Chapter 75
Security of the Cloud

Khalid Al-Begain
University of South Wales, UK

Michal Zak
University of South Wales, UK

Wael Alosaimi
University of South Wales, UK

Charles Turyagyenda
University of South Wales, UK

ABSTRACT

The chapter presents current security concerns in the Cloud Computing Environment. The cloud concept and operation raise many concerns for cloud users since they have no control of the arrangements made to protect the services and resources offered. Additionally, it is obvious that many of the cloud service providers will be subject to significant security attacks. Some traditional security attacks such as the Denial of Service attacks (DoS) and distributed DDoS attacks are well known, and there are several proposed solutions to mitigate their impact. However, in the cloud environment, DDoS becomes more severe and can be coupled with Economical Denial of Sustainability (EDoS) attacks. The chapter presents a general overview of cloud security, the types of vulnerabilities, and potential attacks. The chapter further presents a more detailed analysis of DDoS attacks' launch mechanisms and well-known DDoS defence mechanisms. Finally, the chapter presents a DDoS-Mitigation system and potential future research directions.

1. INTRODUCTION

Security is one of the most presented obstacles against broader expedition of Cloud computing. Majority of the customers are struggling to make the decision to move into the cloud computing arena because of security concerns and data protection aspects. A survey conducted by Intel (2012) proved that almost 9 out of ten respondents expressed their concerns regarding the security within the cloud environment.

DOI: 10.4018/978-1-5225-5634-3.ch075

In the traditional approach, sensitive business data was stored in-house. However, the migration to the cloud implies that vital information is stored offsite at multiple locations and often in a way that is hardly understood by most people.

There are several security aspects that may pose multiple threats to the cloud. The list of these threats includes the; possibility of a breach of privacy, likelihood of phishing, possibility of information loss and the loss of direct control of data. In addition, several important aspects need to be addressed prior to the migration to the cloud, i.e. data location, a disaster recovery plan, information segregation, regulatory compliance, long-term viability and investigation support. (Kuyoro & Ibikunle, 2011).

In general, all computer systems, the cloud included, have to provide integrity, confidentiality and availability. However, as soon as the system is connected to the network, and it is available for the users, it inevitably becomes available to the attackers. Attackers can affect the availability of cloud service resulting in a significant inconvenience to the intended users.

This chapter presents the current security threats on cloud computing. Section 2 presents, a general overview demonstrating the basic security risks within the Cloud Computing environment. This section also discusses the specific threats that may affect the availability of the Cloud particularly the Denial of Service (DoS) and the distributed version of the DoS, known as DDoS.

Section 3 presents an overview of current defence mechanisms designed to mitigate DDoS security threats. Additionally the section introduces the Enhanced DDoS-Mitigation System architectural framework.

Finally, the section 4 concludes the chapter with a discussion on future challenges and research direction presented from three perspectives. Namely; the general security challenges within the cloud, future concerns regarding DDoS attacks and future challenges regarding the Enhanced DDoS-Mitigation System are presented.

2. CLOUD SECURITY THREATS

Various aspects that may pose security threats to the cloud user or even the cloud provider will be discussed in this section. To facilitate presenting these threats, they are classified into four groups, namely: policy and organisational risks, technical risks, physical security issues, and legal risks (ENISA, 2009).

2.1 Policy and Organizational Risks

This category of threats involves the concerns that may affect the customers' data security as a result of changes to the providers' business situation and/or the lack of their commitment to the agreed contract and Service Level Agreement (SLA) with customers. SLA is a document that identifies the relationship between the provider and the customer. This is obviously a very vital piece of documentation for both parties. If employed accurately it must:

- Recognise and identify the customer's requirements.
- Facilitate complicated problems.
- Decrease areas of conflict.
- Support dialog in the event of a conflict.
- Reduce unrealistic expectations (The Service Level Agreement, 2007).