Chapter 4
Cryptography in Big Data Security

Navin Jambhekar
S. S. S. K. R. Innani Mahavidyalaya Karanja, India

Chitra Dhawale
P. R. Pote College of Engineering and Management, India

ABSTRACT

Information security is a prime goal for every individual and organization. The travelling from client to cloud server can be prone to security issues. The big data storages are available through cloud computing system to facilitate mobile client. The information security can be provided to mobile client and cloud technology with the help of integrated parallel and distributed encryption and decryption mechanism. The traditional technologies include the plaintext stored across cloud and can be prone to security issues. The solution provided by applying the encrypted data upload and encrypted search. The clouds can work in collaboration; therefore, the encryption can also be done in collaboration. Some part of encryption handle by client and other part handled by cloud system. This chapter presents the security scenario of different security algorithms and the concept of mobile and cloud computing. This chapter precisely defines the security features of existing cloud and big data system and provides the new framework that helps to improve the data security over cloud computing and big data security system.

DOI: 10.4018/978-1-5225-2863-0.ch004

1. INTRODUCTION

1.1 Background

Nowadays due to recent technological development, the amount of data generated by internet, social networking sites, sensor networks, healthcare applications, Banking Sector and many other companies, is drastically increasing day by day. All the enormous measure of data produced from various sources in multiple formats with very high speed (Bagheri & Jahanshahi, 2015) is referred as big data. The term big data (Bosch et al, 2014; Chan, 2009) is defined as "a new generation of technologies and architectures, designed to economically separate value from very large volumes of a wide variety of data, by enabling high-velocity capture, discovery and analysis".

From this definition, we can say that big data are reflected by 3V's, which are, volume, velocity and variety. A common theme of big data is that the data are diverse, i.e., they may contain text, audio, image, or video etc. This big data is stored on cloud and to attain the big data security over cloud computing, the mono encryption technique is not adequate. Because of the voluminous architecture of cloud computing system, the traditional data security systems are not adequate to provide the complete security solution.

During mobile communication, the encryption and decryption facilities are harder to implement. Clouds can work in collaboration, even if they have their own security features. Therefore, without modifying the sequence of the encryption process, the parallel and distributed encryption facilities will be available at every cloud during surfing from cloud to cloud. Every cloud manages the essential resources and allocation can be done on every request of the resource while user moves from one cloud to another. The major issues when dealing with the cloud computing system is the network and resource availability. If the resources are not allocated during cloud computing, the encryption and decryption cannot feasible and can be difficult to pursue. The cloud collaborative encryption is a technique where, various clouds can work concurrently with distributed processing facilities. Here, the security can be enhanced by implementing the homomorphic encryption.

2. BASICS OF CRYPTOGRAPHY

Data communication plays a vital role for every individual or organization all over the world. Every organization completely relies on the day-to-day data processed by their systems. Massive amount of data transferred from one location to another,