Simulating DDoS Attacks in Cloud Networks Using GNS3 and Exploring AI Mitigation Techniques

Muhammad Aqeel Mehdi
Electrical and Computer Engineering
Habib University
Karachi, Pakistan
mm08442@st.habib.edu.pk

Basil Khowaja
Electrical and Computer Engineering
Habib University
Karachi, Pakistan
bk08432@st.habib.edu.pk

Syed Muhammad Zaki Hussain Rizvi
Electrical and Computer Engineering
Habib University
Karachi, Pakistan
sr08468@st.habib.edu.pk

Tariq Mumtaz
Electrical and Computer Engineering
Habib University
Karachi, Pakistan
tariq.mumtaz@sse.habib.edu.pk

***Abstract*—DDoS attacks pose a significant threat to cloud environments by exploiting their scalability to disrupt services and exhaust resources. This paper simulates DDoS attacks using GNS3 to evaluate their impact on cloud infrastructure. The study demonstrates how botnet-generated traffic can overwhelm network resources, highlighting vulnerabilities in the setup. Additionally, existing AI-based DDoS mitigation techniques are explored, emphasizing their potential for enhancing cloud security. This work serves as a foundation for understanding and addressing DDoS challenges in cloud networks.**

I. Introduction

Cloud computing has revolutionized modern technology by offering scalable, on-demand access to computing resources, enhancing innovation across various domains. However, this advancement has also exposed cloud environments to significant cybersecurity challenges, particularly Distributed Denial-of-Service (DDoS) attacks. These attacks aim to disable cloud services by overwhelming network and server resources with excessive traffic, leading to service disruptions, degraded performance, and financial losses for organizations relying on cloud infrastructure. Although Artificial Intelligence (AI) has emerged as a promising solution for detecting and mitigating such attacks, understanding the mechanisms and consequences of DDoS attacks remains crucial for effective defense strategies. This study focuses on implementing a comprehensive simulation of DDoS attacks in a virtualized cloud environment using tools like GNS3 to analyze their impact on network performance and resource utilization. By simulating real-world attack scenarios, including volumetric floods and application-layer disruptions, this research evaluates the vulnerabilities of cloud systems to these threats. While the conceptual potential of AI-based mitigation techniques is discussed, the core of this work emphasizes the detailed implementation and analysis of DDoS attack simulations to provide actionable insights into the resilience of cloud infrastructures.

II. Background knowledge

A. What is Cloud Computing?

Cloud Computing means storing and accessing the data and programs on remote servers that are hosted on the internet instead of the computer's hard drive or local server. Cloud computing is also referred to as Internet-based computing. It is a technology where the resource is provided as a service through the Internet to the user. The data that is stored can be files, images, documents, or any other storable document.

The following are some of the operations that can be performed with Cloud Computing:

- Storage, backup, and recovery of data
- Delivery of software on demand
- Development of new applications and services
- Streaming videos and audio [1]

B. How Cloud Computing Works?

Cloud computing helps users easily access computing resources like storage and processing over the internet rather than relying on local hardware. Here is an overview of how cloud computing works:

- **Infrastructure:** Cloud computing depends on remote network servers hosted on the internet to store, manage, and process data.
- **On-Demand Access:** Users can access cloud services and resources on demand. They can scale up or down without needing to invest in physical hardware.
- **Types of Services:** Cloud computing offers various benefits such as cost savings, scalability, reliability, and accessibility. It reduces capital expenditures and improves efficiency [1].

C. Cloud Computing Architecture

Cloud computing architecture encompasses the client and server, divided into front-end and back-end components. The front-end comprises the user interface and application access

mechanism, while the back-end handles service delivery and data management.

- **Front-End:** This layer is visible to users and includes the software or hardware interfaces, such as web browsers or applications, enabling user interactions with the cloud services.
- **Back-End:** The back-end includes servers, storage, and computing resources. It manages the primary service models:
  - **Software-as-a-Service (SaaS):** Provides hosted software applications over the internet, eliminating the need for installation or maintenance.
  - **Platform-as-a-Service (PaaS):** Offers a platform allowing users to develop, test, and deploy applications without managing underlying infrastructure.
  - **Infrastructure-as-a-Service (IaaS):** Delivers computing infrastructure like servers and storage on a scalable, on-demand basis.

Additionally, deployment models like private, public, hybrid, and community clouds offer varying levels of control, security, and cost-effectiveness. This architecture allows scalable and efficient resource utilization, significantly impacting businesses by reducing infrastructure costs and enabling flexibility [2].

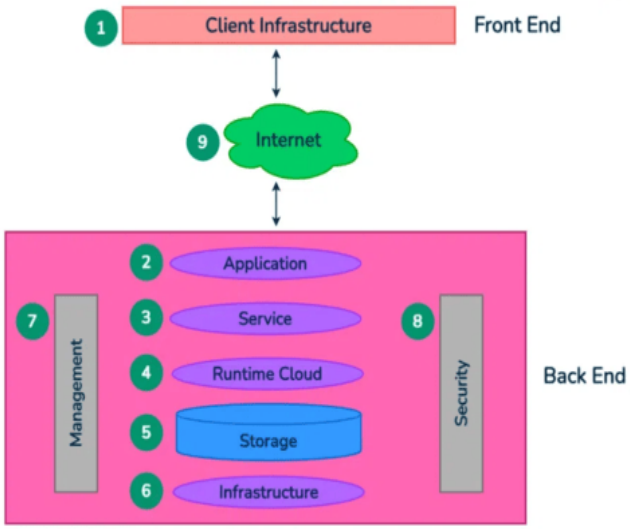

Fig. 1. Cloud Computing Architecture Overview

D. DDoS (Distributed Denial-of-Service) Attack

One of the significant challenges in cloud computing today is Distributed Denial-of-Service (DDoS) attacks. Before delving into its impact on cloud computing, it's crucial to understand what DDoS entails.

DDoS is a cyberattack where an attacker floods a server with excessive internet traffic, rendering online services and websites inaccessible. It is a subset of the broader category of Denial-of-Service (DoS) attacks. In a DoS attack, a single internet connection is used to overwhelm a target with requests or exploit vulnerabilities. DDoS, on the other hand, leverages thousands or even millions of connected devices, making it more challenging to mitigate [3].

*1) **Types of DDoS Attacks**:*

- **Volume-Based Attacks:** Aim to overwhelm the bandwidth between the target and the internet. An example is DNS amplification, where a small query from the attacker results in a massive response sent to the victim.
- **Protocol Attacks:** Consume server or resource capacity by exploiting vulnerabilities in Layers 3 and 4 of the OSI model. A SYN flood, where numerous spoofed handshake requests overload the server, is a common example.
- **Application-Layer Attacks:** Target Layer 7 of the OSI model, exhausting server resources by generating excessive HTTP requests and forcing the victim to process more traffic than it can handle. An HTTP flood exemplifies this type.

*2) **Current Methods to Launch DDoS**:* Currently, there are two main methods to launch DDoS attacks in the Internet. The first method is for the attacker to send some malformed packets to the victim to confuse a protocol or an application running on it (i.e., vulnerability attack). The other method, which is the most common one, involves an attacker trying to do one or both of the following:

- **Disrupt a legitimate user's connectivity:** This is achieved by exhausting bandwidth, router processing capacity, or network resources. These are essentially network/transport-level flooding attacks.
- **Disrupt a legitimate user's services:** This is achieved by exhausting the server resources such as sockets, CPU, memory, disk/database bandwidth, and I/O bandwidth. These essentially include application-level flooding attacks.

Today, DDoS attacks are often launched by a network of remotely controlled, well-organized, and widely scattered Zombies or Botnet computers that are simultaneously and continuously sending a large amount of traffic and/or service requests to the target system. The target system either responds so slowly as to be unusable or crashes completely.

Zombies or computers that are part of a botnet are usually recruited through the use of worms, Trojan horses, or backdoors. Employing the resources of recruited computers to perform DDoS attacks allows attackers to launch a much larger and more disruptive attack. Furthermore, it becomes more complicated for the defense mechanisms to recognize the original attacker because of the use of counterfeit (i.e., spoofed) IP addresses by zombies under the control of the attacker [5].

*3) **DDOS Attacks in Cloud Computing**:* For cloud computing, DDoS attacks represent a critical threat, as they exploit the scalability of cloud platforms to generate enormous volumes of malicious traffic. This not only disrupts services but also leads to increased resource usage, driving up operational costs and impacting user trust.

In 2024, Cloudflare mitigated the largest DDoS attack ever recorded, reaching 5.6 Tbps and 666 million packets per

second. The attack lasted 80 seconds and was part of a larger hyper-volumetric DDoS campaign. Cloudflare's network automatically mitigated this attack, protecting its customers [4].

III. Setup and Simulations

This section presents the simulation setup and results obtained from modeling Distributed Denial-of-Service (DDoS) attacks in a virtualized environment using GNS3. The simulation focused on analyzing the impact of DDoS attacks carried out by botnets on cloud performance. Key metrics such as CPU usage and RAM were evaluated to assess the severity of the attacks and the network's ability to handle such disruptions.

A. Setup

The network setup involves configuring a cloud environment using GNS3 with a loopback adapter acting as the backbone connection. The following steps outline the setup:

- **Configuring the Loopback Adapter:** The Microsoft KM-Test Loopback Adapter was enabled on the host machine (laptop) to simulate a physical connection to the cloud. This adapter is accessible by default through the network adapters settings ('ncpa.cpl').
- **Connecting the Cloud Node:** In GNS3, the cloud node was added and configured to use the loopback adapter. This created a bridge between the virtual network and the physical network of the host.
- **Configuring the Router:** The router (R1) was added and connected to the cloud via the '10.10.10.0/24' network. The router's interface connected to the cloud was assigned the IP '10.10.10.1'.
- **Testing the Connectivity:** The setup was tested by successfully pinging the cloud's IP ('10.10.10.10') from the router to ensure the connection was functional.
- **Connecting the Virtual PCs:** The switches and PCs were added to the network. The normal users and botnet PCs were configured on separate switches (Switch1, Switch2, and Switch3), connecting them to the router via different subnets.
- **Final Validation:** Pinging and communication were tested across all network nodes, ensuring the setup was operational and ready for simulating DDoS attacks.

B. Topology

The simulated network topology for this experiment is shown in Fig. 2. The setup represents a cloud-based environment with three key components: normal users, a cloud server, and botnets. Below are the critical aspects of the topology:

- **Cloud Server and Loopback Adapter:** The cloud server is represented by the IP '10.10.10.10', which is connected to the router via a loopback adapter. The Microsoft KM-Test Loopback Adapter, pre-installed on most Windows systems, acts as a virtual network adapter. It was chosen because it allows the GNS3 environment to connect to the host machine's simulated cloud network seamlessly.

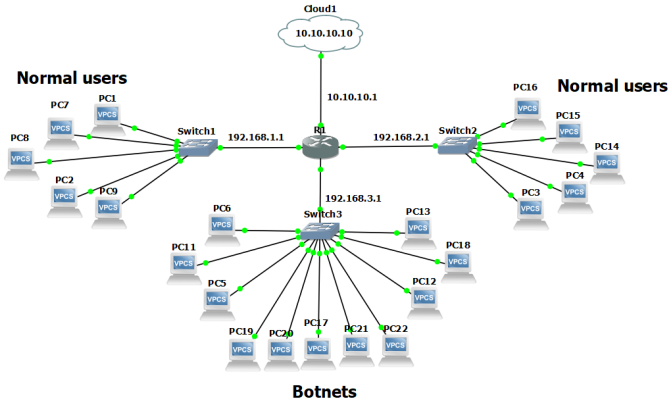

Fig. 2. Simulated Network Topology

The loopback adapter enables testing without requiring physical network hardware.

- **Npcap and WinPcap for GNS3:** While setting up GNS3 for this simulation, we encountered compatibility issues with Npcap, which is installed by default during GNS3 installation. Npcap was found to be incompatible with the Microsoft KM-Test Loopback Adapter in most cases on Windows systems. To resolve this issue, we uninstalled Npcap and installed WinPcap, an older but more compatible packet capture driver. This allowed GNS3 to properly connect the simulation to the loopback adapter and enabled successful communication with the cloud server.
- **Normal Users:** The network includes two sets of normal users, each connected via separate switches (Switch1 and Switch2). Each group operates in different subnets ('192.168.1.0/24' and '192.168.2.0/24') to simulate real-world segregated user traffic.
- **Botnet Network:** A dedicated botnet network is connected via Switch3 and operates in the subnet '192.168.3.0/24'. The botnets are configured to simulate Distributed Denial-of-Service (DDoS) attacks by flooding the cloud server with traffic.
- **Router Configuration:** The router, R1, acts as the central hub, connecting all switches to the cloud. Each router interface is configured with unique IPs to enable communication between the subnets and the cloud.

C. Methodology

This experiment simulated a Distributed Denial-of-Service (DDoS) attack in GNS3 to analyze its impact on a cloud server ('10.10.10.10'). The network topology included a cloud server connected to a router (R1) via a loopback adapter, three switches, normal users in subnets '192.168.1.0/24' and '192.168.2.0/24', and a botnet network in subnet '192.168.3.0/24'. Initially, normal users sent ICMP requests to the server to confirm connectivity. The server was successfully pinged using the command `ping 10.10.10.10 -t -l 10000`. Subsequently, botnets were configured to flood the server with high-volume ICMP requests using variations of

the same command, simulating a DDoS attack. The server's response to legitimate traffic was monitored during the attack, revealing how excessive traffic rendered it unresponsive, demonstrating its vulnerability to DDoS attacks in the absence of mitigation strategies.

IV. Results

The simulation demonstrated the impact of a Distributed Denial-of-Service (DDoS) attack on a cloud-connected network. When botnets were configured to flood the router with high-volume ICMP requests directed at the cloud server ('10.10.10.10'), an internal server error was observed. This error indicated that the router, acting as the central hub of the network, was unable to handle the excessive traffic load and subsequently crashed. The crash rendered the cloud server inaccessible, effectively disrupting communication for both normal users and botnets. This result highlights the severity of DDoS attacks on network infrastructure, emphasizing the need for effective mitigation strategies.

The output of the 'debug ip icmp' command, as shown in Fig. 3, provides a detailed view of the ICMP traffic, including the echo requests and replies being processed by the router until it eventually failed.

Fig. 3. Debug output of 'debug ip icmp' showing ICMP echo requests and replies before the router crash.

After the router reached its resource limits due to the flood of ICMP requests, an internal server error was displayed, as shown in Fig. 4. This error explicitly confirms that the router crashed and was unable to process further requests, resulting in the server becoming unreachable. The error message underscores the devastating effect of DDoS attacks on network stability and reliability.

Fig. 4. Internal server error displayed after the router crashed due to excessive ICMP requests.

In addition to the ICMP traffic and error message, resource utilization metrics such as CPU and RAM usage were monitored on the router. Table I provides a comparison of resource usage before and after the DDoS attack. The results show that the router's CPU and RAM usage significantly increased after the attack, ultimately leading to the router's failure.

TABLE I
Router Resource Usage Before and After DDoS Attack

Metric	Before DDoS Attack (%)	After DDoS Attack (%)
CPU Usage	35.8	44.6
RAM Usage	40.5	78.7

V. Detection and Prevention of DDoS Using AI on Clouds

A. Simple Machine Learning Techniques: Machine learning algorithms are the most central component of AI-based DDoS detection. These models use the traffic that flows within a network to distinguish between normal behavior and malicious behavior.

- **Random Forest:** Uses a number of decision trees to provide the best prediction. Its success rate in identifying the traffic as malicious is high, and it can be as high as 99.9974%.
- **Support Vector Machines (SVMs):** Separate data into normal and malicious traffic in order to identify an attack.
- **Decision Trees:** A simple decision-making process that divides data into segments to make it easier to work with. These are easy to understand and quite helpful in recognizing typical attack patterns.

B. Unsupervised Learning: Whereas supervised models are effective for known threats, the unsupervised learning deals with unknown and emerging attack patterns, which make it crucial.

- **Clustering:** Aggregates measurements to identify irregular patterns of related data. This makes it easier to detect traffic that is different from the normal traffic indicating an attack.
- **Feature Reduction:** Reduces the amount of information that is transmitted to the point that only the critical aspects of traffic can be easily noticed to be abnormal.

C. Adapting with AI: The contemporary attacks are dynamic, and so are the threats; hence, the need for dynamic solutions. AI models like reinforcement learning work in real-time to counter the new attack methods, as well.

- **Reinforcement Learning:** Enables systems to adapt to the experience and modify their defense mechanisms over time in order to counter new and evolving threats.

D. Advanced AI Models: Other sophisticated AI models such as deep learning techniques are able to beyond conventional methods to identify and counter new and different forms of attack. These models study traffic details and, therefore, are useful in cloud security.

- **Convolutional Neural Networks (CNNs):** Can analyze patterns in traffic and can see that an attack is coming in a large amount of data at once.

- **LSTMs:** Continuity of track sequences to be able to detect continuous or intricate attack process.

E. Real-World Applications: The potential of AI is not in what it is, but what it can do. AI applications are employed in practice to safeguard cloud networks. These systems are always on, and they detect any activities in the traffic as suspicious. They also minimize on false positives hence normal users are not locked out.

F. Natural Language Processing (NLP): Besides traffic analysis, AI also uses NLP for text data analysis including threat intelligence reports and alerts. This improves the assessment of the environment and decision making.

- **Text Analysis:** Implements and comprehends the type of threats from the alerts or reports that are read and classified.
- **Entity Recognition:** Extracts important features such as IP address under suspicion from the data.

AI-based solutions for DDoS detection and prevention assist cloud networks to remain protected by identifying threats, responding promptly and evolving with new threats. They are becoming crucial as DDoS attacks become more complex and sophisticated, to keep cloud systems available and dependable.

REFERENCES

[1] "Cloud Computing," GeeksforGeeks, [Online]. Available: https://www.geeksforgeeks.org/cloud-computing/. [Accessed: Nov. 24, 2024].

[2] I. Odun-Ayo, M. Ananya, F. Agono, and R. Goddy-Worlu, "Cloud Computing Architecture: A Critical Analysis," in *2018 International Conference on Computational Science and Its Applications (ICCSA)*, IEEE, 2018. Available: https://doi.org/10.1109/ICCSA.2018.8439638.

[3] A. Kumar, "Understanding DDoS Attacks," [Online]. Available: https://example.com/ddos-intro. [Accessed: Nov. 24, 2024].

[4] Cloudflare, "Cloudflare mitigates largest DDoS attack," [Online]. Available: https://example.com/cloudflare-ddos. [Accessed: Nov. 24, 2024].

[5] S. T. Zargar, J. Joshi, and D. Tipper, "A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks," in *IEEE Communications Surveys Tutorials*, vol. 15, no. 4, pp. 2046–2069, 2013.

[6] S. Ahmadi, "AI in the Detection and Prevention of Distributed Denial of Service (DDoS) Attacks," *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 15, no. 10, pp. 23–28, 2024. Available: https://thesai.org/Downloads/Volume15No10/Paper_4-AI_in_the_Detection_and_Prevention.pdf.

[7] R. Khanna, "Harnessing AI for Network Security and DDoS Attack Detection," *Journal of Artificial Intelligence Cloud Computing*, vol. 3, no. 5, pp. 1–3, Sep. 2024. Available: doi.org/10.47363/JAICC/2024(3)384.