Chapter 7
Security Considerations of SDN Networks During DDoS Attacks in Load Balancing

Adrija Das
School of Computer Engineering, KIIT (Deemed to Be) University, Bhubaneswar, India

Tanisha Saini
School of Computer Engineering, KIIT (Deemed to Be) University, Bhubaneswar, India

Pratyasha Nanda
School of Computer Engineering, KIIT (Deemed to Be) University, Bhubaneswar, India

Sneha Bhaskar
School of Computer Engineering, KIIT (Deemed to Be) University, Bhubaneswar, India

Ritika Jain
School of Computer Engineering, KIIT (Deemed to Be) University, Bhubaneswar, India

Hitesh Mohapatra
https://orcid.org/0000-0001-8100-4860
School of Computer Engineering, KIIT (Deemed to Be) University, Bhubaneswar, India

ABSTRACT

Cloud computing deals with the dynamic allocation of resources on demand from any location. Load balancing is the phenomenon of ensuring the distribution of traffic and the operation of loads on multiple servers. There are security considerations where the load balancers are potential targets for Distributed Denial of Service (DDoS) attacks. This occurs when the attacker overwhelms the system with a flood of traffic, causing it to become unresponsive. The paper discusses the

DOI: 10.4018/979-8-3693-9235-5.ch007

security challenges and attacks that affect workload distribution across servers dealing with access control mechanisms and concerns about multi-tenancy risks. The analysis involves identifying attacks in load-balancing systems from pre-existing frameworks by utilizing tools like Snort, Wireshark, and MATLAB for DDoS attacks. Furthermore, the paper does a comparative study on the established works. It addresses the best mitigation strategies for different types of DDoS attacks, such as Smurfing and TCP-SYN attacks, thus enhancing resilience with SDN architecture and multi-layered defense mechanisms.

1. INTRODUCTION

Cloud computing is a popular method to access resources from a shared area referred to as the cloud using a user-friendly interface. It is predicated on the flexible distribution of resources according to need and cost. Because of its lower prices, scalability, remote access, and various other advantages, it is a growing trend in computing. This model's scalability—which allows organizations to only pay for what they use—is one of its greatest benefits, as it may significantly lower manufacturing costs. There are four different kinds of cloud deployment models, depending on the abstraction level offered. A single entity that manages an on-site private cloud infrastructure and provides cloud computing services to users is granted access to private cloud authentication. The organization may also agree via a third-party cloud provider to host and manage dedicated servers off-site. The most popular kind of cloud deployment architecture is the public cloud, which employs shared infrastructure and resources held by a third-party cloud service provider, (Buvaneswari, Loganathan, & Sangeetha, 2017). It stores and controls the accessibility of data and apps via the Internet. This model's primary benefit is that it enables resource scalability, allowing customers to pay for what they use. However, its primary drawback is the safety of the user's data. The benefits of both public and private cloud computing are combined in the hybrid cloud model, allowing users to access shared resources and secure data through the utilization of pre-existing IT infrastructure. It enables businesses to internally store sensitive data that is accessible through apps hosted on public cloud infrastructure. A collection of organizations can access services through the Community Cloud. The members who make up the group are the ones who own, run, and manage it, (He, 2022).