Kasu Journal of Computer Science Vol. 1 No. 4 [December, 2024], pp. 778-795
https://doi.org//10.47514/kjcs/2024.1.4.006

Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

DDoS Attacks on Cloud Computing and IoT Devices: Strategies for Mitigation

Joshua John[1] and Egba Anwaitu Fraser[2]
[1]Iya Abubakar Institute of Information and Communication Technology, Ahmadu Bello University, Zaria, Kaduna State, Nigeria
[2]Department of Computer and Robotics Education, Federal College of Education Technical Omoku, Rivers State, Nigeria
jjoshua@abu.edu.ng[1], egbaaa2@gmail.com[2]

Abstract

This study has the goal of developing security model that detected and prevented the risks of Distributed Denial of Service (DDoS) attacks in cloud computing systems and IoT devices which are gravely potent and on the increase today, especially with the rapid growth of internet during the last one and a half decades. This is more prevalent because of the several benefits that an organization enjoys after adopting cloud computing and Internet of Things (IoT). However, the harm that may result after a DDoS attack on a cloud computing infrastructure or service and IoT devices can be very huge, and all efforts must be made to secure it. Therefore, the traditional security mechanism cannot satisfy the security requirements of cloud computing and IoT. While several models exist on tackling this menace which operate on a particular layer (mostly layer 3) of the Open System Interconnection (OSI), we have developed a cloud-based hybrid defense and detection mechanism to prevent DDoS attacks in cloud computing environment and IoT that operates in layers 3 (network), 4 (transport) and 7 (application) of the OSI model. This was done using two approaches: analyzing Transmission Control Protocol/Internet Protocol (TCP/IP) header features of incoming packets in cloud computing environment in order to detect and classify spoofed IP address during DDoS attack via a custom-made Web Application Firewall (WAF); and the integration of the cloud resources with Cloudflare. In the first instance, TCP syn flood attacks were targeted to a particular webserver on port 80 through an attacking lab machine. This machine did not have this custom-made WAF (prevention/detection mechanism) against these attacks. There was 100% packet loss as no replies were received, overwhelming the system. The result shows that a total of 1,625,192 packets were transmitted in a short period which were captured and analyzed via Wireshark. Several TCP errors were observed over a very short time interval which indicated successful DDoS attack effectively crashing the system. The result varied when the custom-made WAF was put in place, and the attacking lab machine launched a TCP syn flood attack against the web server on port http port 80. A total of 2,353,585 packets were transmitted in a short period which were captured and analyzed using Wireshark and contained less TCP errors indicating successful mitigation of DDoS attacks. When the resources were hosted online and integrated with Cloudflare, integrity checks were successful before the resources were loaded, indicating complete mitigation of attacks. In the end, an enhanced, cloud-based, hybrid (WAF + Cloudflare) security model that prevented the risks of DDoS attacks on cloud computing and IoT devices was designed and implemented. The methodology adopted for this research work is Open Source Security Testing Methodology Manual (OSSTMM) and programming language used is batch script. The model will be useful in education, healthcare, ecommerce, financial, political/electoral, web hosting providers/ISPs offices, homes and online gaming sites. However, these advancements also make IoT and cloud applications vulnerable to a variety of security threats. To broaden the scope of this research, it is recommended to extend the study to include Man-in-the-Middle (MitM) attacks and routing attacks targeting IoT devices and cloud applications.

Keywords: Botnet, DDoS, Cybersecurity, Mirai and Network

Kasu Journal of Computer Science Vol. 1 No. 4 [December, 2024], pp. 778-795
https://doi.org//10.47514/kjcs/2024.1.4.006
Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

1. Introduction

Cloud computing and Internet of Things have expanded rapidly and dramatically all over the world. The estimated number of cloud-connected devices between 2025 and 2030 ranges from 23 to 25 billion, while the number of IoT devices is projected to reach 40 billion IoT devices by 2030 (Sinha, 2024). Cloud Computing is the delivery of computing services, including servers, storage, databases, networking, software, analytics, and more over the internet (Cloud). These Cloud services are offered in the form of Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). Internet of Things(IoT) is an interconnection of trillion of devices over the Internet which can sense, communicate and actuate in the environment and among themselves (Hassan, 2018). Internet of Things (IoT) on the other hand, is defined as a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers (UIDs) and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction.(Gillis, 2022) Additionally, it enables the collection of data through the monitoring or census of physical, chemical, or biological variables, as well as facilitating communication between devices, human-device interactions, identification, location tracking, and monitoring, among other functions. The advent of emerging technologies has introduced new avenues for cyber attacks. Cyber attacks on these devices are often attributed to botnets; Botnets are also known as "zombie armies" is a group of infected computers under the control of attackers used to perform various scams and cyber-attacks. The attackers use malware to take control of vulnerable IoT and cloud computing devices to block legitimate users from accessing internet services by executing DDoS attacks. A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic. The more Internet-connected devices there are, the greater the potential for extremely large botnets. The widespread adoption of the Internet of Things (IoT), cloud computing, artificial intelligence (AI), and blockchain has opened up new attack vectors and vulnerabilities. The increasing complexity of network security and the rise of cyberattacks, specifically Distributed Denial of Service (DDoS) attacks, pose significant challenges and many users and enterprises are reluctant to migrate to cloud computing and Internet of Things (IoT) technologies. The ultimate goal of a DDoS hacker who hacks into an IoT and cloud computing device is not to interfere with consumer heating systems or interrupt their morning coffee ritual; rather, the aim is to harness thousand network resources like a server or a website to turn them into a zombie army. The impact of such attacks includes overwhelming resources, leading to service outages, performance issues, higher costs, data breaches, reputational harm, exploitation of IoT devices as botnets, and challenges in recovery efforts.

1.1 Understanding DDoS Attacks: Targets and Types

A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic. DDoS attacks achieve effectiveness by utilizing multiple compromised computer systems as sources of attack traffic. Exploited machines can include computers and other networked resources such as IoT devices. From a high level, a DDoS attack is like an unexpected traffic jam clogging up the highway, preventing regular traffic from arriving at its destination.

1.1.1 How does a DDoS attack work?

DDoS attacks are carried out with networks of Internet-connected machines. These networks consist of computers and other devices (such as IoT devices) which have been infected with malware, allowing them to be controlled remotely by an attacker. These individual devices are referred to as bots (or zombies), and a group of bots is called a botnet. Once a botnet has been established, the attacker is able to direct an attack by sending remote instructions to each bot. When a victim's server or network is targeted by the botnet, each bot sends requests to the target's IP address, potentially causing the server or network to become

Kasu Journal of Computer Science Vol. 1 No. 4 [December, 2024], pp. 778-795
https://doi.org//10.47514/kjcs/2024.1.4.006
Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

overwhelmed, resulting in a denial-of-service to normal traffic. Because each bot is a legitimate Internet device, separating the attack traffic from normal traffic can be difficult. A typical setup on how DDoS Attack is performed showed in Figure 1

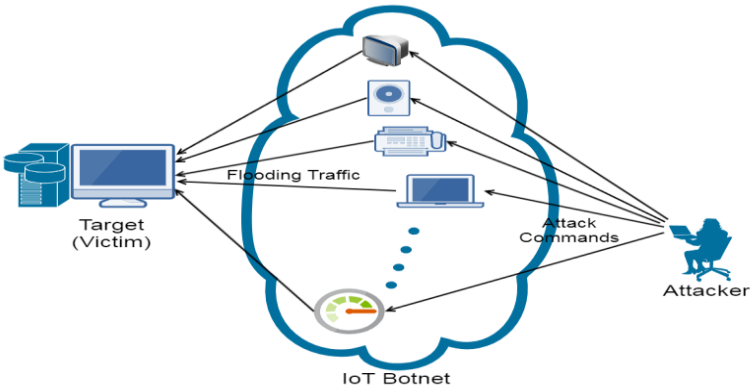

Figure 1: Illustrating how DDoS Attack is performed

1.1.2 Taxonomy of various IoT-based DDoS attacks

IoT attackers aim to exploit the security vulnerabilities and infiltrate systems. Their goal is multi-dimensional and hence it is not limited to a single layer or security principles. DDoS attacks exhibit a broader range of diversity and intricate due to heterogeneity of IoT devices. All such attacks can be further classified in terms of different IoT Layers. An essential point to note regarding DDoS attack classification is its dependency on the impact within an IoT network's server site. DDoS attack categories resemble traditional ones but adapt to the network architecture as a reference model. Another DDoS class emerges, centered on generating numerous pseudo requests from IoT sources to target servers. Currently, the sole known method to generate this volume of fraudulent requests via the IoT network involves the use of bots and malware (Mäki, et al, 2016). Here we are classifying the DDoS attacks at various layers of the IoT network as shown in Fig. 8. Every layer can be specifically targeted to compromise the security of an IoT network. Figure 2: DDoS attacks taxonomy in IoT

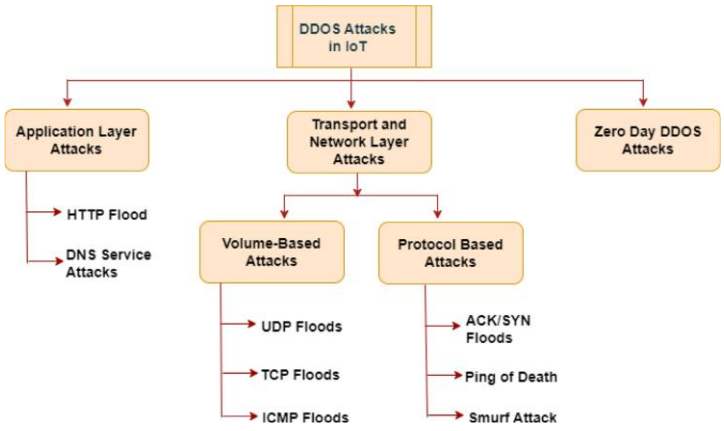

Figure 2: DDoS attacks taxonomy in IoT layered architecture.

1.1.3 Taxonomy of various Cloud-based DDoS attacks

Kasu Journal of Computer Science Vol. 1 No. 4 [December, 2024], pp. 778-795
https://doi.org//10.47514/kjcs/2024.1.4.006
Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

Distributed Denial of Service (DDoS) attacks pose a serious threat to cloud computing environments by overwhelming resources and making services inaccessible. Within the framework of a cloud computing layered architecture, these attacks can be classified based on the targeted layer, the techniques employed, and the attack vectors. Figure 3:A taxonomy of DDoS attacks in such environments.

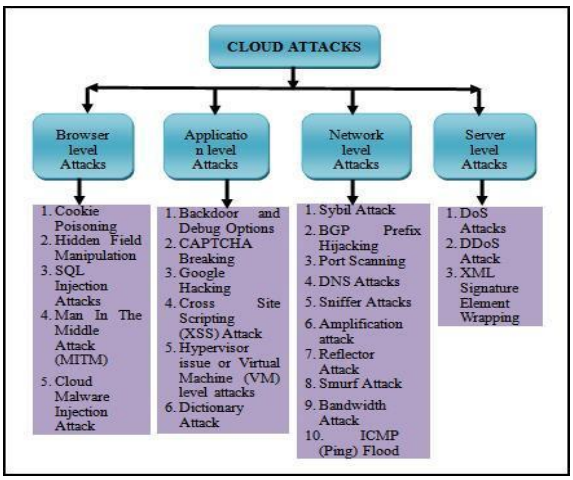

Figure 3: DDoS attacks taxonomy in Cloud-based DDoS attacks

1.1.4 Targets of DDoS Attacks

DDoS attacks can target various components, such as applications, hosts, networks, or infrastructure (Mirkovic & Reiher, 2004).Although the specific effects may vary depending on the targeted point in the communication channel, the primary objective remains consistent: to disrupt services at some level. For instance, a network-targeted DDoS attack may differ in impact from an application-focused attack, yet both aim to degrade the victim's ability to provide services to its clients. In a network-based DDoS attack, the attacker may overwhelm the victim's connection bandwidth, rendering it inaccessible to legitimate users. Conversely, an application-based DDoS attack might involve sending a smaller number of malicious packets designed to disrupt the application's resource allocation mechanisms. Among the potential targets of DDoS attacks applications, hosts, networks, and infrastructure all are vulnerable to service degradation or disruption.

1. 2 Types of DDoS Attacks

A very typical example of a DoS or DDoS attack is designed to attack a single server, network or application with an overwhelming number of requests, packets or messages, so that the users of the server cannot connect to it or get the service that they expect from this server. DDoS attack becomes successful and this attack imposes some direct and indirect effects on the services and revenues. It has also led to distributed attacks such as IP spoofing, SYN flooding, buffer over-flow, ping of death, smurf, **U**DP flood attack, ICMP flood, the slowloris,Teardrop, and land attack are some examples of DDoS attacks in the cloud platforms (Darwish et al., 2013). These attack methods are presented below:

1.2.1 IP Spoofing Attack

Kasu Journal of Computer Science Vol. 1 No. 4 [December, 2024], pp. 778-795
https://doi.org//10.47514/kjcs/2024.1.4.006
Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

In an Internet Protocol (IP) spoofing attack, packet transmissions between the end user and cloud server are intercepted. Their headers are modified so that the IP source field in the IP packet is forged by using either a legitimate IP address or an unreachable IP address, as shown in Figure 4. Consequently, the server responds to the legitimate user machine, thereby affecting that machine, or the server is unable to complete the transaction to the unreachable IP address, which affects the server resources. Tracing such an attack is difficult because of the forged IP address in the IP source field of the IP packet.

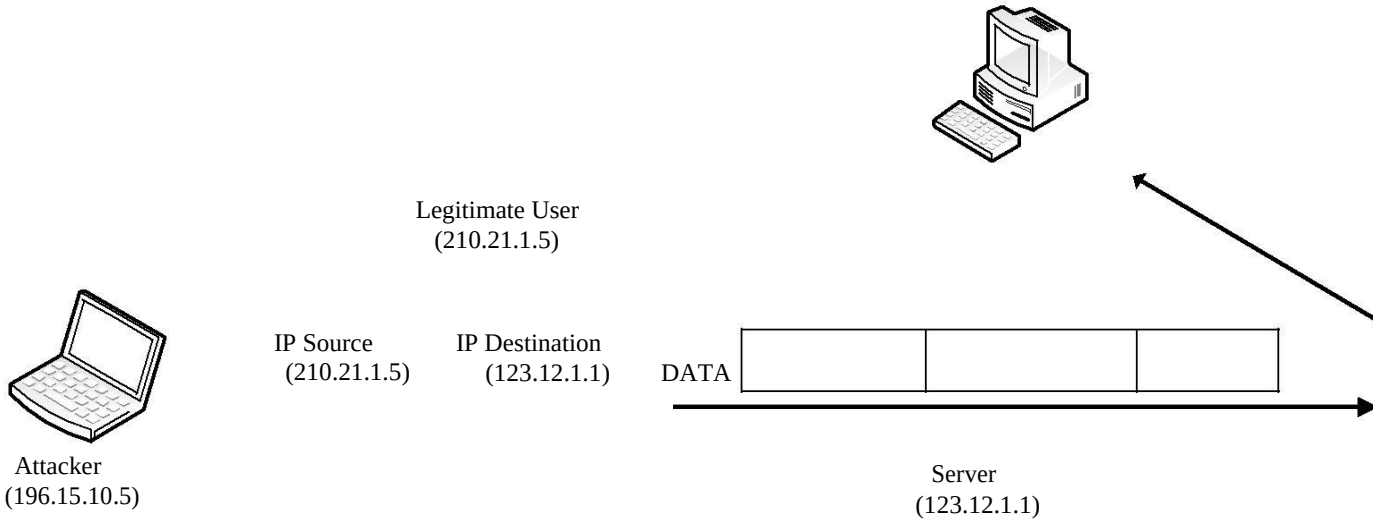

Figure 4: IP spoofing attack

1.2.2 SYN Flooding Attack

A Transmission Control Protocol (TCP) connection starts witha three-way handshake, as shown in Figure 5. A typical three-way handshake between a legitimate user and the server begins by sending a connection request from the legitimate user to the server in the form of a synchronization (SYN) message. Subsequently, the server acknowledges the SYN message by returning a request (SYN-ACK) to the legitimate user. Finally, the legitimate user sends an ACK request to the server to establish the connection. SYN flooding occurs when the attacker sends innumerable packets to the server but does not complete the three-way handshake process. Consequently, the server waits to complete the process for all of those packets. This prevents the server from processing legitimate requests. Moreover, SYN flooding can be executed by sending packets with a spoofed IP address. A sniffing attack is considered a type of SYN flooding attack. In a sniffing attack, the attacker sends a packet with the predicted sequence number of an active TCP connection with a spoofed IP address. Thus, the server is unable to reply to that request, thereby affecting the performance of the cloud system because of extensive resource consumption (Niraj et al., 2012).

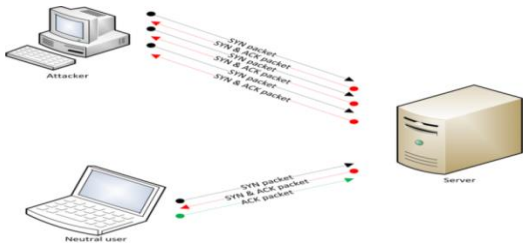

Figure 5: SYN Flooding Attack

Kasu Journal of Computer Science Vol. 1 No. 4 [December, 2024], pp. 778-795
https://doi.org//10.47514/kjcs/2024.1.4.006
Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

1.2.3 Smurf Attack

In a smurf attack, the attacker sends many Internet Control Message Protocol (ICMP) echo requests. These requests are spoofed so that their source IP address is the IP address of the victim, and the IP destination address is the broadcast IP address, as shown in Figure 6. Therefore, the victim is flooded with broadcasted addresses. In the worst-case scenario, the number of hosts who reply to the ICMP echo requests is excessively large (National Institute of Standards and Technology, 2004).

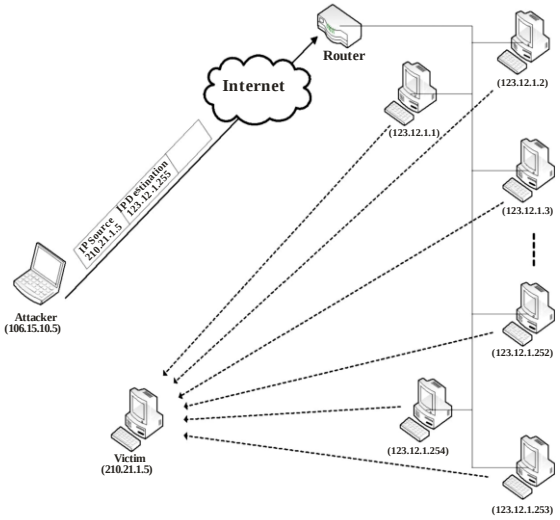

Figure 6: Smurf Attack

1.2.4 Ping of Death

In the ping of death attack, the attacker sends an IP packet larger than the IP protocol limit, which is 65,535 bytes, as shown in Figure 7. Processing an oversized packet affects both the victim machine within the cloud system and the cloud system resources (Ping-of-death-attack (2017).

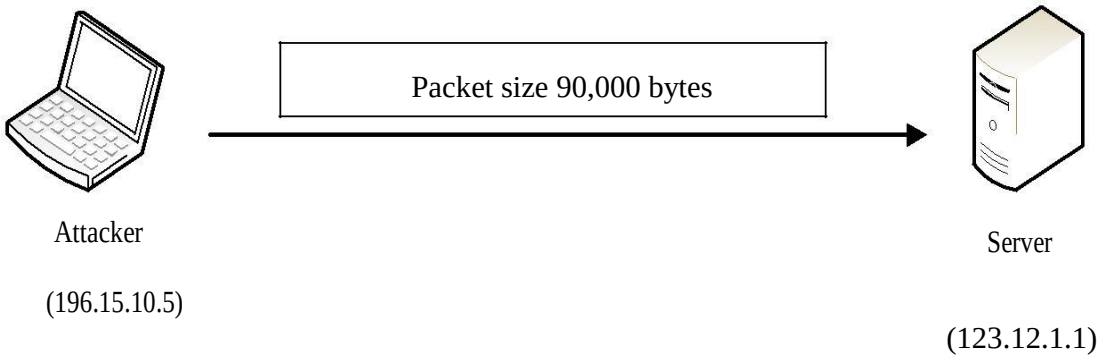

Figure 7: Ping of death attack

Kasu Journal of Computer Science Vol. 1 No. 4 [December, 2024], pp. 778-795
https://doi.org//10.47514/kjcs/2024.1.4.006
Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

1.2.5 Teardrop Attack

In this form of attack, based on the IP protocol, the attack is launched by sending malformed fragmented TCP/IP packets with their fragment offset fields overloaded. This offset is one of the fields in the IP header. It indicates the starting position, or offset, of the data contained in the fragmented TCP/IP packet relative to data of the unfragmented packets. So that fragment offset is not in accord with the packet length of the fragment. Therefore, this discrepancy can cause the victim host to crash or reboot when it tries to reassemble the fragment TCP/IP packet. Figure 8 shows the details of the teardrop attack mechanism (Chopade et al., 2013).

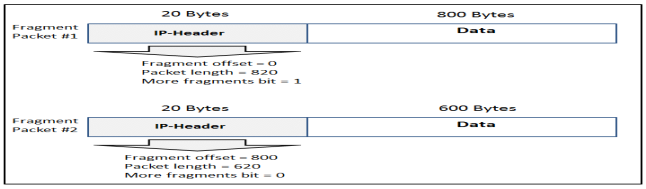

Figure 8: Teardrop Attack

1.2.6 Buffer Overflow Attack

The attacker sends an executable code to the targeted system in order to create buffer overflow attack. In such way, the victim's machine will be controlled by the attacker. As a result, the attacker can use the infected machine to perform cloud based DDoS attack, as in figure 9 Patel &Borisagar, 2012).

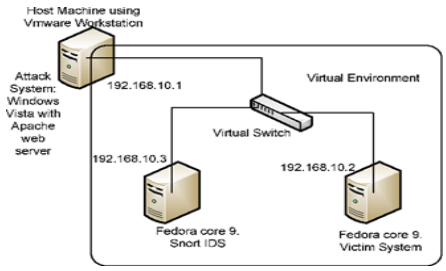

Figure 9: Buffer Overflow Attack

1.2.7 Land Attack

It is similar to ping attack where it uses "land.c" program to send the modified TCP/SYN packets with the victim's IP address in both source and destination IP fields. As a result, the machine itself sends the requests and crashes. DDoS attacks are highly distributed, offensive assaults on services, hosts and infrastructure of the Internet (Ouda et al., 2013). As seen in figure 10.

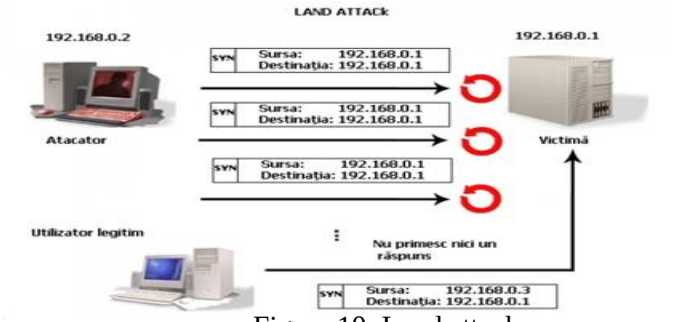

Figure 10: Land attack

Kasu Journal of Computer Science Vol. 1 No. 4 [December, 2024], pp. 778-795
https://doi.org//10.47514/kjcs/2024.1.4.006

Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

2. Related Works

The adoption of cloud computing and IoT devices has revolutionized data storage and processing. However, it has also introduced unique security concerns that should be understood to enable us improvise solutions to the challenges that could arise from misconfigurations, inadequate access controls, and vulnerabilities in cloud infrastructure which are also responsible for data breaches and unauthorized access to sensitive information. Many studies have been made of how to handle DDoS attacks and many elegant algorithms have been suggested. Some research deals with attack prevention and/or detection, some focus about how to filter DDoS attack and some research considers attack trace back. Here we discuss different research papers.

Bhardwaj et al. (2021) in their paper presented the state-of-the-art of the DDoS attacks in the cloud. They mentioned the DDoS incidents which occurred since 2014, with the objective to demonstrate how DDoS attacks can targeted cloud platforms and consequently the importance of implementing and evolving DDoS solutions. They also described the different types of DDoS attacks that can be performed on cloud infrastructures, cloud services and cloud costumers. Alharbi et al. (2021) proposed a Local Global Best Bat Algorithm with Neural Network (LGBBA-NN) for selecting hyper parameters and feature subsets for effective detection of botnet attacks. The presented hybrid approach adapted the inertia weights from the LGBB algorithm to update the parameters of the solution in the swarm. In order to address the swarm diversity for the solutions, a Gaussian distribution was employed during the initialization of the population. However, Ahuja et al. (2021) proposed a hybrid ML model Support Vector Classifier with Random Forest (SVC-RF) for the classification of traffic as BENIGN or DDoS. The authors extracted the number of features from the original dataset and created a new dataset called SDN dataset with novel features. The proposed model results showed that the classifier SVC-RF can successfully classify the traffic with an accuracy of 98.8% using SDN dataset. Similarly, a network Intrusion Detection System (IDS) to detect attacks and malicious activities in Cloud environment was designed by Ghosh et al. (2018). The proposed IDS include two stages. The first stage consists of creation of a feature subset by using a novel algorithm called BCS-GA which combines the advantages of Binary Cuckoo search algorithm (BCS) and Genetic Algorithm (GA). The proposed BCS-GA algorithm was applied on NSLKDD training dataset to remove several irrelevant features, in order to reduce the training time and memory storage space required for such high dimensional dataset. Thus, initial NSLKDD dataset contains 41 features, but after applying BCS-GA algorithm, it successfully reduced to 16 features. In the second stage, Neural Network classifier was trained by the reduced training dataset using 16 features. Thereafter, classification accuracy of that classifier was tested by means of a separate reduced testing dataset. Experimental results indicate that the proposed IDS produce 78.229% of accuracy. Zekri et al. (2017), focused on how Distributed Denial of Service affects cloud performance by utilizing network resources. The attack techniques implemented and evaluated different ML algorithms in a cloud computing environment. The authors presented a DDoS protection design, and the algorithms they implemented and evaluated in cloud environments were Naive Bayes, Decision Tree (C4.5), and K-Means (KM). The results showed that their accuracy and detection time of algorithms Naive Bayes, Decision Tree (C4.5), K-Means were 91.4% in 1.25 s, 98.8% in 0.58 s, and 95.9% in 1.12 s, respectively. This approach can work on real-time anomaly detection and mitigation techniques and other security challenges. The drawback of this approach is that they evaluated only a few models to detect DoS attacks. In another study, a novel security model for authentication-supported cloud computing was advocated by Rajeswari, et al. (2017). The model introduced a new idea for a biometric security system based on fingerprint recognition. The proposed method automated the verification process to match human fingerprints, where fingerprints are used to identify the individuals and verify their identity. Users are authenticated based on the fingerprint templates, which must be given based on random numbers generated each time. The experimental results showed that the proposed system outperforms the single-fingerprint authentication system. Tamanna (2016) discussed about the cloud computing, the form of IoT, that has

Kasu Journal of Computer Science Vol. 1 No. 4 [December, 2024], pp. 778-795
https://doi.org//10.47514/kjcs/2024.1.4.006
Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

taken the computing from the desktop to the Internet, and the DDoS attacks that happen in this cloud environment. This author proposes a solution against the DDoS attacks in the form of Software Defined Networks (SDN) features, since SDN is flow based concept with standardized API and support for IDSs and Intrusion Prevention Systems (IPSs). The work from Salim et al. (2019) makes a survey of DDoS attacks in IoT. The paper discusses the motivations why attacker choose IoT devices, as well as the motivations why attacker precede to do DDoS attacks. It also describes some DDoS attack types and DDoS attack tools. The authors provide a deep description of DDoS defense mechanisms, in which they divide in three categories: prevention, detection and mitigation. To help visually it is demonstrated a table with all defense mechanisms and DDoS attacks type, presented in the paper, in which those attacks that are protected by the defense mechanism are marked, therefore is easily visualized which attacks are defended with which mechanisms. Ahmed, et al (2023) addressed novel application layer DDoS attacks by analyzing incoming packet characteristics, such as the size of Hypertext Transfer Protocol (HTTP) frame packets and the number of Internet Protocol (IP) addresses sent. They employed a deep learning algorithm called Multi-Layer Perceptron (MLP). Based on simulation results, the proposed algorithm achieved a high detection efficiency of 98.99% for DDoS attacks, effectively safeguarding the IoT infrastructure. Shoket and Aulakh (2018) concentrated on improving Voice over LTE (VoLTE) and Voice over IP (VoIP) network security. They proposed the Packet Level Restraining Technique (PLRT) approach, which identifies the source of DDoS attacks and prevents the affected node from connecting to the entire network. This method effectively mitigates DDoS attacks and their impacts on the network. Dao et al (2017) discussed about the heterogeneous IoT networks, which are characterized by multiple access technologies and mobile edge computing capabilities, and securing them from the intelligent DDoS attacks. The solution they propose as a prevention of DDoS attacks is called MECshield, a framework consisted of central controller and multiple agents located at the edge of each local network, which enables the network to defend against malicious traffic.In their paper, authors Peraković et al (2019) analyze data that they collected from the domestic company regarding the trends in DDoS attacks. Through their research, it is stated that the Simple Service Discovery Protocol (SSDP) is the most common when it comes to conducting DDoS attacks. They also analyzed the amount of these attacks happening in regarding IoT, and concluded that the rise in IoT devices also mean rise in the DDoS attacks. Simple study on handling DDoS attacks has been conducted by the Mukhopadhyay et al (2015), where they presented four major approaches that can be considered in order to defend against these attacks. Given approaches for defense against DDoS attacks are by rate limit framework, defense by offense, by active filtering and by IP traceback. In the research conducted by Khalil (2017), the main topic was the security of Internet of things against DDoS attacks, where he talked about the security measures by using machine learning algorithms. Author provides algorithm that helps in monitoring, analyzing and recognizing attack patterns .In the paper, Dao, (2017) touched upon the malwares in IoT with DDoS capabilities. The malwares, such as Linux.Hydra, PsybOt, Chuck Norris, Tsunami, Aidra, Spike, Mirai, show the growth in popularity and are able to hit the targets with much more attacks than in past. This research is conducted in order to raise the awareness for the researchers to look more into the higher security measures in this field. Authors Bhardwaj et al (2018) explore the option of DDoS attacks prevention in IoT using edge computing, where the edge computing, by their definition, is usage of computing resources near the end devices. They develop a solution called ShadowNet, which serves as the defense against DDoS attacks by making the edge computing a first line of defense. Solution is based on the edge functions that establish fast path between networks that send packets with information about the traffic in IoT to their main service. However, Hallman et al (2017) discussed about the details behind IoT security vulnerabilities and IoT-based botnets and botnet malware used in DDoS attacks. They mentioned some of the cyber security vulnerabilities of Internet of Things. This paper also talks about Mirai botnet malware, which is a part of Trojan malware family that serves as a DDoS attack on the IoT devices. After the analysis, authors showed that this newly released malware has a soft spot that can be research into much deeper, which is regarding the SQL injection attack, where the counterattack is possible to be implemented. Javaid et al (2018) conducted a research in the field of DDoS attacks on the IoT devices, and their prevention using blockchain technology, a technology that serves as online distribledger consisted of list of blocks.

Kasu Journal of Computer Science Vol. 1 No. 4 [December, 2024], pp. 778-795
https://doi.org//10.47514/kjcs/2024.1.4.006
Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

For the proposed model online software platform called Ethereum was used, that helps with the generation of addresses of devices, as well as the customized smart contract that enabled the defense mechanism against DDoS attacks. Authors have conducted experiments to prove that their model is capable of better detection and prevention of DDoS attacks. The literature survey by Zeeshan et al (2021) focused on the detection and mitigation of DoS attacks in a network environment. The experimental setup involved a network topology with a Ryu controller managing the network and an application for detection and mitigation running on top of it. Different types of DoS attacks, including flooding and TCP SYN flood attacks were considered in the experiments. Entropy-based algorithms were used for attack detection, and flow tables were modified to drop malicious traffic while preserving legitimate traffic. These algorithms measure the randomness or uncertainty of network traffic patterns to identify abnormal or malicious behavior. The use of entropy-based algorithms allows for effective and accurate detection of DoS attacks, enabling timely mitigation measures to be implemented. Additionally, the authors in Al-Begain et al (2022) proposed a lightweight security model for home environments, aiming to protect IoT devices from being enslaved as bots. The authors simulated a scenario and introduced a mechanism to monitor, detect, and filter suspicious traffic patterns. The results showed that the detection mechanism operates smoothly, ensuring network efficiency and avoiding delays

The major drawbacks (knowledge gaps) of the systems reviewed are: Most of them operate only at the network layer and only concerns themselves with IP addresses and data packets. Other layers especially transport (layer 4) and application (Layer 7) are prone and susceptible to DDoS attacks. There is, therefore, the need to improve on this approach by coming up with a cloud and IoT security model that checks different layers of the Open Systems Interconnection (OSI) model. The model developed will not only concern itself with checks on layer 3 (network, IP based) but also on layers 4 and 7.

3. Methodology

The paper utilized the OSSTMM (Open Source Security Testing Methodology Manual) methodology, a scientific framework for conducting network penetration testing and vulnerability assessments. This approach enables testers to tailor their assessments to the unique needs and technological context of the organization. By doing so, it provides a precise overview of the organization's network cybersecurity posture and delivers reliable, context-specific solutions. These insights support informed decision-making to enhance the security of the organization’s network(s).

3.1 High Level Model of the New System

Figure 11 presents a DDoS resilient security architecture that is to be designed as part of the research work. The architecture is set up to protect critical network infrastructure from cyber-attacks and ensure to continuous service availability during DDoS attacks. Importantly, it includes a web application firewall and network firewall configured to employ the different attack detection techniques identified as part of this research. Typical solutions during DDoS attack are: the entire traffic is diverted to a DDoS mitigation provider’s cloud and IoT devices, where it is scanned, scrubbed with the attack traffic getting identified and removed before being re-routed back to the in house data center of the enterprise.

Kasu Journal of Computer Science Vol. 1 No. 4 [December, 2024], pp. 778-795
https://doi.org//10.47514/kjcs/2024.1.4.006
Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

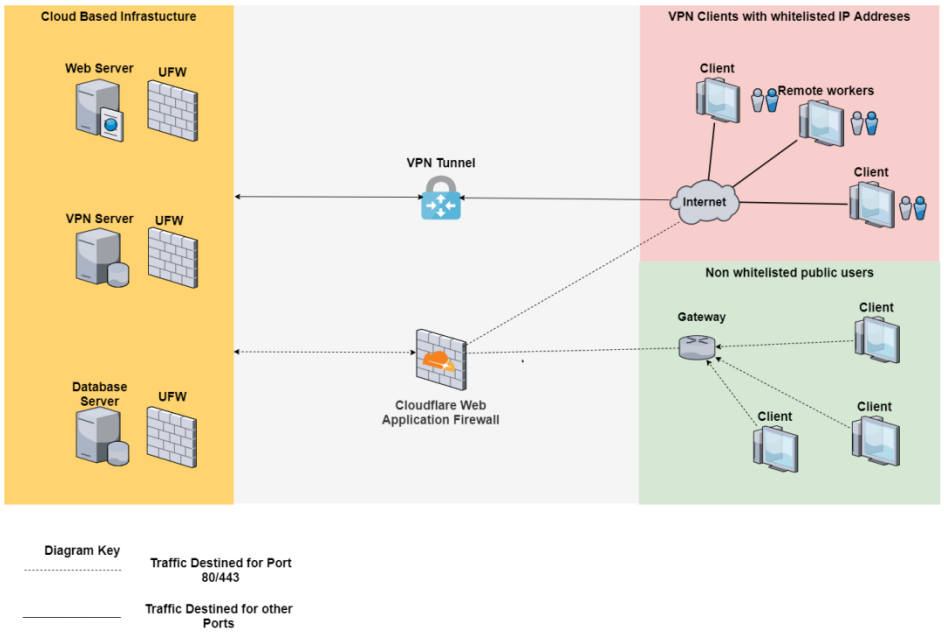

Figure 11: Proposed Hybrid System Architectural Design

3.2 System Testing

To test the new model on real-time network traffic, a simulation environment will be set-up within Linode. The proposed application captures real-time network traffic and predicts the presence or absence of an attack based on the user-selected model through command line interface. The set-up consists of a 64-bit, 2GB RAM, Debian 10 Web Server, a VPN Server to facilitate access to the cloud-based lab, A 64-bit, 4GB Kali Linux and Windows 10 Hosts to send attack traffic. The Attacking Hosts are connected to simulation environment via VPN tunnel and the Debian 10 Web Server and VPN server reside within the same data center. The set-up is shown in figure (12). This was done to create a Virtual Private Network (VPN) to contain the attack simulations within a cloud environment. Now, each of the four machines is assigned an internal IP address by the VPN Server. This is shown in table (3.1).

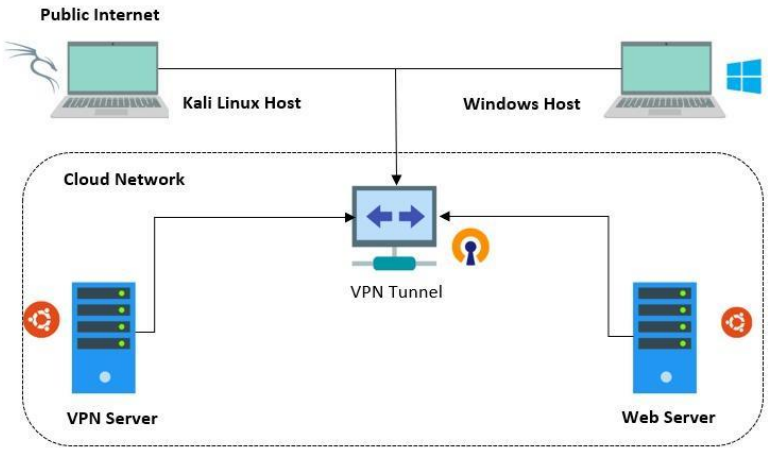

Figure 12: Simulation Test-bed Setup Diagram

Kasu Journal of Computer Science Vol. 1 No. 4 [December, 2024], pp. 778-795
https://doi.org//10.47514/kjcs/2024.1.4.006
Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

Table 3.1: Internal IP addresses assigned by the VPN Server to the machines used in the simulation

Host and Servers	**Assigned IP**
Debian Web Server	192.168.10.2/24
VPN Server	192.168.10.3/24
Kali Linux (Host)	192.168.10.15/24
Windows 10 Host	192.168.10.16/24

Table 3.1: Internal IP addresses assigned by the VPN Server

The Debian Web Server is the host running the DDoS Detection and Prevention tool whereas the Kali Host runs Hping3 and Windows 10 Host runs software called Low Orbit Ion Cannon (LOIC) to send UDP/TCP/HTTP attack traffic to the Debian Web Server. Low Orbit Ion Cannon (LOIC) is an open-source network stress testing and denial-of-service attack application, written in C#. LOIC can be used to perform both DoS and DDoS attack (depending on the number of people using the software to target the same server) on a target by flooding it with TCP, UDP or HTTP packets with the aim of disrupting the services and also the use of bash programming to simulate the attack

3.3 Algorithm to Secure Hybrid Clouds Against DDoS Attacks

Input: Inbound traffic on VPS – comprise of valid users and cyber attackers
Output: Outbound traffic from VPS – return traffic of authenticated user after VPN access
Start DDoS Attack
Step 1: Reconnaissance
Scan for open ports and IP address Identify Attack Target IP and Port

Step 2: Weaponization - Prepare Botnet Army for Attack
Load DDoS Tools with attack parameter values
Web Server IP Address and Port
Send attack information to initiate Botnets using command server
Initiate Attack using Command & Control server
Execute DDoS on the network layer

Step 3: Preparation – Configure DDoS Detection tool (TCPDUMP)
Step 4: Detection - Check Inbound traffic for Network level DDoS attack
Inbound High Volume & High Packet Rate Attack /*** ICMP Flood or Malformed PacketsCheck Rate Limiting & ICMP Threshold at Network Firewall
Check (Inbound Rate > Average Rate) Review
syslog
If (Inbound Data Packet size > 65,536 bytes)
Confirmed Ping of Death attack

Step 5: Remaining Traffic Check
Continue filtering /*** Throughput analysis

Step 6: Initiate DDoS Attack Mitigation
Notify for DDoS Flood and HTTP Attack mitigation process
Compare and illustrate results from key performance indicators
Update Network Firewall & Web Application Firewall configurations
Initiate blocking of confirmed IP Addresses and URLs
Close

Kasu Journal of Computer Science Vol. 1 No. 4 [December, 2024], pp. 778-795
https://doi.org//10.47514/kjcs/2024.1.4.006
Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

3.4 System Flowchart

Figure 13 presents how the proposed hybrid architecture is designed to monitor, detect, analyze and mitigate against multiple DDOS attack techniques targeting critical information system infrastructure.

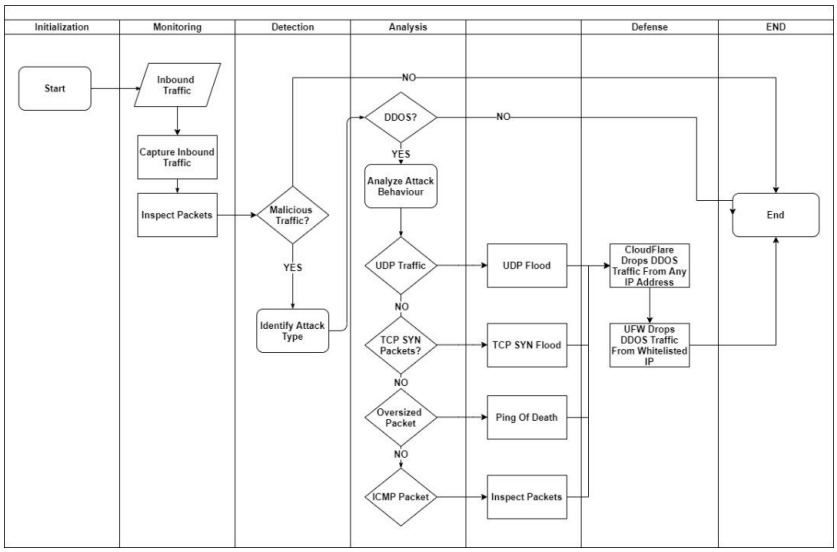

Figure 13: Proposed System Flowchart

4. Results and Discussion

The model was set up in such a way that TCP syn flood attacks were targeted to a particular webserver (41.33.72.47) on port 80 through an attacking lab machine using hping3. This is depicted in the flowchart shown in Figure 14 while the command line for the attack is shown in Figure 15.

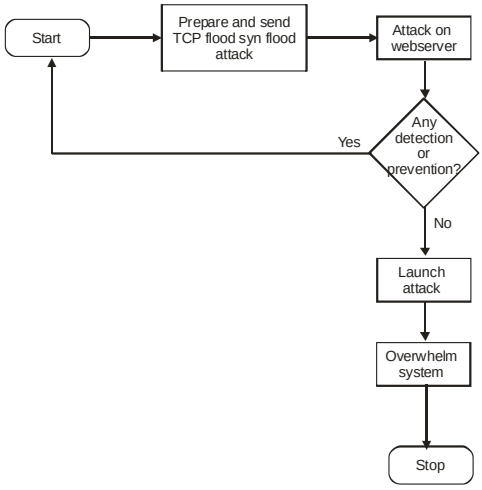

Figure 14: Flow chart of the attack on vulnerable host

Kasu Journal of Computer Science Vol. 1 No. 4 [December, 2024], pp. 778-795
https://doi.org//10.47514/kjcs/2024.1.4.006

Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

```
oluwatobi@kali:~$ sudo hping3 -S --flood -V -p 80 45.33.72.47
[sudo] password for oluwatobi:
using eth0, addr: 45.33.100.49, MTU: 1500
HPING 45.33.72.47 (eth0 45.33.72.47): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- 45.33.72.47 hping statistic ---
1625192 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Figure 15: Hping3 TCP SYN Flood Attack on an Unsecured Targeted Host

This machine did not have any prevention/detection mechanism against these attacks. There was 100% packet loss as no replies were received, effectively overwhelming the system. A total of 1,625,192 packets are transmitted in a short period.

Using Wireshark, the file is analyzed to show the distribution of traffic recorded over time, it can be observed that there was a lot of TCP errors within a short time interval (Figure 16); this is an indication of a successful DDoS attack.

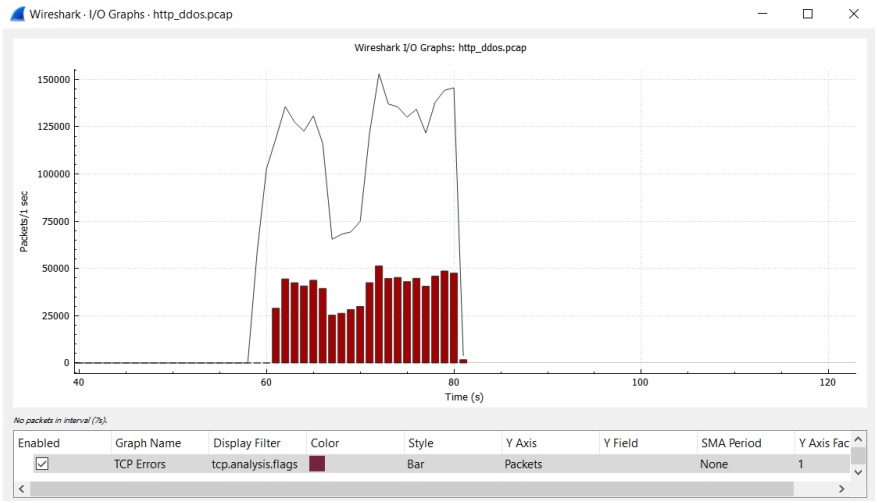

Figure 16: Distribution of traffic over time on an Unsecured Host

While in the second scenario of a protected host, tcpdump was also used to capture packets on the eth0 interface and using Wireshark, the file was analyzed to show the distribution of traffic recorded over time. It was observed that there less of TCP errors within a short time interval. This was an indication of a successfully mitigated DDOS attack with a network and application layer firewall as shown in Figure 17.

Kasu Journal of Computer Science Vol. 1 No. 4 [December, 2024], pp. 778-795
https://doi.org//10.47514/kjcs/2024.1.4.006

Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

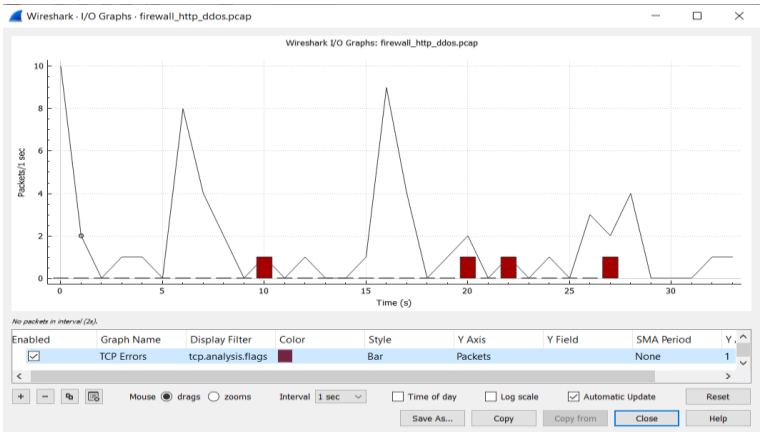

Figure 17: Distribution of traffic over time on a Secured Host

The Cloudflare firewall setting implemented in this design is the "Managed Challenge" feature. Unlike the "Legacy CAPTCHA" rule, it automatically handles challenges as they arise. Upon receiving a request from a client browser, it performs essential security checks to ensure everything is secure before redirecting the traffic.

It can be seen from Figure 18 that Cloudflare security setting has been set to automatically manage threats.

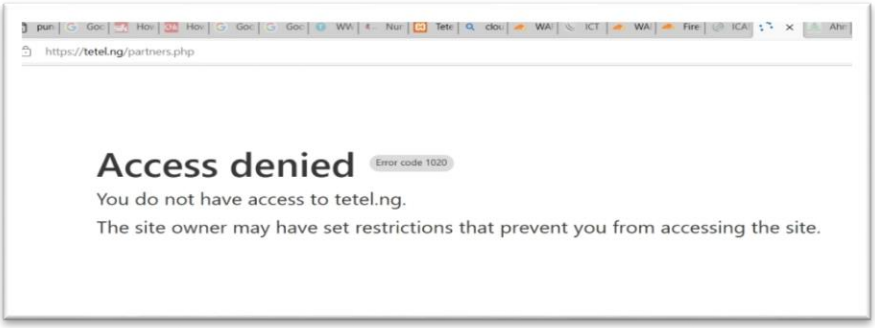

Figure 18: Blocked request to tetel.ng via Clouflare WAF

Figure 19 shows the result of a security setting by Cloudflare Web Application Firewall (WAF) to restrict access to tetel.ng, effectively blocking any predetermined menance.

Figure 19: Cloudflare processing a new request

Kasu Journal of Computer Science Vol. 1 No. 4 [December, 2024], pp. 778-795
https://doi.org//10.47514/kjcs/2024.1.4.006
Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

Figure 20 shows some of the processes Cloudlfare follows to ensure that clients connecting to tetel.ng are using the correct and secure means. Otherwise, the error shown on Figure 19 will be activated.

Figure 20: Cloudflare certifying a request as been secure

When all necessary checks have been carried out and certified to be in order, Cloudflare gives the affirmation that the connection is secure (as in Figure 20) and proceeds to load contents of the site.

5. Conclusion

Cloud computing and Internet of Things has introduced a range of new security threats and challenges. With vast amounts of data being stored in the cloud especially in public cloud services these platforms become prime targets for malicious actors. Successful attacks by such individuals can result in significant losses, including data breaches, financial costs, wasted time, and resource depletion. Implementing a system that effectively prevents or mitigates unauthorized access to an organization's cloud-based systems and IoT devices is not just desirable but essential. While numerous security systems are available in the market and more are being developed, they often exhibit certain weaknesses, as discussed in this study. Many existing solutions focus on securing one or two layers of the OSI model. In contrast, this study enhances security measures and monitoring across three OSI layers: network, transport, and application. By fortifying these layers, the likelihood of a threat bypassing all defenses is significantly reduced, ensuring more comprehensive protection. However, these advancements also expose IoT and cloud applications to various security threats. To enhance the scope of this research, It is, therefore, suggested that this study be extended to cover Man-in-the-Middle (MitM) and Routing Attacks on IoT devices and cloud applications.

References

Ahmed, S., Ali Khan, Z., Muhammad Mohsin, S., Latif, S., Aslam, S., Mujlid, H., Adil, M., & Najam, Z. (2023). Effective and Efficient DDoS Attack Detection Using Deep Learning Algorithm, Multi-Layer Perceptron. Future Internet 2023, 15, 76. [CrossRef]

Ahuja, N., Singal, G., Mukhopadhyay, D., & Kumar, N. (2021). Automated DDOS attack detection in software defined networking. J. Netw. Comput. Appl. 2021, 187, 103108.

Al-Begain, K., Khan, M., Alothman, B., Joumaa, C., Alrashed, E. (2022). A DDoS Detection and Prevention System for IoT Devices and Its Application to Smart Home Environment. Appl. Sci. 2022, 12, 11853. [CrossRef]

Alharbi, A., Alosaimi, W., Alyami, H., Rauf, H.T. & Damaševičius, R. (2021). Botnet Attack Detection Using Local Global Best Bat Algorithm for Industrial Internet of Things. Electronics, 10(11), p.1341.

Bhardwaj, K., Miranda, J., & Gavrilovska, A. (2018). "Towards IoT – DDoS Prevention Using Edge Computing", 2018

Chopade, S. S., Pandey, K.U., Bhade, D.S., & Wardha, D.M.I.E.T.R. (2013). Securing Cloud Servers against Flooding Based DDOS Attacks. International conference on Communication Systems and Network Technologies, IEEE. Retrieved September 18, 2019 from doi 10.1109/CSNT.2013.114. Computing

Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

resources in future Internet," in: Proceedings of IEEE Ninth International Conference on Dependable, Autonomic and Secure Computing (DASC), Dec 2011

Dao, N. (2017). "Securing Heterogeneous IoT with Intelligent DDoS Attack Behaviour Learning", IEEE Communications Magazine, 2017

Darwish, M., Ouda, A., & Capretz, L.F. (2013). Cloud-based DDoS attacks and defenses. In: Proceedings of theinternational conference on information society (i-Soci-ety), Toronto, ON, Canada, 24–26, pp.67–71. New York: IEEE.

Ghosh, P., Jha, S., Dutta, R., & Phadikar, S. (2018). "Intrusion Detection System Based on BCS-GA in Cloud Environment". In: Shetty N., Patnaik L., Prasad N., Nalini N. (eds.) Emerging Research in Computing, Information, Communication and Applications, 393-403. Springer, Singapore, Singapore (2018). Doi: 10.1007/978-981-10-4741-1_35.https://securelist.com/it-threat-evolution-q2-2019-statistics/92053/

Gillis, A. (2022). What is IoT (Internet of Things) and How Does it Work? - Definition fromTechTarget.com. TechTarget. https://www.techtarget.com/iotagenda/definition/Internet-of-Things-IoT

Hallman, R., Bryan, J., Palavicini, G., Divita, J. & Romero-Mariona, J. (2017). "IoTDDoS – The Internet of Distributed Denial of Service Attacks: A Case Study of the Miraj Malware and IoT-Based Botnets", SCITEPRESS, pp. 47-58, California, USA, 2017

Javaid, U., Siang, A., Aman, M. & Sikdar, B. (2018). "Mitigating IoT Device based DDoS Attacks using Blockchain", CryBlock'18, pp. 71-76, Germany, 2018

Khalil, T. (2017). "IoT Security against DDoS Attacks Using Machine Learning Algorithms", International Journal of Scientific and Research Publications, vol. 7, June, 2017

Mäki, P., Rauti, S., Hosseinzadeh, S., Koivunen, L., & Leppänen, V. (2016). Interface diversification in IoT operating systems. Proceedings of the 9th International Conference on Utility and Cloud Computing - UCC '16. 2016. doi:10.1145/2996890.3007877

Mirkovic, J., & Reiher, P. (2004). A Taxonomy of DDoS Attack and DDoS Defensem Mechanisms. ACM SIGCOMM Computer Communication Review, 34(2): 39–53.

Mukhopadhyay, D., Oh, B., Shim, S. & Kim, Y. (2015). "A Study on Recent Approaches in Handling DDoS Attacks", International Journal of Computer Science Trends and Technology, vol. 3, 2015

National Institute of Standards and Technology (NIST). (2004). "Computer Security Incident Handling Guide".

Niraj, S., Katkamwar, A., Grish, P., & Purva, D. (2012). "Securing Cloud Servers against Flooding Based DDoS Attacks," International Journal of Application or Innovation in Engineering & Management (IJ AI E M), vol. 1, pp. 50 – 55.

Ouda, A., Darwish, M., & Luiz, F. (2013). Cloud-based DDoS Attacks and Defenses, 978-1-908320. IEEE.

Patel, C. M., &Borisagar, V. H. (2012). "An intrusion detection and prevention system in Cloud computing: A systematic review", Journal of Network and Computer Applications. Retrieved February 12, 2019 from http://dx.doi.org/10.1016/j.jnca.2012.08.007

Peraković, D., Periša, M. and Cvitić, I. (2015). "Analysis of the IoT Impact on Volume of DDoS Attacks", PosTel 2015, Belgrade, December, 2015

Ping-of-death-attack (2017). "Ping Of Death (POD) attack explained," DDoS Protection. Retrieved September 15, 2019 from http://www.ddosprotection.net/ping-of-death-attack-explained/.

Qusay F. H., Introduction to the Internet of Things, in: Internet of Things a to Z: Technologies and Applications, 2018, pp. 1–50, http://dx.doi.org/10.1002/9781119456735.ch1.

Rajeswari, P., Raju, S.V., Ashour, A.S., & Dey, N. (2017). "Multi-fingerprint unimodel-based biometric authentication supporting cloud computing". In Intelligent Techniques in Signal Processing for Multimedia Security; Springer: Cham, Switzerland; pp. 469–485.

Salimm, M. M., Rathore, S. & Park, J. H. (2019). "Distributed denial of service attacks and its defenses in IoT: a survey," The Journal of Supercomputing, vol. 76, p. 5320–5363, 2020.

Satyajit, S. (2024) State of IoT: from https://iot-analytics.com/number-connected-iot-devices/

Online ISSN: 1597-2216
Print ISSN: 1597-2178
www.kjcs.edu.ng

Tamanna,T. (2016). "DDoS Attack in "Cloud of Things" environment, Software Defined Networking (SDN) and a research on defense mechanism against DDoS using SDN", International Journal of Scientific & Engineering Research, vol. 7, 2016

Tushir, B., Dalal, Y., Dezfouli, B., & Liu, Y. (2020). A quantitative study of DDoS and E-DDoS attacks on WiFi smart home devices. IEEE Internet Things J. 8 (8), 6282–6292 April .

Zeeshan, M., Riaz, Q., Bilal, M. A., Shahzad, M. K., Jabeen, H., Haider, S. A., & Rahim, A. (2021). Protocol-based deep intrusion detection for dos and ddos attacks using unsw-nb15 and bot-iot data-sets.

Zekri, M., Kafhali, S. E., Aboutabit, N., & Saadi, Y. (2017). DDoS attack detection using machine learning techniques in cloud computing environments. 2017 3rd International Conference of Cloud Computing Technologies and Applications (CloudTech). http://doi.org/10.1109/cloudtech.2017.828473