International Journal of Cloud Applications and Computing
Volume 15 • Issue 1 • January-December 2025

Information Theory-Based DDoS Attack Detection in Cloud Computing:

A Systematic Survey of Approaches, Challenges, and Future Directions

Mohammad Alarqan
School of Computer Sciences, Universiti Sains Malaysia, Malaysia

Bahari Belaton
School of Computer Sciences, Universiti Sains Malaysia, Malaysia

Ammar Almomani
https://orcid.org/0000-0002-8808-6114
Higher Colleges of Technology, UAE

Mohammad Alauthman
https://orcid.org/0000-0003-0319-1968
University of Petra, Jordan

Mohammed Azmi Al-Betar
https://orcid.org/0000-0003-1980-1791
Ajman University, UAE

Varsha Arya
Hong Kong Metropolitan University, Hong Kong & Center for Interdisciplinary Research, University of Petroleum and Energy Studies (UPES), Dehradun, India & UCRD, Chandigarh University, Chandigarh, India

ABSTRACT

Distributed denial of service (DDoS) attacks have emerged as a critical challenge for cloud computing, impacting service availability and raising concerns among providers. Despite cloud computing's scalable and flexible architecture, its vulnerabilities make it an attractive target for attackers. This paper presents a comprehensive survey of DDoS attacks in cloud environments, focusing on detection mechanisms leveraging information theory. Key contributions include an analysis of cloud computing characteristics exploited by attackers, a taxonomy of DDoS attacks, and a discussion of effective anomaly detection approaches. Solutions based on information theory, encompassing detection parameters, metrics, and validation techniques, are reviewed for their ability to enhance security with high accuracy and low computational costs. This survey aims to guide researchers and practitioners in developing advanced defenses for cloud applications. Open issues and future research directions are identified to inspire further innovation in mitigating DDoS attacks.

KEYWORDS

Anomaly Detection, Cloud Computing, Correlation Coefficient, Information Distance, Information Entropy, DDoS

INTRODUCTION

Cloud computing has experienced accelerated growth and has become a competitor to traditional computing systems (Liu et al., 2020; Moura & Hutchison, 2016; Muteeh et al., 2021; Somani et al., 2017; Sunyaev, 2020). It supports the easy sharing of web applications, resources, and services between cloud providers and consumers by using on-demand self-services that enable consumers to use services and resources without buying them. Also, it allows them to pay for the resources they

DOI: 10.4018/IJCAC.369817

consume using the pay-as-you-go feature (Osanaiye et al., 2016). Thus, cloud consumers do not require any maintenance overhead. Cloud computing also allows its service users to access computing from anywhere and on any device connected to the internet. It enables customers to allocate and release resources efficiently (Kaaniche & Laurent, 2017). These advantages have motivated governments, organizations, and industries to transfer their traditional information technology systems mostly or entirely to cloud computing (Arjun & Vinay, 2016; Khalil et al., 2014; Sharma & Trivedi, 2014; Somani et al., 2017).

The provision of cloud computing services over the internet makes the environment vulnerable to security threats that hamper adopting or transferring traditional computing systems to cloud computing (Kaaniche & Laurent, 2017; Khalil et al., 2014). Therefore, cloud service providers must take countermeasures to protect the cloud environment from security threats that may lead to poor quality of service or denial of service (DoS) to cloud users (Khan, 2016). These security threats include all cloud environment components, allowing malicious or unauthorized users to access and disrupt the cloud environment (Iqbal et al., 2016).

Participants in the cloud computing environment consist of three classes: service users, service providers, and cloud services providers. A specific kind of application programming interface is used to interact with participants. The cloud computing application programming interface depends on three service models, namely software as a service, platform as a service, and infrastructure as a service (IaaS). These service models provide cloud computing resources to consumers through interfaces such as websites (Gruschka & Jensen, 2010).

Even though there are several security threats inherent in cloud computing distributed denial of service (DDoS) attack is considered one of the cyber threats that aim to compromise the availability principle. Therefore, when a system is under a DDoS attack, legitimate users cannot use services and resources available in cloud computing systems (Moustafa et al., 2019). DDoS attack has become one of the major distinctive threats to cloud computing; it causes problems by targeting the services and resources of cloud computing (Behal & Kumar, 2017a, 2017b; Behal et al., 2021; Bhandari et al., 2016; Bhatia & Verma, 2017; Bhuyan et al., 2015b, 2016; Kushwah & Ranga, 2020; Mishra et al, 2021; Sachdeva et al., 2016; Saxena & Dey, 2020; Velliangiri et al., 2021; Vissers et al., 2014; Xiao et al., 2015; Zhou et al., 2014).

A DoS attack is an explicit attempt by an attacker to deny legitimate users access to shared services or resources provided by a victim server (Bhandari et al., 2016). This type of attack targets the victim server by sending massive malicious packet traffic to a victim server to overload the victim server's network or consume its resources by targeting the services provided by the victim server (Behal & Kumar, 2017b; Bhuyan et al., 2015b; Osanaiye et al., 2016; Wong & Tan, 2014). On the other hand, when the incoming DoS attack packets arrive on the victim server from various resources, it is called a DDoS attack A. Bhandari et al. (2016).

Indeed, there is a difference between flash events (FEs) and DDoS attacks. FEs are network traffic generated by multitudes of legitimate users who simultaneously request access to a specific computing resource, as in a server hosted in cloud computing (Behal & Kumar, 2017a). According to incoming traffic rates coming to a particular server in a cloud computing environment, DDoS attacks are classified into low-rate DDoS attack traffic (similar to legitimate traffic) and high-rate DDoS attack traffic (similar to FEs). Usually, these types of traffic can disrupt a cloud network or the services a cloud server provides with DDoS attacks (Bhuyan et al., 2015b).

This paper aims to provide a detailed survey of solutions for DDoS attacks in cloud computing using information theory to evaluate different solutions. We have introduced a taxonomy of these methods and identified each method's weaknesses. The remaining sections of this article are organized as follows: The next section explains the characteristics of cloud computing and its role in DDoS attacks. The subsequent section presents the DDoS attack scenario in cloud computing. Next, a taxonomy of DDoS attacks in Cloud computing is presented. Then previous approaches used to