Deep Science Publishing
https://doi.org/10.70593/978-93-49307-78-0_1

Chapter 1

Cloud security vulnerabilities: Analysing DDoS attack methods and mitigation strategies

1.1 Introduction

Cloud computing systems are intensely competitive compared with traditional computing. It is now a suitable internet method to access applications, services, and resources using various network access techniques. Cloud computing enables simple data access between cloud service providers and cloud computing clients from anywhere, any time. It can efficiently distribute and release resources, hence, it enables users to only pay for resources that are used. Although, governments, businesses, and organizations have moved all or most of their IT systems to the cloud (Kati et al. 2022); many security concerns with cloud computing prevent its adoption and use. This is because cloud computing enables access to the environment and services through the internet. Cloud Computing is more vulnerable to security problems that could result in unsatisfactory service (Bamasag et al. 2022). Figure 1 displays the benefits of cloud computing that make it more competitive compared to traditional computing.

Distributed Denial of Service (DDoS) attacks is a popular security concern, which is a cyberattack where several infected systems or compromised virtual machines attack a single target (the cloud), creating a denial of service to cloud users of the targeted system. A zombie or bot is a computer that is being controlled by an invader whereas, a botnet is referred to as a zombie army which is a collection of hijacked computers (Cheema et al. 2022).

1.2 Motivation

The passion for problem-solving especially in our society cannot be overemphasized, hence, the reason for venturing into IT cyber security after completing my first degree and seeing the issue facing the recent digitalized business world.

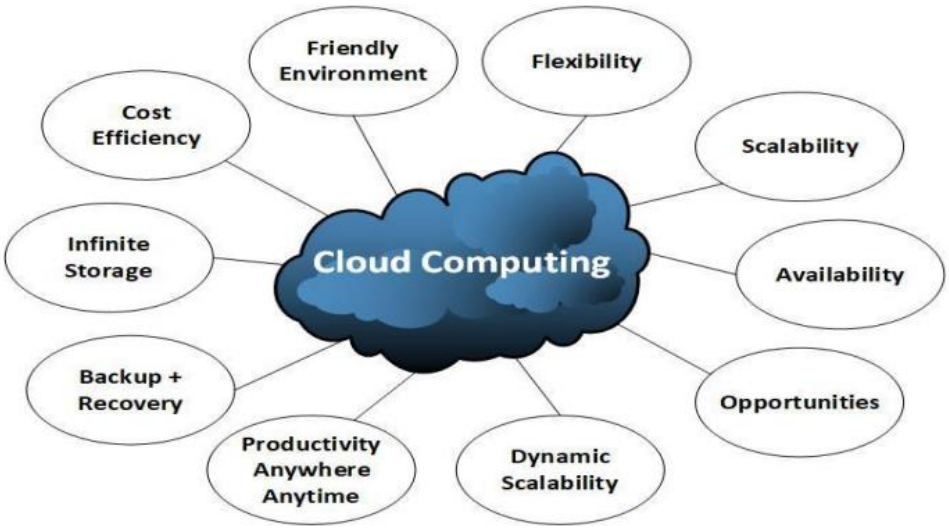

Figure 1: Benefits of Cloud Computing (Kati et al. 2022)

As the internet evolves, many cyber threats like DDoS attacks have become a major challenge as activities are carried out in the cloud or online, causing instability in the online business. Numerous cyber-attacks pose a hazard to the cloud computing platform and software as data is stored in the Cloud Computing environment. The availability of data and applications is more important to users and organizations than understanding the complexity required in service delivery. Although numerous threats such as DDoS attacks can disrupt virtualization, safeguarding hypervisors and virtual machines in the cloud. It is critical for protecting sensitive information from intrusions (Abubakar et al. 2020).

The focus of every industry using cloud platforms is to increase productivity and operational cost. However, the effect of hackers on the network reduces operational costs because of downtime.

In addition, one of the major challenges in the IT industry, especially in Africa, is cyber-attacks, for example, the detection of DDoS attacks in the cloud system. The information technology team back in Nigeria has been seeking solutions to detecting this attack but has no headway. However, the knowledge acquired from one of the program modules

(Machine learning) will help to provide a solution to this problem. The excitement is that this research will be among the contribution that will help to tackle the problem in Africa.

Detection of DDoS attacks on the cloud environment is very essential as it will help to mitigate downtime and increase operational costs. The idea of this study is not to build a new system but to help optimize existing IT infrastructure by mitigating the cyberattack technique on networks.

1.3 Problem Overview

Since most enterprises are moving to the cloud to enhance and accommodate remote working, the major problem in this study is to address how to optimize cloud security to detect the security issue in DDOS attacks on cloud computing. Usually, DDOS attacks are still a very big threat to the network system, hackers still have access to information stored in the cloud which often leads to errors due to unforeseen circumstances. The observation of DDoS attacks is a basic defence mechanism and the area that any detection system provides is a valid measure of its performance. This is because such attacks are not focused on exploiting faults or flaws, but rather on a specific volume of attack traffic. The attack traffic would be very similar to legitimate or normal traffic, raising the chance of increased traffic being construed as an attack. The pace of resource depletion is one feasible metric for detection and can be detected using an anomaly-based system.

1.4 Research Questions

This part constructed an effective research hypothesis that would help deliver desired outcomes for this problem.

Q1: What type of dataset should be used to solve this problem?

Q2: How can multi–supervised machine learning techniques be used to analyse the dataset (DDoS and benign traffic) to achieve better accuracy of DDoS attack detection in the cloud?

Q3: What is the most efficient supervised ML algorithm to detect DDoS attacks in a cloud environment?

1.5 Aims and objectives

This work aims to develop DDoS detection systems for cloud environments aided by machine learning. The following objectives support the above-mentioned goal in more detail.

- Setup a cloud base system for conducting benign and malicious traffic.
- Examine the existing intrusion detection system and datasets.
- Employ the most relevant machine learning methods to detect DDoS from a dataset (malicious and benign network traffic).
- Create outcomes for each algorithm by training, validating, and testing the dataset against machine learning algorithms.
- Analyse the models' performance and select the most efficient Machine learning algorithm.

In addition, the project will be extended using part of a benchmark dataset (CSE-CIC-IDS2018) for large data size model building.

1.6 Project Scope

This study focused on cybersecurity where cyber-attacks are evaluated using the Machine Learning Technique. It examined one of the famous cyber-attacks known as the Distributed Denial-of-Service attacks in the cloud, using a programming language to build supervised machine learning models which were used to predict the accuracy of how DDoS attacks are detected in the cloud.

This research reviewed papers on both cloud and other network environments since there are limited papers on DDoS detection in Cloud systems.

The primary focus of this study is the DDoS dataset generated from the cloud environment to detect DDoS attacks. So, the goal is to analyse DDoS traffic from the dataset generated using ML-supervised models.

1.7 Report Organisation

The rest of the report is structured as follows:

Chapter 2: Background

This section is divided into two namely the theoretical and the experimental background. The theoretical discusses the understanding of some factors about the threat – DDoS attack, the network -Cloud Computing and the techniques -Machine learning which will be used to solve this problem. While the experimental background summarises, the existing work carried out in this research area and its gaps. Also, the investigation report will be summarised in this chapter.

Chapter 3: Project Implementation

This section is also divided into two parts namely the initial system setup design and the experimental design. The system setup design includes the explanation of the topology implemented to generate both benign and DDoS traffic. On the other hand, the experimental design explains the detailed ML techniques used to tackle this issue.

Chapter 4: Performance Analysis Results

This part reviews the results of the performance metrics used to build the models inclusive of tables and charts of both newly generated and open source datasets. These metrics measured are accuracy, precision, recall and F1-score. Some measures stated in the investigation report were reflected in this section to evaluate achievement.

Chapter 5: Conclusion and future work

The section discusses the conclusion of the whole work carried out and also recommendations for the future work.