Denial of Service Attacks

Student Name

Institution

Abstract

Information security is one of the critical components of an organizational information technology infrastructure. With the increasing cases of cyber-attacks, it has become pertinent for business organizations to implement advanced network and data protection technologies to protect the information resources against deliberate or accidental access by unauthorized individuals. Denial of service (DoS) is a common cyber-attack that is usually targeted at denying legitimate users access to a specific resource in the network. While DoS attacks are not primarily made for theft, destruction, or manipulation of the stored records, they are very costly as they result in paralyzed processes, delayed business operations, canceled business deals, dissatisfied customers, and overhead expenditure to alleviate the issue. Further, in some cases, DoS attacks are used by hackers to mask an ongoing severe attack, targeting same or different network resources. This report presents a critical analysis of the DoS, and the various solutions that can be implemented dot prevent and/or mitigate the attacks in XYZ, a fictitious data analytics company.

Denial of Service Attacks

Cyber-attacks have become increasingly common in the 21st century, with their financial impact also rising tremendously. According to Bhandari, Sangal, and Kumar (2016), organizational networks are faced by different types of attacks, including but not limited to phishing, denial of service attacks, skimming, SQL injection, malwares, and brute force attacks. As such, any organization operating at a national or global scale must exhibit strong network security, characterized by up to date information technology infrastructure that is managed by information security experts. A report by Salunkhe, Jadhav and Bhosale (2017) shows that the adversities associated with a breach of organizational network are many, including possible litigations by the victims of the attack, the use of the acquired information for identity theft, tainted organizational image due to poor data security, and reduced customer trust on the organization. The main aim of breaching an organizational network is usually to steal, manipulate, and destroy specific data or make it inaccessible to the right persons (Alkasassbeh, Al-Naymat, Hassanat & Almseidin, 2016).

The denial of service (DoS) attack is a common cyber-attack that, by itself not made to steal, manipulate, or destroy organizational data but rather, to make it inaccessible. Kshirsagar, Sawant, Rathod, and Wathore (2016) explain that in some cases, the DoS attacks are used as a cover another major attack, while the attackers exploit other vulnerabilities in the network, using malwares and Trojans. This implies that DoS attacks should be dealt with absolute caution and expertise, just like other attacks. In explicating the DoS attack, Bhandari et al. (2016) posit that the end goal of the perpetrators of such attacks is disruption of service of a specific host, server, or network device in the network, thereby making it indefinitely or temporarily unavailable. This research paper presents a critical analysis of DoS attacks and the solutions that can be implemented at XYZ to avoid or mitigate different types of DOS. These types of attacks, if not resolved could lead to significant finical losses, in addition to triggering network loopholes that can be exploited by the cyber attackers.

## Summary of the Company: XYZ Data Analytics Inc.

XYZ is a fictitious company that deals with data analytics for individual and corporate customers. The company has been operational for a decade, and over the last four years, it has experienced massive growth. Currently, XYZ occupies three flours in a skyscraper building in New York. The company has 120 employees, distributed over the five departments; sales and marketing, analytics, information technology, human resource, and finance. The IT department has 10 employees; four IT personnel, two software developers who update and monitor the analytics system used; two system administrators; one information security expert; and one overall IT department manager. The duties and responsibilities of each of the IT personnel are well outlined, an aspect that promotes a coherent working environment.

The company IT infrastructure comprises of three servers, four routers, four Wi-Fi access points, and six switches, all of which are networked and placed in strategic locations. The workstations are then connected to the switches or wireless network. One of the servers is dedicated to network domain services, and active directory services, while the other two servers are made for development and live web hoisting, respectively. The organizational databases are held in the production server. It is critical to note that the network devices used by the organization are conventional and hence do not possess additional intelligence features exhibited by the advanced networking gadgets.

Recently, the organizational live web server that holds the customer database, as well as web files, was rendered inaccessible by DoS attack. The IT department detected excessive HTTP flood to the server, which overwhelmed it, thereby tempering with load balancing and resulting in freezing of the server. This, in turn, triggered unresponsiveness of the system on the front end, used by the organization staff and the customers. The issue persisted for approximately three days. Moreover, the IT department argues that this is not the first time the DoS attack has been experienced by the organization; attacks of similar nature usually happen at least once or twice a year.

## DoS Attacks Overview

A DoS attack is a type of cyber-attack that entails the prevention of legitimate users from accessing specific information resources, such as stored data in an organizational server. As such, a DoS attack is not holistic but rather, an attack that focuses on preventing the delivery of a specific information service. According to Mallikarjunan, Muthupriya, and Shalinie (2016), whereas DoS attacks can take various forms, they mostly entail the use of massive network requests that asks for the authentication of the targeted server, without having return addresses. As such the data packets used in perpetrating a DoS may have a valid or masked origin address but invalid destination; this implies that the sever ties to route them to appropriate destination to no avail. Eventually, the massive request starts overwhelming the server due to the existence of numerous requests that have been made without exist addresses.

On a different note, Mallikarjunan et al. (2016) note that DoS attacks do not necessarily have to entail the filling of the network with illegitimate traffic; the latter still can entail physical or logic disruption of the data connections, making a specific network resource unavailable. Further, DoS attacks can also target a specific individual, whereby the perpetrator can compromise an existing connection to prevent such individuals from accessing a particular service (Ďurčeková, Schwartz, Hottmar & Adamec, 2018). Some attackers also engage in disruption of the state of information, thereby making a particular service unavailable; this may entail the resetting of the transport control protocol sessions (Ďurčeková et al., 2018).

Irrespective of the approach used to steer the DoS attack, it always results in connection interference, network traffic interruption, inaccessible services, and/or ineffective service. Prolonged DoS attacks also make the network vulnerable to other forms of attacks, hence the need for the IT personnel to identify the root cause and alleviate them.

## Types of DoS Attack

DoS attacks can take numerous forms, the most common being HTTP flood, SYN flood, Ping of Death, Internet Control Message Protocol (ICMP) flood attacks, Network Time Protocol (NTP) amplification attacks, and Slowloris (Bhandari et al., 2016).

**The HTTP Flood Attack**

The HTTP flood as a type of DoS attack, whereby the perpetrators use a seemingly legitimate POST or GET HTTP requests to attack a specific web server. The seemingly legitimate data packets sent to the servers make it hard for the server to distinguish them from the legitimate ones, hence committing time in processing the invalid requests (Sreeram & Vuppala, 2017). The HTTP flood attacks are usually orchestrated using botnets that run on interconnected computers over the internet that have been taken over maliciously. As such, each of the computers sends the invalid request to the targeted server continuously, an aspect that results in voluminous HHTP requests on the server, thereby swamping it and making it impossible to process the legitimate user requests. Sreeram and Vuppala (2017) explain that for this attack f to be successful, the attackers must use either numerous hijacked machines to generate high traffic or a supercomputer.

The HTTP flood attack is quite sophisticated and capable of freezing the targeted host machine within a short period. This is because the attack does not entail the use of malformed data packets but rather, fully formed data packets that request the targeted information resource to grant the maximum resources possible to HTTP requests (Bhattacharyya & Kalita, 2016). In this sense, HTTP flood attacks do not focus on generating voluminous traffic for the purpose of consuming up the bandwidth and preventing the access of the targeted resource, but rather, overwhelming the server with numerous “illegitimate” request for resource allocation. This implies that the propagation of the attack requires a system that is capable of cloning the valid data packets in an effort to trick the servers (Kumar, 2017).

**SYN Flood Attack**

Synchronize (SYN) flood is another type of DoS attack that is commonly employed by cyber attackers. The SYN flood attack is based on the TCP three-way handshake, which entails an SYN, SYNA/ACK, and acknowledge (ACK) (Bhattacharyya & Kalita, 2016). Usually, the users of a particular web application access the server through terminal, such as workstations via a TCP connection. SYN is a short form of synchronizing message. In establishing a communication with the server, a terminal sends SYN message to the server, requesting synchronization upon successful authentication. Synchronization over the TCP connection is quite vital as it facilitates real-time data exchange, and overall improved performance of interconnected machines (Bhattacharyya & Kalita, 2016). When a client machine sends an SYN message to the server, seeking to establish a secure connection, the server responds by sending SYN-ACK message to the address from which the SYN request originated; the response is made to acknowledge the receipt of the request. A secure connection is then established by sending a final ACK to the server.

The SYN flood attack converts the three-way handshake into a two-way handshake, whereby after sending the SYN message and receiving the SYN/ACK, the perpetrating machine does not send a final ACK to establish a full connection. In such a circumstance, the server would keep the connection open, waiting for the ACK from the client computer in order to establish full connection (Kshirsagar et al., 2016). To actualize the attack, the attackers establish voluminous half-open connections to the server, which unknowingly continues assigning the computational resources to the open connections while awaiting final ACK messages to establish full connections. Eventually, the voluminous half-open connections inundate the server by depleting its computation resources; it thus becomes impossible for the server to handle any new request, whether legitimate or illegitimate (Kshirsagar et al., 2016).

Salunkhe et al. (2017) explain that the SYN flood attacks are usually lethal, and often result in crashing or malfunctioning of the server operating system (O.S) as the core functions of the O.S are starved of the computational resources. On a different note, Kshirsagar et al. (2016) explain that a SYN flood can also be sued by malicious individuals to attack a resource in the network, in order to create more vulnerabilities. For instance, a SYN flood to crash or overwhelm, a network s server, which is configured to provide the firewall and advanced security can result in weakened security of the organization network, as the malfunctioning or crashing of such a server would result in open ports and compromised information security, which can be easily exploited (Salunkhe et al., 2017).

**Internet Control Message Protocol (ICMP) flood attacks**

ICMP flood attacks are yet another DoS attack that is commonly used by malicious individuals to propagate attacks on organizational information resources. According to Gupta, Jain, and Saini (2016), this type of attack is propagated through the use of ICPM echo requests and echo replies. This attack is also referred to as the ping of death. To begin with, the ICPM is a sub-protocol if internet protocol suite, and usually used for control and diagnosis of the network devices, as well as generating and directing errors to respective IP addresses on success or failure during communication with different computers. To orchestrate the ICPM attackers, the penetrators usually send ICPM ping packets to the targeted network device such as the DNS server continuously, in order to capture its computational resources and make it unavailable to the legitimate users (Gupta et al., 2016). It is critical to note that once the server receives an ICMP message, it generates an automatic response, based on the state of the connection. This implies that the more the number of the ICPM messages sent to the server, the higher the number of ICPM responses that will be sent back.

Yihunie, Abdelfattah, and Odeh (2018) argue that this type of attack cripples the targeted network resource in two ways; first, it leads to the allocation of resources to respond to the ICPM messages thereby denying legitimate users, application programs and the operating system access to vital computation resources. Ultimately, the server becomes inaccessible. On the other hand, the numerous ICPM request sends to the server, as well as the server counter-responses for each request, also increase the network traffic, thereby consuming bandwidth and making it impossible for legitimate users to access the needed resources (Gupta et al., 2016). Some example of the ICMP messages entails the use of traceroute command and ping command, which request a response from the targeted device. Yihunie (2018) holds that even the simple ICPM messages used for diagnosis and checking the health of the connectivity, such as the ping command and trace rout, can be used to overwhelm a server, by sending numerous and continuous traceroute and ping requests.

**NTP Amplification Attack**

This is another type of DoS attack commonly experienced by the organization. Just as the name indicates, this type of attack entails exploiting the network time protocol in an effort to overload the targeted server, through the use of voluminous user datagram protocol (UDP) traffic (Sieklik, Macfarlane & Buchanan, 2016). Technically, the NTP network-based protocol is conventionally used for clock synchronization of machines in the network. This type of attack is common in the older NTP versions that allowed the monitoring and querying of the traffic counts on the NTP servers (Rytilahti & Holz, 2016).

For instance, queries such as *monlist* are used to obtain the IP addresses connected to the server in question. This implies that for a server that experiences constant access, at any point, the list could entail thousands of machines. This implies that a malicious individual can, therefore send numerous commands such as *get monlist¸, which* would eventuallyoverload the server as it tries to populate a spoofed list of IP addresses of all the host machines that have accessed it (Rytilahti & Holz, 2016). As such, while this attack does not necessarily flood the traffic with data packets, it amplifies the amount of work done by the server, therefore contributing to increased consumption of the available bandwidth and the allocation of the server resources to invalid request (Sieklik et al., 2016). Ultimately, a deadlock is arrived at, whereby the server is incapable of handling any more requests from both legitimate and illegitimate origins.

**Slowloris Attack**

Slowloris is the fifth and final type of DoS attack. Unlike other attacks, this attack is more specialized and isolative as it only affects the targeted machine and possesses minimal effects on other machines in the network that are not targeted by the attack (Choi, Park, Heo, Park & Kim, 2016). Further, this attack is designed for attacking webserver and requires minimal bandwidth. Unlike the HTTP flood attack, which entails flooding the server with GET and POST requests, this type of attack establishes communication with this server but keeps the connection open as long as possible, through the use of partial requests (Choi et al., 2016). The attack usually originates from a single computer and sends HTTP requests that are left uncompleted. To ensure that the established HTTP connection remains open, the perpetrator periodically sends HTTP headers for the respective request without completing the requests. This tricks the server into keeping the connections open while waiting for the completion, as the connections are refreshed every time the HTTP headers for the respective requests are sent.

A critical point to note is that this type of attack does not entail the use of malformed data packets that can be easily detected by intrusion detection systems; it uses legitimate data packets, only that it seeks to open multiple HTTP connections without actually completing them (Bhattacharyya & Kalita, 2016). As such, it only takes a minimal number of open HTTP connections to overwhelm the server as the connections accumulate and are allocated vital resources. The attacker, therefore, does not need to interfere with the bandwidth of the web server, but rather, establish numerous half connections even with limited bandwidth. The result is failed system that denies services to legitimate users.

**XYZ DoS Attacks**

Out of the five discussed types of DoS attacks identified, XYZ has experienced two main attacks; HTTP flood and Slowloris. Both attacks have been targeted toward paralyzing the web server, which is responsible for the serving files and web pages as per the clients’ (front-end) requests. During these two attacks, the company analytics services, which are offered through a web application, are usually paralyzed, making it impossible to execute project and handle customer orders. The company relies on the traditional server backup system, whereby routine back up is scheduled every day 11 pm to an external hard drive connected to the servers. The organization lacks a live backup server that runs parallel to the production server in case of an attack or a hiccup with the main server. Owing to this, the occurrence of a DoS attack completely paralyzes the organization's operations, as all the services have to be temporally stopped for recovery procedures to be executed and the server to be restored.

The recent DoS attacks, which happened a week ago, resulted in approximately $6000 loss to the organization is in terms of time wastage, lost business deals, customer refunds, and IT consultancy services. A projection of the company’s growth indicates that in the future, it will be handling large volumes of data from the customers, characterized by hundreds of ongoing projects that are highly sensitive in terms of data security and financial returns to the company. This, therefore, necessitates a solution that is capable of thwarting the persistent attacks

## Solutions DoS Attacks

Essentially, cyber-attacks cannot be wholly eliminated; however, the frequency and impact of the attacks can be tremendously reduced. Bhattacharyya and Kalita (2016) argue that the weaker the security of an information system, the more prone to attacks it is. This, therefore, necessitates the need to put in place strategies that are geared towards ensuring optimal data protection protocols, technologies, and policies. A study by Rytilahti and Holz (2016) indicates that DoS attacks are common among business organizations, and the cumulative effect of such attacks amounts to thousands of dollars.

**Prevention of DoS Attacks**

DoS attacks are challenging to prevent since it may be quite difficult to isolate the illegitimate traffic form the legitimate traffic, without significantly affecting the delivery of service to the users (Singh et al., 2017). With the vast technological revolution, characterized by the development of powerful computers, fast internet speeds, DoS attacks are more likely to become severe, frequent and robust. This necessitates the need for using advanced technologies to prevent such attacks too. Kshirsagar et al., 2016) recommends the integration of intrusion detection systems into organization network in order to filter out any malicious activity. Further, Burke (2018) also argues that modern intrusion detection systems run on intelligent machine learning algorithms that are capable of analyzing the network traffic, monitoring load balancing, and triggering an alert whenever an anomaly is detected. The IDS can also aid in identifying and stopping bot traffic, through the identification of IP reputation and tracking of abnormal activity, and malformed data packets (Burke, 2018).

On the other and, Sahi, Lai, Li, and Diykh (2017) recommend the use of a strong firewall, through a dedicated firewall proxy server, and intelligent routers that have inbuilt capabilities for filtering out data packets from suspicious IP addresses. A dedicated firewall server makes it possible to configure layered security of the organizational intranet, which is significantly hard to achieve using a multipurpose server. Bhattacharyya and Kalita (2017) recommend appropriate configuration of advanced features of server operating systems, specifically the production servers to disallow pings whose IP addresses do not originate from the organizational intranet. The implementation of data encryption protocols such as secure socket layer (SSL) and Transport Layer Security (TLS) can aid in filtering out suspicious IP addresses visiting a website and blocking any malicious activity, including spammers.

**Mitigation of DoS attacks**

Mitigation is a term used to describe an act of reducing the magnitude of the consequence. In this case, the mitigation entails the measures that are aimed at ensuring minimal effect on the organizational operations should a DoS attack happen. Accordion to Mustapha and Alghamdi (2018), the critical mitigation measures entails having a real-time back up of the production server and databases, characterized by sufficient network redundancy. This can be achieved through the implementation of a distributed computing architecture, supported by live backups; therefore, in case of a DoS attack on one of the servers, the backup server can kick in immediately, without the users even noticing. Load balancing triggers, intrusion detection systems, and traffic monitoring systems can be implemented to promote real-time activation of the backup server in the event that the primary server is down (Bawany, Shamsi & Salah, 2017). This mitigating measure can aid in reducing the adversities associated with financial losses, dissatisfied customers, and increased office backlogs.

Implementation of cloud computing through a platform as a service (PaaS) or infrastructure as a service (IaaS) can also aid in transferring the risk associated with DoS attacks to the service provides (Osanaiye, Choo, & Dlodlo, 2016). This would mitigate the possible negative aspects associated with a DoS attack on the information resources. On a different note, Boraten and Kodi (2016) also recommend the establishment of a qualified network security team for continuous auditing and evaluation of the network for any vulnerabilities or suspicious activity. The team can then outline fast response guidelines whenever suspicious activity is noted, including the areas to focus on, the gadgets to inspect, and the services to temporarily disable to prevent critical failure and complete DoS.

**The Recommended Solutions for DoS Attack** **at XYZ and Associated Cost**

To ensure complete security of the information resources from DoS attacks, there is the need for a multifaceted strategy, that addressee all the vulnerable areas. The recommended solution for the DoS attacks experienced at XYZ entail:

1. Procurement and installation of a dedicated Firewall proxy server
2. Replacement of the current routers with advanced intelligent routers
3. Use of intrusion detection system
4. Implementation of live server back up system
5. Implementation of next-generation firewall routers.

The cost associated with the DoS attack prevention and mitigation comes in the form of the network gadgets purchased, as well as the network security experts hired to install, configure, and provide continuous network security services.

**Implementation of Proposed DoS Solution For XYZ**

The flowing is the planned implementation of the identified solutions to prevent future DoS attacks at XYZ.

1. Use a dedicated Firewall proxy server for packet analysis and IP addresses filtering (Bhattacharyya et al., 2016). A firewall server such as the HP ProLiant DL380 Gen9 can be procured and rolled out. This is a powerful server that can be configured to provide optimal network security through a string proxy firewall. The server can be installed with IBM i Firewall software for easy and advanced configuration of the network security.
2. Use of reliable real-time server backups (Osanaiye et al., 2016): A backup server, preferably Dell PowerEdge R810 Server, can be purchased and be configured offer real-time backup, supported by a redundant network. This server runs on 128GB RAM, coupled with 4X E7-4870 40 Cores processor. As such, it is capable of withstanding constant use by numerous users.
3. Replacement of the current routers with advanced intelligent routers and switches: The organization currently runs on conventional TP-link routers and switches. These can be replaced with advanced and intelligent routers, such as Cisco Router ISR 1900 router series, and Cisco Catalyst 2960 Series switches that are capable of malicious IP monitoring ad filtering.
4. Use of the intrusion detection system for the detection of traffic anomalies in the network (Bawany et al., 2017; Burke, 2018). An intrusion detection system can as well be integrated into the network for continuous monitoring and evaluation of the traffic for any malicious activity. This can be achieved through the implementation of the Cisco stealth watch enterprise system.
5. Implementations of a strong firewall using next-generation firewall routers (Maraj, Jakupi, GRogova & Grajqevci, 2017): Finally, next-generation firewalls can be installed as well used to tighten organization intranet security, and supplement the security provided by the firewall proxy server. This can be achieved through the use of the Fortinet Next-Generation Firewall, such as The FortiGate 7060E system.

## Conclusion

Data and information have become vital organizational assets that must be protected at all costs. The 21st century has realized increased number and magnitude of cyberattacks, owing to the advanced technologies which have provided tools and technologies that can be used by malicious individuals to perpetrate advanced attacks on organizational information resources. The main aim of this report was to critically analyze the DoS attacks and how they can be prevented and/or mitigated at XYZ, a fictitious data analytics company currently faced with such attacks.

DoS attacks are a common cyber-attack, in which the main aim of the attackers is to disrupt the provision of network services, and in some cases, crash the targeted servers. The common types of DoS attacks include Flood, SYN flood, Internet Control Message Protocol flood attacks, Network Time Protocol amplification attacks, and Slowloris. While the mode of execution for these attacks is inherently deferent, they are all targeted towards denying legitimate users access to a particular service. XYZ is a company that specializes in the provision of analytics services to individual and corporate customers. The organization network is weak, characterized by the use conventional network switches and routers. Over the last couple of years, the organization has realized frequent DoS attacks, the common ones being HTTP flood and Slowloris attacks. The attacks have resulted in losses amounting to thousands of dollars. To prevent the attacks, various strategies can be undertaken, which include procurement of a dedicated Firewall proxy server, replacement of the current routers with advanced intelligent routers, use of intrusion detection system, and implementations of next-generation firewall routers is pertinent.

## References

Alkasassbeh, M., Al-Naymat, G., Hassanat, A. B., & Almseidin, M. (2016). Detecting distributed denial of service attacks using data mining techniques. *International Journal of Advanced Computer Science and Applications*, *7*(1), 436-445.

Bawany, N. Z., Shamsi, J. A., & Salah, K. (2017). DDoS attack detection and mitigation using SDN: methods, practices, and solutions. *Arabian Journal for Science and Engineering*, *42*(2), 425-441.

Bhandari, A., Sangal, A. L., & Kumar, K. (2016). Characterizing flash events and distributed denial‐of‐service attacks: An empirical investigation. *Security and Communication Networks*, *9*(13), 2222-2239.

Bhattacharyya, D. K., & Kalita, J. K. (2016). *DDoS attacks: Evolution, detection, prevention, reaction, and tolerance*. Chapman and Hall/CRC.

Boraten, T., & Kodi, A. K. (2016, May). Mitigation of denial of service attack with hardware trojans in noc architectures. In *2016 IEEE International Parallel and Distributed Processing Symposium (IPDPS)* (pp. 1091-1100). IEEE.

Burke, D. (2018). *Preventing DDOS attacks against IoT devices* (Doctoral Dissertation, Utica College). Retrieved from <https://search.proquest.com/openview/43313d89a65f45ca5e88bc172814f461/1?pq-origsite=gscholar&cbl=18750&diss=y>

Choi, J., Park, J. G., Heo, S., Park, N., & Kim, H. (2016, August). Slowloris dos countermeasure over websocket. In *International Workshop on Information Security Applications* (pp. 42-53). Springer, Cham.

Ďurčeková, V., Schwartz, L., Hottmar, V., & Adamec, B. (2018). Detection of attacks causing network service denial. *Advances in Military Technology*, *13*(1).

Gupta, N., Jain, A., & Saini, P. (2016, March). DDoS attack algorithm using ICMP flood. In *2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom)* (pp. 4082-4084). IEEE.

Kshirsagar, D., Sawant, S., Rathod, A., & Wathore, S. (2016). CPU load analysis & minimization for TCP SYN flood detection. *Procedia Computer Science*, *85*, 626-633.

Mallikarjunan, K. N., Muthupriya, K., & Shalinie, S. M. (2016, January). A survey of distributed denial of service attack. In *2016 10th International Conference on Intelligent Systems and Control (ISCO)* (pp. 1-6). IEEE.

Maraj, A., Jakupi, G., Rogova, E., & Grajqevci, X. (2017, June). Testing of network security systems through DoS attacks. In *2017 6th Mediterranean Conference on Embedded Computing (MECO)* (pp. 1-6). IEEE.

Mustapha, H., & Alghamdi, A. M. (2018, June). DDoS attacks on the internet of things and their prevention methods. In *Proceedings of the 2nd International Conference on Future Networks and Distributed Systems* (p. 4). ACM.

Osanaiye, O., Choo, K. K. R., & Dlodlo, M. (2016). Distributed denial of service (DDoS) resilience in the cloud: Review and conceptual cloud DDoS mitigation framework. *Journal of Network and Computer Applications*, *67*, 147-165.

Rytilahti, T., & Holz, T. (2016). Poster: The curious case of ntp monlist. *European S&P*, *2016*.

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

Salunkhe, H., Jadhav, S., & Bhosale, V. (2017). Analysis and review of TCP SYN flood attack on a network with its detection and performance metrics. *IJERT*, *6*(1), 250-256.

Sieklik, B., Macfarlane, R., & Buchanan, W. J. (2016). Evaluation of the TFTP DDoS amplification attack. *Computers & Security*, *57*, 67-92.

Singh, K., McKee, P., & Kumar, K. (2017). Application layer HTTP-GET floods DDoS attacks: Research landscape and challenges. *Computers & Security*, *65*, 344-372.

Sreeram, I., & Vuppala, V. P. K. (2017). HTTP flood attack detection in application layer using machine learning metrics and bio-inspired bat algorithm. *Applied Computing and Informatics*. Retrieved from <https://www.sciencedirect.com/science/article/pii/S2210832717301655>

Yihunie, F., Abdelfattah, E., & Odeh, A. (2018, May). Analysis of ping of death DoS and DDoS attacks. In *2018 IEEE Long Island Systems, Applications, and Technology Conference (LISAT)* (pp. 1-4). IEEE.