

Chapter 7

A Review of Security Challenges in Cloud Storage of Big Data

Sara Usmani

National University of Sciences and Technology (NUST), Pakistan

Faiza Rehman

National University of Sciences and Technology (NUST), Pakistan

Sajid Umair

National University of Sciences and Technology (NUST), Pakistan

Safdar Abbas Khan

National University of Sciences and Technology (NUST), Pakistan

ABSTRACT

The novel advances in the field of Information Technology presented the people pleasure, luxuries and ease. One of the latest expansions in the Information Technology (IT) industry is Cloud Computing, a technology that uses the internet for storage and access of data. It is also known as on-demand computing. The end user can access personal data and applications anywhere any time with a device having internet. Cloud Computing has gained an enormous attention but it results in the issues of data security and privacy as the data is scattered on different machines in different places across the globe which is a serious threat to the technology. It has many advantages like flexibility, efficiency and scalability but many of the companies are hesitant to invest in it due to privacy concerns. In this chapter, the objective is to review the privacy and security issues in cloud storage of Big Data and to enhance the security in cloud environment so that end users can enjoy a trustworthy and reliable data storage and access.

INTRODUCTION

Cloud Computing is considered as the standard for next generation computation. In Cloud Computing, the resources i.e., end user applications, personal data or DBMS (Database Management Systems) are provided by a third party over internet like services. National Institute of Standards and Technology (NIST) defines Cloud Computing as universal, appropriate, on-demand network access to a shared pool

DOI: 10.4018/978-1-5225-3142-5.ch007

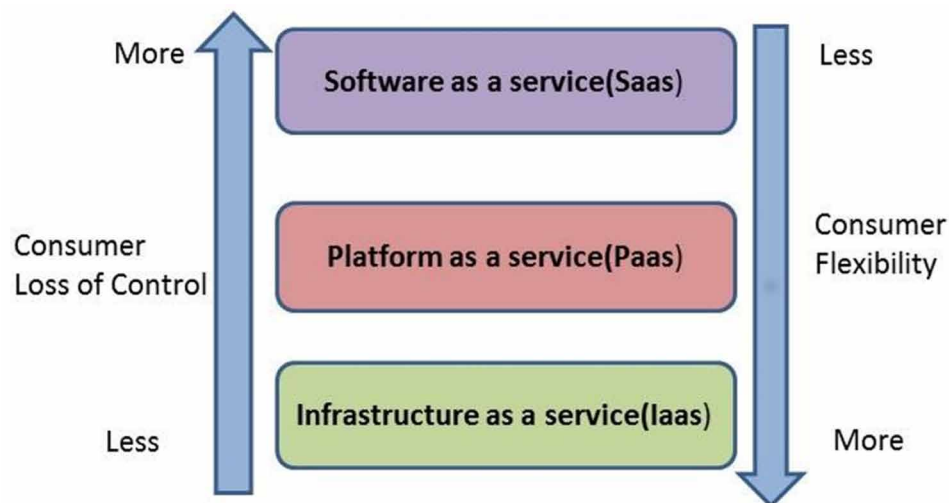
of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction (Mell & Grance, 2011). There is a service provider that manages and provides the services over the internet while the clients purchase them according to their needs. The architecture of cloud includes several modules like databases, software competencies, applications, etc. planned to influence the power of cloud resources to solve problems of enterprise. The architecture of cloud includes modules and the relationship between these modules. The cloud architecture has several components like

- Resources on ground cloud resources.
- Software services and components middleware.

The cloud architecture is intended at providing the users with huge bandwidth allowing them continuous access to their data and applications and having the ability to move rapidly and competently between servers or even between clouds. The service model comprises three levels: Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) as described in Figure 1.

In SaaS, applications are accessed via web browsers that are managed by cloud service provider and interfaces available on the end-user side. It removes the need to perform any installation or download on individual devices. In PaaS, applications are built on the platform. The services are provided to the user through a set of programs that can carry out the specific task. It makes the building and deployment of applications quick and economic. IaaS facilitates services through virtual machines. It provides the computer infrastructure with on demand resources. The users do not have to purchase the equipment; they have to purchase the service.

Figure 1. SPI Cloud Service Delivery Model (Almorsy, 2010)



19 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

www.igi-global.com/chapter/a-review-of-security-challenges-in-cloud-storage-of-big-data/198762

Related Content

Categorizing Post-Deployment IT Changes: An Empirical Investigation

David Kang (2007). *Journal of Database Management* (pp. 1-24).

www.irma-international.org/article/categorizing-post-deployment-changes/3368

Merging, Repairing, and Querying Inconsistent Databases

Luciano Caroprese and Ester Zumpano (2009). *Handbook of Research on Innovations in Database Technologies and Applications: Current and Future Trends* (pp. 358-364).

www.irma-international.org/chapter/merging-repairing-querying-inconsistent-databases/20720

Component-Based Generalized Database Index Model

Ashraf Gaffar (2005). *Encyclopedia of Database Technologies and Applications* (pp. 87-92).

www.irma-international.org/chapter/component-based-generalized-database-index/11127

Monitor and Detect Suspicious Transactions With Database Forensic Analysis

Harmeet Kaur Khanuja and Dattatraya Adane (2018). *Journal of Database Management* (pp. 28-50).

www.irma-international.org/article/monitor-and-detect-suspicious-transactions-with-database-forensic-analysis/227036

Rapid Privacy Preserving Algorithm for Large Databases

K. Anbumani and R. Nedunchezian (2009). *Database Technologies: Concepts, Methodologies, Tools, and Applications* (pp. 1050-1061).

www.irma-international.org/chapter/rapid-privacy-preserving-algorithm-large/7958