# Chapter 22
# Ensure Hierarchal Identity Based Data Security in Cloud Environment

**Shweta Kaushik**
*JIIT Noida, Noida, India*

**Charu Gandhi**
*JIIT Noida, Noida, India*

## ABSTRACT

*Cloud computing has emerged as a new promising field in the internet. It can be thought as a new architecture for the next generation of IT enterprises. It allows the user to access virtualized resources over the internet which can be dynamically scaled. Here, the owner's data is stored at a distributed data centre, which are responsible for its security constraints such as access control and data transmission to user. As the owner does not have physical access on their own data, the data centres are not trustworthy, this resulted in the cloud data security demand. Today, many cloud service providers (CSPs) are using the asymmetric and public key cryptography (PKG) for authenticating and data security purposes using the digital identity of the user. To this end, this article focuses on cloud data storage and its delivery to authorized user. For this purpose, a hierarchal identity-based cryptography method is used for data security and checking the data integrity, in order to make sure that there is no alteration or modification done by a malicious attacker or CSP for its own benefit.*

## INTRODUCTION

Cloud computing has been envisioned as a new model in distributed system to allow large amount of resource access, distributed over large network and pooled as per scaled requirement. The National Institute of Standard & Technology (NIST) (Mell et al., 2011) explain cloud computing as a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources. This all can be achieved through the use of Infrastructure as a Service (IaaS), Platform as a

DOI: 10.4018/978-1-7998-5351-0.ch022

Service (PaaS), and Software as a Service (SaaS). Users are able to acquire their required computing resources, services over Internet as per their need. Resource elasticity facilities, for computing resources are also supported by cloud. All these tasks are managed and controlled by Cloud Service Provider (CSP).

Nowadays, cloud computing concept is used by almost each and every application related to software services such as social networking (Gupta et al., 2018, Li et al., 2018), photo editing, image processing, word processing, online presentation etc. and also in combination with other techniques such as IoT (Stergiou et al., 2018), mobile computing (Raja et al., 2018) Big Data (Gupta et al., 2018), etc. Use of cloud computing allows the data owner to store their confidential and sensitive data over Internet and abolish the burden of its management and security. Afterwards, CSPs are totally responsible for data storage, management, distribution and security from any malicious attacker and its leakage. Today many organizations in banking, education and healthcare domain are utilizing the facility of cloud computing for storage of their sensitive data as well as access of the data by authorized users from anywhere across the globe at any time via the internet Many big, medium and small companies such as Google, Amazon, Yahoo, and Microsoft, etc., are also providing various kinds of cloud services to their users for fast, safe and easy access of data. They all have their own defined security policies and model. Gupta et al. (2016) defined security policies as a set of rules that provide the guidelines for behaviour of different entities that are related to an organization. Unfortunately, cloud technology will not always come alone, it compels various security issues related to owner's data security. Broadly, these issues can be divided into data confidentiality, integrity and its access control.

Access control requires that only the authorized users who are fulfilling the access criteria, defined by the owner, can only get the required data. This feature is used to ensure that owner's critical and sensitive data will not be disclosed to any unauthorized user. Integrity requirement arise to maintain a trust level between different communicating parties to ensure that the data has not been altered by sender. Integrity plays an important role between CSP and cloud user. User accesses their required data from CSP not from the owner. Here data integrity gives user a belief that received data is intact without any alteration. Integrity of data can be checked in two parts- i) signature generated by the owner and ii) data verification by receiver.

To protect owner's critical and sensitive data from any malicious attack confidentiality is prime requirement. This can be achieved by encrypting the data before transmitting over cloud environment and only authorized users are facilitated with decryption key (Chow et al., 2009) and (Kamara et al., 2011) also stated that encryption of outsourced data is a good option to mitigate this security concern. (Gupta et al., 2018), (Negi et al., 2013) discuss the various cryptography way to ensure the cloud data security, privacy and trust management among different parties. Confidentiality requires complex, flexible and efficient sharing of key among users. To achieve this, Public Key Generator (PKG) with certification approach has been widely used since last many years. A variant of this technique is Identity Based Cryptography (IBC) (Water et al., 2009, Boneh et al., 2008) which is gaining high consideration. In IBC, each entity works as a public key generator, is responsible for generating its own public key and a corresponding private key. Public key is generally the identity of the entity which is on-the-fly, used for authentication purpose. Main advantage of IBC is to provide a great flexibility for all entities, defined under particular security environment. In contrast, certificate approach is not required in IBC, which helps in dynamic nature of cloud computing. In other word, we can say that in comparison to traditional PKG approach IBC provides more flexible and lightweight key management approach among different entities under cloud environment. To improve scalability a variant of IBC called Hierarchal Identity Based Cryptography (HIBC) has been used in recent (Lim et al., 2004; Dai et al., 2006; Lim et al., 2005).