# DDoS Mitigation: A review of Content Delivery Network and its DDoS Defense techniques

Mohammed Imthiyas[1], Sharyar Wani[2], Rawad Abdulkhaleq Abdulmolla Abdulghafor[3], Adamu Abubakar Ibrahim[4], Abdul Hafeez[5]
[1]Dept. of Information Systems, International Islamic University Malaysia, Kuala Lumpur, Malaysia.
[2,3,4]Dept. of Computer Science, International Islamic University Malaysia, IIUM, Kuala Lumpur, Malaysia.
[5]Dept. of Computer Science, Bahria University, Lahore, Pakistan
imthiyasm811@gmail.com, sharyarwani@iium.edu.my, rawad@iium.edu.my, adamu@iium.edu.my, ahafeez.bulc@bahria.edu.pk,

***Abstract***— Distributed Denial-of-Service (DDoS) attacks continue to pose major threats overwhelming entire networks. They slacken the availability of Internet service by sending huge malicious requests and spreading volumetrically. This survey recognizes fundamental theories across various disciplines to advance and improve the research of DDoS mitigation. These studies focus on DDoS mitigations with Content Delivery Network (CDN) from two views: (1) CDN's layout model and (2) its DDoS defense classifications. Content Delivery Network (CDN) refers to the Internet and delivers contents to the end-users. CDN is used for the basis of reverse proxying, web serving, and load balancing, etc. This literature finds that CDN serves clients from a scalable set of proxies that automatically deploys multiple websites. It protects the websites against DDoS and categorizes each view with various suitable defense methods. By reviewing DDoS mitigation characteristics among the DDoS attacks, this study features some possible methods to mitigate DDoS attacks with Content Delivery Network (CDN).

***Keywords***— Distributed Denial of Service (DDoS), Content Distributed Network (CDN), Network Security.

## I. INTRODUCTION

DDoS attacks are expanding globally, varying from a single system to multiple systems. Currently, DDoS attacks have risen from 8 Gbps to 500 Gbps compared to 2004. The DDoS attack has now spread towards cloud-based services too. Many cloud-based services use hybrid deployment design for the prevention of the DDoS attacks [1]. DDoS attacks target the server by sending a large number of malicious packets. The attackers use a number of malicious packets or compromised hosts to send unwanted traffic to the server, which inundates the server, drains the server's resources, and makes it inaccessible to the users or customers [2]. Many techniques, such as packet labeling, often allow a large number of packets to be tracked and processed, which further overloads the processing capability. The application of such techniques based on the installation of modules or computers increases implementation complexity [3]. An extensive network link-state tables on the system installation are expected to be maintained at routers or switches, resulting in additional storage and overloads computational capacity. Overall, the present design and implementation in the DDoS protection suggest a lack of autonomy, leading to non-trivial labor costs and latency in response while also increasing the downtime [4]. The studies' early efforts to develop autonomous DDoS response, scalability and operational expenses are still inadequate in large-scale implementation. Due to intense coordination and communication between various detection modules; the large scale implementation must be in advance [4]. Moreover, the existing solutions to prevent DDoS attacks are expensive in purchasing dedicated devices, including firewalls and cloud storage [5].

Several Distributed Denial of Service (DDoS) attacks have been launched to slow down public and private companies' networks [6]. Few of the known DDoS attack incident which has been reported include the "mem cached" DDoS attack traffic known as Distributed Reflective Denial of Service (DRDoS) which reached 1.7 Tbps since March 2018. This attack does not explicitly target the network but sends packets request to an exploitable third party server (i.e., the reflector) [7]. Due to the amplification effects, protocols of DDoS attacks with response messages are substantially more extensive than the request messages [8]. These DDoS attacks operate the services with no existing client-server connection. The report says that 99.27 percent of all DRDoS attacks use NTP, DNS, CharGen, SSDP, and RIPv1 protocols; they are UDP-based and have a registered or well-known port number [9]. Another DDoS attack incident on Kaspersky Labs was reported to affect one in three businesses (33 percent) since 2017 [10]. Some recent events have also shown that the occurrence of DDoS attacks has increased significantly. For example, the 2013 attack on Spamhaus generated 300 Gbps. This number spreads every year and exceeded 1 TbpS by 2016.

Among the DDoS attack, the bulk of attack traffic is IP spoofing attacks where the source IP addresses are spoofed. SYN flood attacks are an example of IP spoofing DDoS attacks, in which a large number of spoofed SYN packets are sent to target the network resources of high loads. An IP

spoofing bot node from compromised botmaster-controlled zombie systems can cause spoofing attacks. However, Distributed Denial of Service (DDoS) attacks have grown significantly accompanied by flood-based attacks such as TCP-SYN, UDP, and ICMP floods [11]. This sort of flood attack is on the rise. The purpose of these voluminous attacks is to deplete victims' computing resources such as CPU, memory, and network bandwidth by sending out an enormous number of bogus packets [12]. DDoS flood attacks can be categorized into various types, such as:

*A. Cloud computing application layer attack*

A DDoS attack on clouds has continued to develop both in volume and complexity over the years. Such attacks adversely affect the cloud provider's profitability, service quality, user experience, and credibility. DDoS attacks on the application-layer target cloud services using flood packets and usually use high-rate HTTP floods to overwhelm a cloud-hosted web server with seemingly legitimate requests. It absorbs the cloud resources and prevents access by authorized users to the target. DDoS types of HTTP flood in the application layer are difficult to handle because they use less bandwidth and are stealthier. HTTP flood attack and XML flood attack are amongst them [13].

*B. Infrastructural-layer attack*

DDoS Infrastructure Attacks (also known as flood attacks) target storage, network bandwidth, CPU circles, and TCP buffers to render them unavailable to legitimate users. In DDoS attacks at the infrastructural level, the attackers target IP address to exploit any vulnerability. DDoS flooding attack is carried out in two different forms: reflector and direct attacks [13].

i. *Reflector attack*

In a reflector-based DDoS attack, the attacker spoofs an IP address and sends a request to many reflector hosts. If the invitation is accepted, the reflector's hosts will respond to the victim node and overload it with the packets. An example of this attack is a smurf attack by sending an ICMP echo request to the hosts with a spoofed IP address (the target's IP address) over the Internet as a broadcast message. Then the hosts intensify the attack by using their ping to focus on their response to the victim [13].

ii. *Direct attack*

A direct attack requires the use of infected victim hosts/zombie computers to send huge malicious packets. It aimed at crippling the victim device by absorbing all available resources, thereby making the network inaccessible to legitimate users. These types of attacks have also occurred in the application layer and the network layer [13].

*C. Application-layer attack*

The attackers leverage network flaws or limitations in carrying out application-bug level attacks to make the services inaccessible to users. The attack Vectors include vulnerability to protocols, device instability, obsolete fixes, and misconfiguration. For instance, weaknesses in the protocol used by target applications can be exploited by attackers, sending specially designed packets to overwhelm the crash application. The ping-of-death attack investigated using 65,535 bytes of a ping packet size is greater than the permissible packet size for the application and network layer. As most modern operating systems attempt to manage these packets, they usually freeze, crash, or reboot due to buffer overflow [13].

*D. Network-layer attack*

Research has shown that the network and transport layers' protocols are used to flood the target host. The layers of such attack types are TCP SYN flood, UDP flood, ICMP flood, HTTP flood attack, and XML Flood attack [13].

*E. TCP SYN flood attack*

Transmission Control Protocol (TCP) is a connection-oriented protocol on the TCP/IP model stack (transport-layer). The connection-oriented characteristics are derived from the three-way handshaking developed between hosts before packet transmission. The connecting host receives the SYN message then the communication process is accepted by the remote host by sending an SYN-ACK message. The connecting host responds with a final ACK to complete the handshaking process and establishing the connection between two hosts. This connection feature is exploited by Attackers, initiating the half-opened connection, which exhausts the kernel memory by creating too many allocations of transmission blocks. It accomplishes executing a concerted attack by filtering weak Internet access nodes. DDoS attacks use flooding to TCP SYN can also allow the use of spoofed IP addresses. The final ACK needed to complete the link process is not received during a spoofed attack, as the host whose IP address has been spoofed might be responding with an RST flag, or the host may not exist [13].

*F. UDP flood attack*

UDP flooding started by creating disproportionate quantities of UDP packets into random target ports. The attack exploits UDP's connectivity-free and unreliability function by directing a high volume of malicious traffic to the victim to fill the response queue. UDP's unstable system doesn't allow the target system to control attackers' sending rate [13].

*G. ICMP flood attack*

ICMP is an IP protocol used to test a host's existing network connectivity status. Attackers used ICMP to launch a ping-and-smurf DDoS attack. The attack is achieved by directing

huge packets of ICMP to a target that aims to absorb the bandwidth. As a result, the victim will not answer legitimate requests from incoming users [13].

*H. HTTP flood attack*

HTTP (also known as H-DoS) flood attacks are designed to flood web servers and cloud applications using malformed HTTP packets (impersonating HTTP GET or POST requests). These attacks do not generally warrant a high traffic flow rate. For example, an HTTP GET attack can be carried out by compromising multiple nodes on the Internet to establish multiple request sessions towards the victim. New research on the global DDoS attack shows a quarter of the attacks hit the application layer by sending HTTP GET requests [13].

I. *XML Flood attack*

The users and cloud service providers use SOAP messages to boot contact when requesting XML-based services. SOAP messages function with HTTP written in XML since it is a widely applicable language on every network. Due to its ease of implementation, X-DoS, an Extensible Markup Language DoS attack, can be performed using less sophisticated instruments [13].

As a result, DDoS mitigation aims to create a robust infrastructure for the above sort of flooding attacks and to mitigate the impact of DDoS attacks on the network infrastructure. A few ways to mitigate flooding DDoS attacks are; the target network or service keep up scaling its resources or telling upstream routers (ISPs) to block the traffic near the sources to reduce the impact. However, these solutions might not be possible in all scenarios. Various techniques have been processed for DDoS mitigation, namely Software Defined Network (SDN)-based mitigation and Content Delivery Network (CDN)-based mitigation. Yet, none of the DDoS mitigation strategies used successfully; it is mainly due to their uncertainties in implementation delivery and prohibitive operating costs [14].

Nowadays, software-defined networks (SDNs) have become the primary source of cyber-attacks, such as DDoS. The concept of the Software-Defined Network (SDN) design brings new features and creates rules to mitigate DDoS threats. It enhances anti-DDoS architectures to decouple the network control plane, data plane, and programmability of controllers. As such, executing and sustaining DDoS mitigation does not generally require human involvement due to mitigation functions incorporated into SDN's application layer. Eventually, in CDN-based DDoS mitigation, a fast-multi-node CDN system helps deter and be used to mitigate or prevent DDoS attacks. CDN services are widely used by most businesses for the quick content delivery time [15].

*J. Content Delivery Network (CDN)*

The Content Delivery Network (CDN) operation is a worldwide content distribution for the users, which performs based on geographical location. CDN is used for the basis of reverse proxying, web serving, and load balancing, etc. A CDN service provider ranges over 233,000 servers based on 1,600 networks in more than 130 countries. More than 1.2 million IP addresses have been registered because of its speed and protection amid users' content distribution services [10]. Protection is part of the fast-multi-node system in CDN that benefits from delivering content as fast as possible and deters malicious attacks. A CDN manages an overlay network that reliably and efficiently delivers the content [16]. The content replicates from its host, i-e, a website, over the resources on surrogate servers spread worldwide to support end-users. End-users' requests are forwarded to the most appropriate surrogate server based on some parameters such as Internet Service Provider (ISP), geographic location, etc. Cache space on the surrogate servers is the main component of an overlay. An overlay refers to items that do not change regularly. There are two types of overlay, namely caching overlay and routing overlay. A caching overlay is more of a reverse proxy that sends a request from an end-user to a service provider and then returns the content to the end-user. A routing overlay is often used to deliver dynamic content that cannot be cached. Consequently, Content Distributed Network (CDN) employs much of today's internet service for content distribution and is predicted to increase to 71 percent by 2021 [17].

## II. AN OVERVIEW OF THE STUDY

This study aims to provide a comprehensive way to analyze DDoS attacks using mitigation techniques. This paper conducted the factual position in the hypotheses, strategies in DDoS mitigation studies. This study also points out open-ended issues that are important but not discussed in DDoS mitigation studies. These reviews extend research from Network Security to analyze, summarize, and assess DDoS attacks. In this review, topics such as Content Delivery Network (CDN) and its DDoS Defense methods are discussed.

Overall, this survey offers the most comprehensive list of fundamental theories built and used in the Content Delivery Network (CDN) and its DDoS Defense Methods. This literature review categorizes each view with various suitable techniques and presents two perspectives, such as the CDN model and its DDoS Defense Classifications from Section 2 to 3. Section 4 is a Discussion and future work, where several summaries have been highlighted that can facilitate further development in DDoS mitigation research. Lastly, the conclusion of the paper is stated in Section 5.

## III. ANALYSIS OF CONTENT DELIVERY NETWORK (CDN) MODEL

This section will address some past related studies in the area of DDoS attacks, ranging from the conventional CDN approach definition to DDoS defense classifications, and how it can be used to identify & mitigate DDoS attacks.

The CDN strategy spread the content across different data centers internationally. Big CDN service providers such as Akamai and Cloudflare deploy many servers on 1,600 networks in over 130 countries around the world [10]. The content distribution is considered into two forms, such as centralized CDN and decentralized CDN. On the one hand, the centralized CDN network's control and information are run by a central source. If the main node (central point) is corrupted, the whole information's centralized systems will fail. On the other hand, the control and information of the CDN are stored as decentralized. If one node fails or is corrupted, then the other node has the information (the system can fix itself) [18]. A centralized CDN is, therefore, less successful against an intruder (DDoS attacker) who aims to damage a content delivery network [18]. The companies that collect data are kept indefinitely by users' personal, highly sensitive data, such as document images, voice records, photos, etc. A CDN is a practical privacy approach to protect sensitive data or content that allows learning with an accurate neural-network model for a specific goal without sharing multiple data sets of inputs. Data stored centrally is subject to legal subcommittees and illegal supervision. For instance, Gringotts, an organization, allows safe monetary incentives to deliver P2P and secure decentralized contents. In Gringotts, a content provider may refuse to pay a colleague for content that has already been provided. Instead, Gringotts' opponents create fake joint clients for colleagues to make money without offering anything [19]. Sometimes this sort of problem relates to the network environment may occur so that the CDN providers send a list of peers to each file chunk to communicate with customers. The list of peer's centralized generation adds computational overhead to the content provider, which has to keep track of the peers hosting files.

A list of the peer's in the CDN provider is based on a cryptocurrency approach known as "cache cash," which sets up new caches in exchange for cryptocurrency tokens. It shows a modest Micro Cash merchant machine that can process 2.250-10.400 tickets/sec, which are about 1.67-4.1x times the MICROPAY limit, with an aggregated 60 percent reduction in payment size [19]. Such files are stored by a server to which a client has outsourced files, such as Proof-of-irretrievability, proof of data possession, and proof of storage, ensuring adequate data storage in the Content Network Delivery (CDN). Simultaneously, in comparison, a modest Micro Cash customer system may issue more than 32,000 micropayments/sec using trust. Micro-pay allows the customer to build more than 1000 escrows to support a comparable problem rate in the Content Network Delivery (CDN). It allowed Micro Cash to reduce transaction fees, add block size by about 50% of a blockchain-based public, and efficient TLS link audit scheme known as Cert chain. In particular, the Cert chain model explains a reliability-rank-dependent consensus protocol and a new data structure to help forward traceable certificates based on the cryptocurrency approach. Decentralized caching for blockchain-based content delivery regulates an efficient caching system within a blockchain-based hierarchical network. The strategic search algorithm caching performs better than random content selection, both in terms of average Cache headers (CHs) pay and the total number of offloaded deliveries. Decentralized, scalable caching software allows cache assistants that unilaterally change their strategies without requiring a centralized audit framework [20].

The subject of decentralization in the content delivery network platform meets consumer privacy between users and content providers. At this point, a new Blockchain-based Content Delivery Network Platform (B-CDN) is introduced, leveraging advances in blockchain, provides a decentralized and protected platform for linking content providers (CPs) to the users [21]. Better coordination between operators and service providers is required to enhance content delivery and resolve expected disruption due to attack traffic. Users connect to centralized servers comprising humans and computers. Such servers function as power, which all users' trust, which allows them to exchange vital information and money among trusted users. This approach also benefits the voting system. A voting system is a device that tracks every transaction in the virtual world and every physical event that occurs. For instance, the voter can complete his vote and sends data to the blockchain-based content ballot box. In this case, every consumer uses a different method to vote as an entry point, which may lead to malicious attacks such as DDoS. So the same hacking system has little impact on voting results, industries, and drains considerable capital.

Following that, the system needs many protective content resources to check such reports for voting [22]. The technical problems in B-CDN include: (1) establishing TCP connections so that IP spoofing is not an option and actual addresses should design; (2) The maximum number of links in the target parameter specifies the maximum number of connections allowed to it. These important features identify the target against an adversary who wants to make a dual-cost attack. Accelerating the dissemination of information in B-CDN will urge the cause of its distributed existence. However, both the pipeline's introduction and the connection to the closest peers reduce the time lag required for the Content Delivery Network node to announce the transaction. As a result, understanding the switching on the B-CDN can lead to protect content-based transactions. For a

network type of attack, in our case, particularly for DDoS attacks, many defense mechanisms have been performed for prevention and mitigation [21].

## IV. STUDY OF DDoS DEFENSE CLASSIFICATIONS

This section discusses various models of DDoS defense classification. One is where the defense tool is switched on, and the other is when the DDoS defense tool has to respond to a potential DDoS attack. DDoS defense classifications are split into a centralized and decentralized method. They are a signature-based method, anomaly-based method, network-based method, source-end method, victim-end method, and hybrid-based method. Nevertheless, if a node fails within a central authority, every node will easily fail [23].

One by one, we will discuss all of the DDoS defense models. Firstly, a signature-based defense method that detects only a set of known patterns of malicious data. It has disadvantages in finding and recognizing many problems with a generalization of the new attacks. The signature-based defense method is a very complex and enduring safety mechanism in mitigating attacks. For this form, therefore, the attack must be watched and updated early. Second is an anomaly-based defense method that involves the collection of data relating to irregular user behavior. It has the disadvantages of extracting network features to recognize a functional profile, requires a training phase, and a threshold value to avoid false positives and false negatives. The third is a network-based defense method, a program that defines security measures of computer networks to defend against vulnerability in denial and interruption of service from network penetration. It has disadvantages in fully implementing the process due to the high storage and overhead processing of routers. Fourth is a source-end defense method, a method that stops the streaming of attacks before entering at the end of the source network. But due to the lack of low deployment, it is unclear who (i.e., customers or service providers) would pay the expenses associated with the services. Lastly, victim-end is a defense method that measures precluding attacks at the end of the target before accessing the Internet. It has the disadvantages of identifying attacks only after it reaches the victim [23].

### *A. DDoS Mitigation Platforms*

As discussed above, there is no exact consistency at the deployment points in the types of source-based, anomaly-based, victim-based, and network-based DDoS defense methods. Clients and servers work with these DDoS mitigation mechanisms to identify and respond to attacks without tight coordination at deployment points. Besides, identification and response often centered on each deployment point (e.g., source-based defense). Unlike centralized security mechanisms, hybrid-based mitigation mechanisms are placed in multiple intermediate network locations integrating with deployment points. Therefore, a hybrid mitigation platform is an advanced system with strong trust-based cooperation at deployment points. A set of usual real-life traffic DDoS mitigation in hybrid platform finds the effect of load control and filtering [24]. When the DDoS attack comes at least from blacklisted addresses, the feature of external blacklist integration and on-demand replica server boosts the scenario-dependent level for regular clients. The Concept of DDoS Mitigation in a hybrid platform governs a system for the DDoS attack is to resize facility in the decentralized environment, guides the DDoS mitigation operation and the overall downtime. The identification of the DDoS attack impacts few other open and important directions due to the low-range attack time [1]. Practical and privacy-aware DDoS security is introduced to mitigate, regulates the hierarchical key and token management systems to boost the Internet access filtering strategy for the server [25].

There will be no fee from the service provider to the application owners because all of the DDoS mitigation processes occur before the public handles the traffic. In determining DDoS attack patterns for existing and future mitigation techniques, a useful approach to select optimal thresholds are needed. Otherwise, it may result in a high rate of false-positive and false-negative. When establishing methods for DDoS attack mitigation, traffic based on anomaly detection gets an enormous number of half-open connections [26]. To fix this problem in DDoS attacks is to disconnect the victim from the network. DDoS mitigation techniques implemented are still in their early stage. Advanced techniques of mitigating DDoS using machine learning must mean to harden the security of the network. A collective machine learning-based detection system verifies and equates the approaches to improve DDoS mitigation efficiency in SDN networks [27]. DDoS mitigation approaches based on Internet architecture generate and filter network-based attack traffic [27]. For ISP, these internet upgrades also require extensive and enforceable implementation. Strengthening Learning-based DDoS mitigation with SDN initiates to mitigate DDoS flooding attacks from different protocols and smartly learn the best mitigation policies [28].

Additionally, another open-source detection method from the Software-Defined Network design provides a secure communication link and contributes to DDoS mitigation [29]. The security issue that the SDN framework deals with QKD communication network minimizes the DDoS attacks [30]. This design guarantees authenticated, stable communication between the central controller and the device for DDoS mitigation. The collaborative based SDN acts quickly to mitigate the real-time DDoS attacks. Many network security model approaches the C-to-C protocol with SDN, namely IP spoofing, SVM algorithm, and centralized

controller [31]. SDN Strategy to Mitigate DDoS Attacks on ISP is more efficient and automated. By calculating different threats, it earns optimum protection to DDoS attacks for ISP. Threat reduction and resilience monitor the issue of the DDoS attack. It facilitates early detection and avoids further impact [32]. In the DDoS attacks, Syn flooding attacks are more complex to understand; they need TCP flags and destination ports, and (sometimes) source IP addresses. TCP source or UDP destination ports are rarely used (< 5 percent) [6]. The IP address always requires destination and the type of transport layer to manage a DDoS attack threat from the ISP and IXP inter-domain viewpoint [33]. A DDoS traffic policer on commodity hardware mitigation calculates a massive performance and measures traffic policeman named Moon Pol in DDoS mitigation. It increases the number of subnets and the different sizes of mitigation packets [34]. Also, SDN solves the issue of network-level and application-level DDoS attacks on the enterprise network.

A DDoS mitigation method in SDN governs a competent and streamlined structure to mitigate the type of TCP-SYN Flood attack. DDoS operates the flow rules and uses the designs to attack the detection time [8]. The detection time for the DDoS attack, however, is based on the polling interval. Detection needs to gather flow information from the switch regularly and use the centralized control feature to make the DDoS attack traceback and source filtering happen [35]. Attack Detection and Mitigation in Wireless Network used the Bayesian implementation method to secure the wireless network against the DDoS attack. It implements a protocol used to predict a physical layer and the different layers of the attack overcome. Using the CAPTCHA system, a series of computer bots conducts a third-party request for the attack mitigation machine to solve the problem of cross-layer or DDoS attack detection. An advantage of the described embodiment is that the DDoS mitigation and third-party validation can be performed along the ordinary request path using the Captcha machine [36].

Another DDoS mitigation design based on Network Function Virtualization (NFV) framework exploits the function of network virtualization through two-stage processes. From the concept of NFV, it uses both a dynamic

## V. DISCUSSION

Distributed denial-of-service attacks (DDoS) have become a challenge for Internet-based computer systems. A Content Delivery Network (CDN) is used to prevent DDoS attacks on websites. There are many successful preventive methods against DDoS provided by CDNs. One fundamental protection is that much of the website's content is static and cached by the CDN and thus supplied directly from the CDN servers, making it difficult for DDoS attackers [38]. The relation between the CDN and the content-origin could be obstructed by an attack, blocking requests. The only protection provided by CDNs against DDoS (1) allowing only traffic between the originating CDN and the originating content, dropping other packets, and (2) using the originating content's exclusive, hidden IP address. Usually, these defenses are costly and not always available. In particular, the use of secret IP addresses is often impossible, especially for smaller websites of the type we concentrate on when traffic load permits, who want to service clients directly from their servers. Finally, these protections frequently fail: DDoS attackers can often identify the 'secret' IP address [39].

DDoS attack research in the CDN set focuses primarily on two things, one of which uses CDNs to protect against DDoS attacks. The fundamental concept of these studies is to use CDNs as a large tool for separating and migrating routes, which means that when DDoS attacks occur, the smart DNS servers will redirect network flows to backup servers to minimize content server strain. Although the CDN network's structural function makes it more resilient for DDoS attacks, these threats are still continuously attacked by some leading CDN network equipment. For example, the DDoS incident that occurred back in 2004 was launched on Akamai's CDN, blocking nearly all links to several pages for more than 2 hours [39]. The past attack incidents show DDoS are becoming more complex, saturating various infrastructure layers and making ineffective conventional origin-based security controls. Besides, the specific and evolving nature of each DDoS attack makes it difficult and challenging to schedule, track, and mitigate the traffic. In short, minimizing DDoS on CDN networks is becoming increasingly difficult and complicated. Although the research objective is to recognize DDoS attacks' growth, it is important to highlight the risk factors. Knowing risk factors implies other researchers that can work together and provide alternative theories or mitigation techniques [40].

As a result, this review was conducted as a scoping approach to analyze the mitigation function of DDoS attacks using CDN. The CDN generally holds two methods that differentiate as collaborative method and non-collaborative method. The Centralized CDN (non-collaborative) techniques such as network-based, signature-based, anomaly-based have the scalability of low network bandwidth based on deployment points. On the other hand, the hybrid or decentralized CDN (collaborative) method has the scalability of medium-high network bandwidth in different deployment points. Research on how Content Delivery Network (CDN) is exposed during DDoS attacks (fraud/malicious) and the associated defensive and preventive measures are needed.

An approach to study DDoS mitigation is from a technical perspective, where the mentioned advantages and disadvantages of all the defense systems can generally

address as many. Still, there is no exact consistency at deployment points in the type of centralization; CDN works very little against DDoS attackers who plan to damage the system. That is why centralized strategies are vulnerable to DDoS due to their more central processes. This review proposed the hybrid or decentralized as an advanced system, which results in strong trust-based cooperation at the deployment points allocation and a reputation machine together.

TABLE I Summary of DDoS Mitigation

| Publication Details | Title | Year | Study purpose | Results Evaluation and Relative Findings |
|---|---|---|---|---|
| A. Kalliola, K. Lee, H. Lee, and T. Aura, "Flooding DDoS mitigation and traffic controller with SDN," in Flooding DDoS mitigation and traffic controller SDN, A. Kalliola, Ed. Korea: IEEE, 2015, pp. 248–254. | Flooding DDoS Mitigation and Traffic controller with SDN. | 2015 | To determine the effects of load control and filtering as an attack. A vast set of real-life usual traffic identifies synthetic attack using Traffic filtering method | The usual traffic as in the flash crowd event was played at twice than the normal rate. The issue of flow entry budget in defenSe machine signified. |
| R. Sahay, G. Blanc, Z. Zhang, and H. Debar, "At autonomic DDoS Mitigation using SDN," in Orders 2015 Workshop on Security of Emerging Networking Technologies, no. February, Reston, VA: Internet Society, 2015, pp. 319–332. | At autonomic DDoS Mitigation using SDN, | 2015 | To determine a circulated collaborative structure, It permits the users to request DDoS mitigation service from ISPs using autonomic mitigation method. | It results an autonomic DDoS mitigation structure using SDN scheme. Concluding management scalability and rule conflicts problems. |
| L. Koh, "( 12 ) United States Patent Figure 1 Thermolysin," vol. 2, no. 12, 2015, pp. 2790–2791. | Design and mechanism for internet DDoS mitigation via transit providers, | 2015 | To determine computer networks that interconnects numerous computing systems to Support their operations and the services to worldwide customers managed by transit providers. It fetches target address of a server using detection method. | It results network administration values over IP transit providers. A provider network comprising a data center described from implementation. |
| O. Osanaiye, K.-K. R. Choo, and M. Dlodlo, "DDoS resilience in cloud: analysis and conceptual cloud DDoS mitigation structure," J. Netw. Comput. Appl., vol. 67, pp. 147–165, May 2016. | DDoS Resilience in Cloud: Evaluation and Conceptual Cloud DDoS Mitigation structure.. | 2016 | To determine on DDoS attack and a conceptual cloud mitigation framework using detection and filtering method. | It performs the identification of new attack and shorter processing time. Reviewed studies on DDoS attack against cloud services and mitigation policies. |
| N. Beigi-Mohammadi, C. Barna, M. Shtern, H. Khazaei, and M. Litoiu, "CAAMP: automated DDoS attack mitigation platform in hybrid clouds," in CAAMP: automated DDoS attack mitigation platform in hybrid clouds, N. Beigi-Moha: IEEE, 2016, pp. 136–143. | Automated DDoS Attack Mitigation Platform in Hybrid Cloud. | 2016 | To determine the influences of DDoS attacks on public cloud applications using the capabilities of SDN and NFV designs using autonmic study method. | No fee will be applied from the cloud provider to application owners as all the mitigation process occurs before the traffic receives the public cloud. A scalability problem of DDoS attacks is discussed. |
| K. S. Vanitha, S. V Uma, and S. K. Mahidhar, "mitigation," 2017 Int. Conf. Circuits, Control. Commun., pp. 226–231, 2017. | DDoS: Attack methods and mitigation. | 2017 | To determine the aspects of DDoS attack methods using detection method. | It receives in a huge number of half-open connections. To fix the issue in DDoS flooding attack by disconnecting the victim form the network. |
| H. K. Jain, "System and design for SDN act DDos Attack Mitigation," Page no. 12, year 2017. | System and Design for SDN act DDoS attack. | 2017 | To determine the DDoS attack using SDN and its mitigation appliances. | It performs the function components of a central controller. The issue of DDoS attack resolved and controlled by using SDN. |
| G. Somani, M. S. Gaur, D. Sanghi, M. Conti, and R. Buyya, "Resizing facility for rapid DDoS mitigation in cloud computing atmospehere," in Service resizing for quick DDoS mitigation in cloud computing environment, vol. 72, no. 5–6, Annals of Telecommunications, 2017, pp. 237–252. | Resizing facility for rapid DDoS mitigation in cloud computing atmosphere. | 2017 | To determine the mitigation activity and overall downtime using mitigation method. | Outcomes the resizing facility algorithm, and TCP tuning method. The attack detection is impacted due to large attack low range period. A structure for overall mitigation activity is provided and basic resources like memory, |
| T. Alharbi, A. Aljuhani, and Hang Liu, "Holistic DDoS mitigation using NFV," in Holistic DDoS mitigation using NFV, T. Alharbi, Ed. United States: IEEE, 2017, pp. 1–4. | Holistic DDoS Mitigation Using NFV,. | 2017 | To determine a structure that leverages NFV and edge computing for DDoS mitigation through two-stage design processes using traditional mitigation method. | The datacenter needs the ISP control for DDoS mitigation, which outcomes in privacy problems. The privacy issue resolved by cloud-based function. |
| S. S. Mohammed et al., "A Machine Learning-based Collaborative DDoS Mitigation in SDN," Int. Conf. Wirel. Mob. Comput. Netw. Commun., vol. 2018–Octob, pp. 1–8, | A Machine Learning-based Collaborative DDoS Mitigation Mechanism in SDN. | 2018 | To determine a DDoS attacks in SDN based networks. A machine learning based on detection and mitigation technique is used. | It performs to equate the methods with increased performance and accuracy for DDoS mitigation in SDN. The problem of DDoS attacks is resolved to mitigate by machine learning in SDN. It results an DDoS mitigation in SDN with NSL-KDD model. |
| Y. Cao, Y. Gao, R. Tan, Q. Han, and Z. Liu, "Observing internet DDoS Mitigation from academic and industrial approaches," IEEE Access, vol. 6, pp. 66641–66648, 2018. | Observing Internet DDoS Mitigation from Academic and Industrial approaches. | 2018 | To determine the challenges in ISP's service and defend against DDoS attacks in the internet, SDN-based prevention method is used. | It performs filtering attack traffic internet based DDoS attacks. The problem of Defending against DDoS attacks in the internet is resolved and provides clear landscape of DDoS prevention. |
| Y. Liu, M. Dong, K. Ota, J. Li, and J. Wu, "Reinforcement Learning based Mitigation of DDoS Flooding in SDN," IEEE Int. Work. Comput. Aided Model. Des. Commun. Links Networks, CAMAD, vol. 2018–Septe, pp. 1–6, 2018. | Reinforcement Learning based Mitigation of DDoS Flooding in SDN. | 2018 | To resolve the alternate sort of attack. The reinforcement based on machine learning framework is used. | It performs to mitigate DDoS flooding attacks of different protocols and smartly learns the optimal mitigation policies. The problem of various kind of attack scenario is resolved to mitigate by using reinforcement machine learning. |

| | | | | |
|---|---|---|---|---|
| S. S. Mohammed et al., "A Machine Learning-based Collaborative DDoS Mitigation in SDN," Int. Conf. Wirel. Mob. Comput. Netw. Commun., vol. 2018–Octob, pp. 1–8, | A Machine Learning-based Collaborative DDoS Mitigation Mechanism in SDN. | 2018 | To determine a DDoS attacks in SDN based networks. A machine learning based on detection and mitigation technique is used. | It performs to equate the methods with increased performance and accuracy for DDoS mitigation in SDN. The problem of DDoS attacks is resolved to mitigate by machine learning in SDN. It results an DDoS mitigation in SDN with NSL-KDD model. |
| Y. Cao, Y. Gao, R. Tan, Q. Han, and Z. Liu, "Observing internet DDoS Mitigation from academic and industrial approaches," IEEE Access, vol. 6, pp. 66641–66648, 2018. | Observing Internet DDoS Mitigation from Academic and Industrial approaches. | 2018 | To determine the challenges in ISP's service and defend against DDoS attacks in the internet, SDN-based prevention method is used. | It performs filtering attack traffic internet based DDoS attacks. The problem of Defending against DDoS attacks in the internet is resolved and provides clear landscape of DDoS prevention. |
| Y. Liu, M. Dong, K. Ota, J. Li, and J. Wu, "Reinforcement Learning based Mitigation of DDoS Flooding in SDN," IEEE Int. Work. Comput. Aided Model. Des. Commun. Links Networks, CAMAD, vol. 2018–Septe, pp. 1–6, 2018. | Reinforcement Learning based Mitigation of DDoS Flooding in SDN. | 2018 | To resolve the alternate sort of attack. The reinforcement based on machine learning framework is used. | It performs to mitigate DDoS flooding attacks of different protocols and smartly learns the optimal mitigation policies. The problem of various kind of attack scenario is resolved to mitigate by using reinforcement machine learning. |
| F. Application, P. Data, B. Rashidi, C. Fung, and M. Rahman, "A scalable and flexible DDoS mitigation system using NFV," IEEE/IFIP Netw. Oper. Manag. Symp. Cogn. Manag. a Cyber World, NOMS 2018, vol. 1, pp. 1–6, 2018. | A Scalable and Flexible DDoS Mitigation System Using NFV. | 2018 | To determine a DDoS defense structure that utilizes (NFV) design to provide low cost and highly flexible solutions for enterprises. NFV-based defense methods is used. | It performs to legitimate traffic and mitigate SYN flood attack. The issue of DDoS attack resolved by collaboration framework among NFV. It mitigate the flow of attack by scalable and flexible in defense. |
| Z. Liu, H. Jin, Y. C. Hu, and M. Bailey, "Proactive DDoS-Attack Mitigation via Endpoint-Driven In-Network Traffic Control," IEEE/ACM Trans. Netw., vol. 26, no. 4, pp. 1948–1961, 2018. | Proactive DDoS-Attack Mitigation via Endpoint-Driven In-Network Traffic Control. | 2018 | To determine the DDoS prevention, Middle Police is able to enhance target traffic manage so that it promises to deliver victim desired traffic regardless of the attacker plan. Network-based prevention method is used. | It performs the policies with trace analysis flooded by attack traffic. The issue is resolved by deployable and proactive defense. Middle police addressed bypass vulnerability of the cloud based solution. Further work may include advanced DDoS prevention mechanism. |
| S. C. Lin, P. W. Huang, H. Y. Wang, and H. C. Hsiao, "Practical and privacy-aware cloud-based DDoS mitigation," IEEE/IFIP Netw. Oper. Manag. Symp. Cogn. Manag. a Cyber World, NOMS 2018, pp. 1–6, 2018. | DAMUP: Practical and Privacy-aware Cloud-based DDoS Mitigation,. | 2018 | To determine DAMUP, it is used to enhance the server's filtering plan on the internet service. It utilized hierarchical key ant token management method. | It performs the evaluation of DDoS mitigation. It resolved the privacy issues of filtering packets on proxies by using DAMUP architecture. |
| G. Somani, M. S. Gaur, D. Sanghi, M. Conti, and M. Rajarajan, " Quick mitigation of cloud DDoS attacks," IEEE Trans. Dependable Secur. Comput., vol. 15, no. 6, pp. 959–973, 2018. | Quick Mitigation of Cloud DDoS Attacks. | 2018 | To determine the attacks, scale inside-out used as a method to reduce the resource utilization factor of the attack. | It performs a huge number of connections in absorbing the attack and also the real time attack. A real time DDoS attack function resolved the resource scaling during attack. |
| T. Lukaseder, K. Stölzle, S. Kleber, B. Erb, and F. Kargl, "An SDN-based Strategy for Defending Against Reflective DDoS Attacks," Proc. - Conf. Local Comput. Networks, LCN, vol. 2018–Octob, pp. 299–302, 2018. | SDN Strategy to Mitigating DDoS Attacks. | 2018 | To determine mitigation, SDN is more efficient method and automated for mitigation on ISP. | It receives an optimal mitigation to DDoS attacks for ISP by estimating various attacks. The issue of DDoS attacks on enterprise network, both transport and application layers are resolved by SDN approach. |
| N. Hinze, M. Nawrocki, M. Jonker, A. Dainotti, T. C. Schmidt, and M. Wählisch, "A Potential of BGP Flowspec for DDoS Mitigation at Two IP Sources," pp. 57–59, 2018. | A Potential of BGP Flowspec for DDoS Mitigation at Two IP Sources. | 2018 | To determine a DDoS attacks major threat in inter domain perspective of ISP and IXP. BGP Flowspec methods is used for mitigation. | It performs to mitigate the attacker and malicious traffic. The issue of DDoS attacks between two sources has resolved. BGP flowspec drops the invalid traffic close to the attack. |
| Q. Xu, C. Jin, M. F. B. M. Rasid, B. Veeravalli, and K. M. M. Aung, "Decentralized Content Trust for Docker Images," Proc. 2nd Int. Conf. Internet Things, Big Data Secur., no. IoTBDS, pp. 431–437, 2017. | Decentralized Content Trust for Docker Images. | 2017 | To determine the use for malicious purpose like siphoning data and impersonation. Decentralized content method is used for mitigation. | It performs the estimation of content by using simulations. The problem of protection and trust with failures and DoS attacks is resolved. |
| Z. Liu, Y. Cao, M. Zhu, and W. Ge, "Umbrella : Enabling ISPs to Offer Readily Deployable and Privacy-Preserving DDoS Prevention Services," pp. 1–11. | Umbrella : Enabling ISPs to Offer Readily Deployable and Privacy-Preserving DDoS Prevention Services,. | 2018 | To determine the defense mechanism enabling ISP to offer DDoS prevention. An umbrella design is used for prevention. | It performs the multilayered defense architecture. The issue of DDoS attacks has been resolved by DDoS prevention method. |
| S. Bhatia, S. Behal, and I. Ahmed, Distributed Denial of Service Attacks and Defense Mechanisms : Current Landscape and Future Directions Distributed Denial of Service Attacks and Defense Mechanisms : Current, no. January. 2018. | Distributed Denial of Service Attacks and Defense Mechanisms : Current Landscape and Future Directions Distributed Denial of Service Attacks and Defense Mechanisms. | 2018 | To determine the landscape of detection and defends mechanism. Multilayered defense method is used. | It performs the attack detection and defense mechanism. The problem of DDoS attacks has been resolved by defense mechanism. |
| D. Andro and N. Vr, "Machine Learning for the Internet of Things Security : A Systematic Review," no. Icsoft, pp. 563–570, 2018. | Machine Learning for the Internet of Things Security : A Systematic Review | 2018 | To determine the function of machine learning for IoT security. Machine learning method is used. | It performs machine learning the techniques and algorithms. The issue of IoT security has been resolved. |

Filtering, capacity, flow allocation, and flow balancing in NFV executes more gracious traffic rates [4]. The traffic screener will work with the resource allocation module and orchestrate to scale up and down the resources of VNF depending on the amount of traffic.

A Scalable DDoS mitigation framework using NFV results in a DDoS protection mechanism delivers low cost and highly flexible business solutions [5]. It is a scalable and flexible system of dispatching the legitimate traffic to mitigate the SYN flood attack. DDoS attack problem can solve by an NFV shared platform that eases the attack flow by being scalable and versatile in protection. And this refers to the vulnerability to dispatch scalability and large-scales based on an increased flow of DDoS attacks. DDoS-Attack Mitigation supports by Endpoint-Driven In-Network Traffic Management. It can enhance target traffic management promises to deliver desired traffic to victims irrespective of the attacker's plan using traffic filtering methods. Therefore, Network detection and mitigation of DDoS attacks needed comprehensive efforts to train user awareness from policy to network management [37]. The summary of the literature is shown in Tables 1.

## V. CONCLUSION

The survey focused on DDoS attacks and analysis of mitigation techniques using CDN. The Content Delivery Network (CDN) based mitigation methods Model has been presented in the paper (e.g., signature-based, anomaly-based, network-based, source-based, and destination-based). The paper highlights challenges and shortcomings of these methods to accelerate more growth in DDoS mitigation research and development.

## REFERENCES


[1] G. Somani, M. S. Gaur, D. Sanghi, M. Cont2244i, and M. Rajarajan, "Scale inside-out: Rapid mitigation of cloud DDoS attacks," *IEEE Trans. Dependable Secur. Comput.*, vol. 15, no. 6, pp. 959–973, 2018, doi: 10.1109/TDSC.2017.2763160.

[2] N. Beigi-Mohammadi, C. Barna, M. Shtern, H. Khazaei, and M. Litoiu, "CAAMP: Completely automated DDoS attack mitigation platform in hybrid clouds," in *CAAMP: Completely automated*, N. Beigi-Mohammadi, Ed. Toronto, [1] : IEEE, 2016, pp. 136–143.

[3] H. K. Jain, "System and Method for Software Defined Behavoral Ddos Attack Mitigation," vol. 2, no. 12, 2017, [Online]. Available: https://patentimages.storage.googleapis.com/db/97/2d/a520f15ff968d2/US9602535.pdf.

[4] V. Fulber Garcia, G. De Freitas Gaiardo, L. Da Cruz Marcuzzo, R. Ceretta Nunes, and C. R. Paula Dos Santos, "DeMONS: A DDoS mitigation NFV solution," *Proc. - Int. Conf. Adv. Inf. Netw. Appl. AINA*, vol. 2018-May, pp. 769–776, 2018, doi: 10.1109/AINA.2018.00115.

[5] F. Application, P. Data, B. Rashidi, C. Fung, and M. Rahman, "A scalable and flexible DDoS mitigation system using network function virtualization," *IEEE/IFIP Netw. Oper. Manag. Symp. Cogn. Manag. a Cyber World, NOMS 2018*, vol. 1, pp. 1–6, 2018, doi: 10.1109/NOMS.2018.8406314.

[6] S. Hameed and H. A. Khan, "SDN based collaborative scheme for mitigation of DDoS attacks," *Futur. Internet*, vol. 10, no. 4, 2018, doi: 10.3390/fi10030023.

[7] T. Lukaseder, K. Stölzle, S. Kleber, B. Erb, and F. Kargl, "An SDN-based Approach for Defending Against Reflective DDoS Attacks," *Proc. - Conf. Local Comput. Networks, LCN*, vol. 2018-Octob, pp. 299–302, 2019, doi: 10.1109/LCN.2018.8638036.

[8] T. Ubale and A. K. Jain, "SRL: An TCP SYNFLOOD DDoS Mitigation Approach in Software-Defined Networks," *Proc. 2nd Int. Conf. Electron. Commun. Aerosp. Technol. ICECA 2018*, no. Iceca, pp. 956–962, 2018, doi: 10.1109/ICECA.2018.8474561.

[9] C. Stathakopoulou, "A Faster Bitcoin Network," 2015.

[10] P. Goyal, R. Netravali, M. Alizadeh, and H. Balakrishnan, "Secure Incentivization for Decentralized Content Delivery," 2018, [Online]. Available: http://arxiv.org/abs/1808.00826.

[11] Z. Liu, H. Jin, Y. C. Hu, and M. Bailey, "Practical Proactive DDoS-Attack Mitigation via Endpoint-Driven In-Network Traffic Control," *IEEE/ACM Trans. Netw.*, vol. 26, no. 4, pp. 1948–1961, 2018, doi: 10.1109/TNET.2018.2854795.

[12] G. A. Jaafar, S. M. Abdullah, and S. Ismail, "Review of Recent Detection Methods for HTTP DDoS Attack," *J. Comput. Networks Commun.*, vol. 2019, pp. 1–10, 2019, doi: 10.1155/2019/1283472.

[13] O. Osanaiye, K.-K. R. Choo, and M. Dlodlo, "Distributed denial of service (DDoS) resilience in cloud: Review and conceptual cloud DDoS mitigation framework," *J. Netw. Comput. Appl.*, vol. 67, pp. 147–165, May 2016, doi: 10.1016/j.jnca.2016.01.001.

[14] R. Sahay, G. Blanc, Z. Zhang, and H. Debar, "Towards Autonomic DDoS Mitigation using Software Defined Networking," in *Proceedings 2015 Workshop on Security of Emerging Networking Technologies*, no. February, Reston, VA: Internet Society, 2015, pp. 319–332.

[15] T. Alharbi, A. Aljuhani, and Hang Liu, "Holistic DDoS mitigation using NFV," in *Holistic DDoS mitigation using NFV*, T. Alharbi, Ed. United States: IEEE, 2017, pp. 1–4.

[16] G. Somani, M. S. Gaur, D. Sanghi, M. Conti, and R. Buyya, "Service resizing for quick DDoS mitigation in cloud computing environment," in *Service resizing for quick DDoS mitigation in cloud computing environment*, vol. 72, no. 5–6, Annals of Telecommunications, 2017, pp. 237–252.

[17] G. Liu, W. Quan, N. Cheng, B. Feng, H. Zhang, and X. S. Shen, "BLAM: Lightweight Bloom-Filter Based DDoS Mitigation for Information-Centric IoT," *2018 IEEE Glob. Commun. Conf.*, pp. 1–7, 2019, doi: 10.1109/glocom.2018.8647872.

[18] D. Gong *et al.*, "Practical Verifiable In-network Filtering for DDoS defense," no. 1, 2019, [Online]. Available: http://arxiv.org/abs/1901.00955.

[19] G. Almashaqbeh, "CacheCash: A Cryptocurrency-based Decentralized Content Delivery Network," 2019, [Online]. Available: http://search.proquest.com/openview/71a0329ba0aa9f805deca1b26fe4223d/1?pq-origsite=gscholar&cbl=18750&diss=y.

[20] J. Chen, S. Yao, Q. Yuan, K. He, S. Ji, and R. Du, "CertChain: Public and Efficient Certificate Audit Based on Blockchain for TLS Connections," *Proc. - IEEE INFOCOM*, vol. 2018-April, pp. 2060–2068, 2018, doi: 10.1109/INFOCOM.2018.8486344.

[21] T. X. Vu, S. Chatzinotas, and B. Ottersten, "Blockchain-based Content Delivery Networks: Content Transparency Meets User Privacy," *IEEE Wirel. Commun. Netw. Conf. WCNC*, vol. 2019-April, pp. 1–14, 2019, doi: 10.1109/WCNC.2019.8885904.

[22] "Dot Defenses And Mitigation Techniques For Iot Device Manufacturers And Cybersecurity Operations by Joel Bilodeau A Capstone Project Submitted to the Faculty of Utica College May 2018 in Partial Fulfillment of the Requirements for the Degree of Master of ," no. May, 2018.

[23] S. Gupta, D. Grover, and A. Bhandari, "Detection Techniques against DDoS attacks: A Comprehensive Review," *Int. J. Comput. Appl.*, vol. 96, no. 5, pp. 49–57, 2014, doi: 10.5120/16794-6390.

[24] A. Kalliola, K. Lee, H. Lee, and T. Aura, "Flooding DDoS mitigation and traffic management with software defined networking," in *Flooding DDoS mitigation and traffic management with software defined networking*, A. Kalliola, Ed. Korea: IEEE, 2015, pp. 248–254.

[25] S. C. Lin, P. W. Huang, H. Y. Wang, and H. C. Hsiao, "DAMUP: Practical and privacy-aware cloud-based DDoS mitigation," *IEEE/IFIP Netw. Oper. Manag. Symp. Cogn. Manag. a Cyber World, NOMS 2018*, pp. 1–6, 2018, doi: 10.1109/NOMS.2018.8406312.

[26] K. S. Vanitha, S. V Uma, and S. K. Mahidhar, "mitigation," *2017 Int. Conf. Circuits, Control. Commun.*, pp. 226–231, 2017.

[27] S. S. Mohammed *et al.*, "A New Machine Learning-based Collaborative DDoS Mitigation Mechanism in Software-Defined Network," *Int. Conf. Wirel. Mob. Comput. Netw. Commun.*, vol. 2018-Octob, pp. 1–8, 2018, doi: 10.1109/WiMOB.2018.8589104.

[28] Y. Cao, Y. Gao, R. Tan, Q. Han, and Z. Liu, "Understanding internet DDoS Mitigation from academic and industrial perspectives," *IEEE Access*, vol. 6, pp. 66641–66648, 2018, doi: 10.1109/ACCESS.2018.2877710.

[29] Q. Yan, W. Huang, X. Luo, Q. Gong, and F. R. Yu, "A Multi-Level DDoS Mitigation Framework for the Industrial Internet of Things," in *A Multi-Level DDoS Mitigation Framework for the Industrial Internet of Things*, vol. 56, no. 2, 2018, pp. 30–36.

[30] E. Hugues-Salas *et al.*, "Experimental Demonstration of DDoS Mitigation over a Quantum Key Distribution (QKD) Network Using Software Defined Networking (SDN)," p. M2A.6, 2018, doi: 10.1364/ofc.2018.m2a.6.

[31] T. Jánský, T. Čejka, M. Žádník, and V. Bartoš, "Augmented DDoS Mitigation with Reputation Scores," pp. 1–7, 2018, doi: 10.1145/3230833.3233279.

[32] G. Lykou, A. Anagnostopoulou, and D. Gritzalis, "Smart airport cybersecurity: Threat mitigation and cyber resilience controls," *Sensors (Switzerland)*, vol. 19, no. 1, 2019, doi: 10.3390/s19010019.

[33] N. Hinze, M. Nawrocki, M. Jonker, A. Dainotti, T. C. Schmidt, and M. Wählisch, "On the Potential of BGP Flowspec for DDoS Mitigation at Two Sources," pp. 57–59, 2018, doi: 10.1145/3234200.3234209.

[34] E. Kirdan, D. Raumer, P. Emmerich, and G. Carle, "Building a Traffic Policer for DDoS Mitigation on Top of Commodity Hardware," *2018 Int. Symp. Networks, Comput. Commun. ISNCC 2018*, pp. 1–5, 2018, doi: 10.1109/ISNCC.2018.8531043.

[35] S. Nithya and C. Gomathy, "Smaclad: Secure Mobile Agent Based Cross Layer Attack Detection and Mitigation in Wireless Network," *Mob. Networks Appl.*, vol. 24, no. 1, pp. 259–270, 2019, doi: 10.1007/s11036-018-1201-1.

[36] F. Application and P. Data, "Patent Application Publication ( 10 ) Pub . No . : US 2019 / 0047093 A1," vol. 1, 2019.

[37] S. Latifi, "Erratum to: Information Technology – New Generations," pp. E1–E1, 2018, doi: 10.1007/978-3-319-77028-4_102.

[38] W. Wang, D. Niyato, P. Wang, and A. Leshem, "Decentralized Caching for Content Delivery Based on Blockchain: A Game Theoretic Perspective," *IEEE Int. Conf. Commun.*, vol. 2018-May, 2018, doi: 10.1109/ICC.2018.8422547.

[39] D. Wang, S. Zhang, Y. Xue, and Y. Dong, "Identifying Influential Factors of CDN Performance with Large-scale Data Analysis," *2018 Int. Conf. Comput. Netw. Commun. ICNC 2018*, pp. 873–877, 2018, doi: 10.1109/ICCNC.2018.8390370.

[40] Y. Gilad, A. Herzberg, M. Sudkovitch, and M. Goberman, "CDN-on-Demand: An Affordable DDoS Defense via Untrusted Clouds," no. 1, 2017, doi: 10.14722/ndss.2016.23109.

[41] D. Wang, S. Zhang, Y. Xue, and Y. Dong, "Identifying Influential Factors of CDN Performance with Large-scale Data Analysis," *2018 Int. Conf. Comput. Netw. Commun. ICNC 2018*, pp. 873–877, 2018, doi: 10.1109/ICCNC.2018.8390370.