Chapter 71
Necessity of Key Aggregation Cryptosystem for Data Sharing in Cloud Computing

R. Deepthi Crestose Rebekah
Ravindra college of Engineering for Women, India

Dhanaraj Cheelu
Ravindra college of Engineering for Women, India

M. Rajasekhara Babu
VIT University, India

ABSTRACT

Cloud computing is one of the most exciting technologies due to its ability to increase flexibility and scalability for computer processes, while reducing cost associated with computing. It is important to share the data securely, efficiently, and flexibly in cloud storage. Existing data protection mechanisms such as symmetric encryption techniques are unsuccessful in preventing data sharing securely. This article suggests Key aggregate cryptosystem which produce constant size ciphertexts in order to delegate decryption rights for any set of ciphertexts. The uniqueness is that one can aggregate any number of secret keys and make them as compact as a single key. This compact aggregate key can be easily sent to others with very limited secure storage.

CLOUD COMPUTING ARCHITECTURE

Cloud computing is a model for delivering information technology services in which resources are retrieved from the internet through web-based tools and applications, rather than a direct connection to a servers (Kanchana & Dhandapani, 2013) (Rajasekhara et al., 2014). However, cloud computing structure allows access to information as long as an electronic device has access to web.

DOI: 10.4018/978-1-5225-8176-5.ch071

Characteristics of Cloud Computing

The five essential characteristics of cloud computing are On-demand self-service, broad network access, resource pooling, rapid elasticity and measured service:

1. **On-Demand Self-Service:** A service provided by the cloud vendors that enable the provision of cloud resources on demand whenever they are required (Zhang et al., 2010).
2. **Broad Network Access:** The resources hosted on a cloud network that are available for access from a wide range of devices such as smart phones, tablets, personal computers etc., and these resources are accessible from different locations that offer online access. (Prakash, 2013).
3. **Resource Pooling:** The computing resources are pooled by cloud vendors to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand [3]. The examples of resources include storage, processing, memory, network bandwidth and virtual machines.
4. **Rapid Elasticity:** It allows the users automatically control and optimize resource by using a metering capability at some level of abstraction appropriate to the type of services (Mell & Grance, 2014). Resource usage can be monitored, controlled and reported providing transparency for both the provider and consumer of the service.

Service Models of Cloud Computing

Cloud service models describe cloud services are made available to users. Figure 1 explains three service models – SaaS, PaaS and IaaS which provide resources to the users:

1. **SaaS:** It provides the customers with ready to use application running on the infrastructure service provider. The applications are easily accessible from several client devices as on demand services. Salesforce, DocLanding, Zoho, Workday are instances of SaaS are used for different purposes such as email, billing, human resource management etc. (Figure 1),
2. **PaaS**: It provides platform oriented service controlling the installed applications and available hosting environment configuration. Google AppEngine, LoadStorm are the instances of PaaS for running web applications and testing their performance.
3. **IaaS**: It provides infrastructure services such as memory, CPU and storage. The consumer can deploy and run software. It reduces hardware costs. Amazon S3 and FlexiScale, Dropbox are the best examples of IaaS for storing and maintaining virtual servers.

Deployment Models of Cloud Computing

While service models describe the specific capabilities of cloud solutions, deployment models describe where, how, and by whom the cloud's physical servers are managed (Armbrust et al., 2010). Cloud computing may be deployed as private, public and hybrid, which are shown in Figure 2:

1. **Private Cloud:** A private cloud is a particular model of cloud computing that involves a distinct and secure cloud based environment in which on the specific client/ organization can operate.