Chapter 52
Security Mechanisms in Cloud Computing-Based Big Data

Addepalli V. N. Krishna
Christ University (Deemed), India

Balamurugan M.
Christ University (Deemed), India

ABSTRACT

In the existent system, data is encrypted and stored when passed to the cloud. During any operations on the data, it is decrypted and then the computation is done. This decrypted data is vulnerable and prone to be misused. After the computations are done, the data and the result are encrypted and stored back in the cloud. This creates an overhead to the system as well as increases time complexity. With this chapter, the authors aim to reduce the overhead of the systems to perform repeated encryptions and decryptions. This can be done by allowing the computations to happen directly on the encrypted text. The result obtained by performing computations on encrypted data will be the same as the ones done on the original plain text. This new security solution is fully fit for processing and retrieval of encrypted data, effectively leading to the broad applicable project, the security of data transmission, and the storage of data. The work is secured further with additional concepts like probabilistic and time stamp-based encryption processes.

INTRODUCTION

The data in cloud is so vast that the primary importance in storing it, is its security. The security issues could be traditional in nature, reachability and unknown person's control of data. The attacks like intrusion detection systems in centralized and distributed environments, Virus or worm types of attacks, Cyber security attacks forms the core of attacks. The data is so vast that it may not be stored at one server or at one location. Thus the data is truly in a distributed environment. The data may be in different formats which make it highly complex in accessing it. These issues make it difficult in providing security to it. One more issue that is relevant to cloud is in real time context, the owner of data is different, the user is

DOI: 10.4018/978-1-7998-5351-0.ch052

also a different person and the control of data lies with a different person or different authority. This type of scenario makes it complex in providing the security to it. Most of Cloud based operations are Data Centric. The number of people who are using cloud environment is increasing every day. Similarly the number of Cloud service providers are also increasing. The main purpose of cloud users will be in its simplicity and efficiency in using the resources and service provider job is to provide the resources at ease, low cost and less time. Thus a frame work has to be developed which supports both the features. The Security to Cloud data may be Application based Encryption and Key Management which support the services like Security, Confidentiality, Authentication and Integrity of Message. The Architecture has to be framed such that it is not only ease, efficiency, low cost or less time but also its security. The security can be provided at multiple levels like network security, data security and application security. Thus the mechanism must be designed such that it supports security at all these levels. It must take care of different vulnerabilities that are to be associated with this type of architecture and designed to overcome them. It must also take care of different tools and services associated with it while operating in cloud environment. The concept of security has been around for quite some time now. It goes all the way back to the Paleolithic era, where cavemen used natural resources such as rocks, and branches to ward off predators and keep themselves out of harm's way. Today, security is present in almost every aspect of our lives. For an enterprise, security is one of the most fundamental essentials on which it is built. From security of employees to financial security and all the way to information security, it is highly impossible for any organization to structure its foundation without security. Most of the organizations generate massive amounts of data, consequently making information security extremely significant. Also, the plethora of data being spawned is now stored on cloud systems thereby providing enterprises with flexibility in the amount of data produced by them.

Cryptography (Stallings,W,2006) is a vital technology in engineering information security in communications, computer systems, and in the emerging information society. It is believed that the art of cryptography originated along with the art of writing. The first known evidences of cryptography traces back to ancient Egyptian civilizations. Since then cryptography has grown exponentially, and today it is an indispensable branch of mathematics, and computer science. Symmetric and asymmetric cryptography are the two basic fields into which cryptography can be broken down to. The former is also known as symmetric key encryption wherein a single key is used for both encryption as well as decryption. The latter (IEEE Standard 1363, 2000) makes use of two different keys for encryption and decryption, and hence is also called as public key cryptography. However, these encryption schemes have a downside; in order to perform computations on data encrypted using these schemes, data has to be decrypted thereby exposing it to all the usual threats.

Cloud systems provide various computing services such as storage, servers, networks, databases, and software's. The services provided by cloud systems are grouped under three major categories. They are IaaS (Infrastructure as a Service), PaaS (Platform as a Service), and SaaS (Software as a Service). Services provided by IaaS are usually for performing computations (servers), and for storage purposes (databases). PaaS provided a platform for the different cloud users to host their applications. SaaS as the name suggests provides software to the users. Instead of having to install software, and then run it, accessing it directly from the cloud would be much simpler, and feasible to the user.

The CIA Triad (Fig.1) symbolizes the security objectives for information security, and computing services. CIA is expanded as Confidentiality, Integrity, and Availability. Confidentiality states only authorized users have access to private information, whereas integrity assures that data is modified only