSTM) and the Stacked Autoencoder (SAE) methods of accuracy. While LSTM and SAE have been used widely for sequence modeling and feature extraction, they may thus have difficulties in capturing te complex patterns present in cybersecurity datasets. Contrary to the functioning of CNNs, the presented approaches are capable to obtain higher accuracy rates by means of their use of hierarchical representations

learned from the raw data input. These advancements in accuracy result in the model having an improved ability to detect and mitigate cybersecurity threats so they can increase the advanced technology of CNN-based approaches in the cybersecurity research and practice field.[1]

The study offer a resilient mitigation model with the core competency of overcoming the formidable data forgery attack (DFA) which is the emerging data threat. DDoS (distributed denial of service) attacks, which are an example of such cyber-threat and are carried out by malicious actors who flood networks with large volumes of meaningless or fake data pose a lot of problems for traditional cyber defenses that relied on perceivable limits. The article responds to the cultivated danger by providing a model mitigation strategy that assesses and removes the threats of DDAs before they can train the traffic flow. Since of the proposed mitigation strategy is to build a new and special algorithm for the precise solution of DDA mitigation which has many boggling and harmful factors. The integrated algorithm is designed to be accomplished by using complex mathematical skills to break down the problem into workable pieces which in turn facilitates for developing of efficient and corrective interventions. Thus, via dividing DDA mitigation problem into smaller, structured parts, the decomposition algorithm serves as a basis for the design of a targeted and responsive countermeasure system which can accurately detect and obstruct malicious data traffic. The eligible strategy modus of this concept undergoes rigorous testing and validation, that return to a promising design in the counteraction of DDAs on network infrastructure. Through the adoption of novel algorithmic procedures and in conjunction with cybersecurity domain-specific expertise, a research into developing tools and techniques that will enable organizations to cope with the cyber attack threats that are continually evolving and protect their critical online resources is being carried out. This is done in order to ensure the overall integrity of computer systems.[2]

Building and proposing a network architecture based on a novel approach of self-evolving cyberprotection through PUFs (Physically Unclonable Functions) is a step forward in digitizing and strengthening the defense of the cyber-space. PUFs use the wide spectrum of physical properties inherent to electronic components to produce a random string that serves as an un-clonable identifier or key, which is resistant to imitation as well. PUFs are an outstanding solution for intrinsic network protection as they interweave with the architecture of network layers and are getting a robust and tamper-resistant base to prevent unauthorized access and malicious activities. Here, the network structure captures the strengths of Transitioning Effect Ring Oscillation-Based Physical Unclonable Functions (TERO-PUFs) in doing the generation of capabilities. TERO-PUFs derive transient effects in ring oscillator chains, which are adapted to challenge inputs and subsequently lead to unique unorganized responses. The approach is a favorable entropy source for cryptographic key generation and authentication. Utilizing the TERO-PUFs, cyber defense will become much stronger, which in turn will lead to a more efficient communication channels' security, secure bootstrapping mechanisms, and access control policies' implementation, as well as to a significant decrease of the number of the threats in the network. Empirical trials and validation indirectly proves the inference of the network architecture in securing the stability and fidelity of the infrastructure. With the ability to utilize an intrinsic randomness and unpredictability of PUF capabilities a company is much more secure because it is less likely data to be intercepted, breached or attacked by some kind of a cyber attack. It means critical network resources will have a high level of confidentiality, integrity, and availability. With cyber attacks constantly evolving and advancing, it is possible to say that PUF-based systems serve as an anticipative measure for protecting data networks and can be considered a key component of cybersecurity. It is a strong and powerful weapon for safeguarding digital systems from the continuously changing threat landscape of the modern age.[3]

The combination of SDN (Software-Defined Networking) technologies with DL (Deep Learning) principles is definitely the next big step in cybersecurity, providing organizations with the ability to proactively and in time respond to cyber threats as part of a fully automated security system. SDN-based security frameworks use the centralized control with programability, given by the SDN architecture, as a basis to enhance network visibility, automate defenses and orchestrate the fast reactions to security incidents. Through the SDN disconnecting of the control plane from the data plane and localization of network management tasks, deep learning attacks are detectable and neutralization is provided, offering to the faulty network organizations unprecedented precision in the mitigation of threats. Highly sophisticated deep learning algorithms like CNNs and RNNs are utilized to analyze the technical networks traffic behavior with features of noting the patterns that are likely to be related to cyber threats. DL models will be trained using the labeled dataset which will distinguish normal and abnormal behavior as an organization can effectively develop highly accurate and adaptable attack detection mechanisms capable of recognizing new and 0Day

attacks. DL learning and subsequent adjustments will aid in the creation of flexible systems that will be able to learn from past attacks and adjust to new threats gradually eliminating the possibility of the system identifying legitimate actions as attacks (false positives) and missing malicious acts (false negatives). The entanglement of SDN in deep learning for identification and detection of attacks is the most prospective of all options that can be explored to make security defenses more effective and resilient. With SDN frameworks that entail indispensable flexibility and agility and deep learning algorithms which provide advanced analytical capabilities, organizations are able to forecast and quickly tackle a broad spectrum of cyber hazards like DDoS attacks, malware infections, and insider's threats. Additionally, security SDN applications provide flexibility in the self-care and self-healing of networks, thus allowing networks to deal with incidents quickly and limit the negative impact on the functioning of critical networks. Since cyberattacks keep on multiplying and developing due to high level of sophistication, integration of SDN and deep learning is a revolutionary step in cybersecurity by which digital infrastructure will be well protected and the confidentiality and integrity of any sensitive information would be preserved.[4]

Exponentially weighted moving average (EWMA) is a statistical technique evenly utilized in cyber security for real-time anomaly detection in network traffic. Through the intake of a weighted average of historical observations, with the most recent data points given the highest priority, EWMA then detects deviations which deviates from the expected trend, leading to the identification of anomalies that serve as indicators of cyber threats. Contrariwise KNN, a KNN, popularly applied in machine learning, classifies incoming data points based upon their resemblance to those previously observed data points. By using the method of near neighbors, both the known and unknown maliciousbehavior can be properly identified. Integration into this toolkit is CUSUM, the algorithm which is able to detect shifts in a mean of time-series data streams. CUSUM aims at finding the cumulative sum of mouths of deviation from the supposed mean through time to allow for the detection of gradual tendencies or sudden change of the network traffic patterns providing the organization with an early detection of a possible security breach or cyber-attack. Differing with these approaches, EWMA, KNN, and CUSUM come in as powerful machines for proactive threat detection and response which are vital for the organizations's development of robust defenses during this fast changing threat environment.[5]

CONCLUSION

As the cyber world keeps expanding and DDoS attacks are becoming more and more complicated and changing, it requires that organizations develop different solutions for protection. Consequently, this survey paper presents a wide range of the innovative solutions aimed at thwarting DDoS threat including the integration of sophisticated technologies such as CNNs, PUFs, SDN and deep learning algorithms. The mentioned approaches carry promising footholds in terms of their ability to improve the detection accuracy, automate incident response, and information processing systems against different kinds of DDoS attacks. Likewise, using statistical technique such as the use of Exponentially Weighted Moving Average (EWMA), K-Nearest Neighbors (KNN), and Cumulative Sum (CUSUM) in fog computing architectures, IoT networks are made even safer. Through the use of these advanced systems, organizations will be one step ahead when tackling cyber threats and DDoS attacks will no longer be considered as a disturbing force for their core business with regards to operational, financial and reputation issues. The future is characterized by need to do further research and to develop the strategies in order to make them more refined and optimized, which should be done by keeping in mind that the threats will evolve and the cybersecurity will be at risk.

REFERANCE

[1] P., Anitha., Wakgari, Dibaba., Raja, Sarath, Kumar, Boddu. (2023). Mitigation of Attacks Using Cybersecurity Deep Models in Cloud Servers. doi: 10.1109/ICDT57929.2023.10150832.

[2] (2023). Robust Mitigation Strategy against Dummy Data Attacks in Power Systems. IEEE Transactions on Smart Grid, doi: 10.1109/tsg.2022.3225469.

[3] (2023). Physical Assessment of an SDN-Based Security Framework for DDoS Attack Mitigation: Introducing the SDN-SlowRate-DDoS Dataset. IEEE Access, doi: 10.1109/access.2023.3274577.

[4] Hannes, Adomeit. (2023). A Novel Multi Algorithm Approach to Identify Network Anomalies in the IoT Using Fog Computing and a Model to Distinguish between IoT and Non-IoT Devices. Journal of Sensor and Actuator Networks, doi: 10.3390/jsan12020019.

[5] (2022). Detecting and Mitigating DDoS Attacks in SDN Using Spatial-Temporal Graph Convolutional Network. IEEE Transactions on Dependable and Secure Computing, doi: 10.1109/tdsc.2021.3108782.

[6] (2022). Detecting and Mitigating DDoS Attacks in SDN Using Spatial-Temporal Graph Convolutional Network. IEEE Transactions on Dependable and Secure Computing, doi: 10.1109/tdsc.2021.3108782.