# Symmetric Cryptographic Key Management in Cloud Based Environment

By

**Faiza Fakhar**

**2010-NUST-MS PhD-IT-27**

Supervisor

**Dr. Muhammad Awais Shibli**

**Department of Computing**

A thesis submitted in partial fulfillment of the requirements for the degree of Masters of Science in Information Technology (MS IT)

In

School of Electrical Engineering and Computer Science,
National University of Sciences and Technology (NUST),
Islamabad, Pakistan.

(Feburary 2014)

# Abstract

Cloud computing is emerging paradigm taking the attention of millions of buyers and suppliers. It provides several benefits to its consumer such as availability, flexible cost model, on demand self services, elastic resources, etc. It facilitates their consumers by providing software, platform and infrastructure as service. Thus, users of Cloud do not have to be concerned about the complexities of software, hardware or infrastructure. Furthermore, increasing bandwidth and trustworthy network connection make it possible for businesses to subscribe to high quality services according to their requirements.

Despite of all the benefits delivered by Cloud computing, several security challenges such as data security etc. are hampering the migration of customer applications on Cloud. These challenges stems from the fact that consumer of public Cloud services has no access on physical servers while utilizing different Cloud services. They do not have any clue about their data locality; hence, data security threats become more challenging at the Cloud. Some security mechanism must be in place in order to address this anxiety.

There are several security mechanisms such as encipherment, digital signature, access control, data integrity, authentication exchange, traffic padding, routing control, notarization and cryptography.

Cryptographic is one of the security mechanisms that protect information from unauthorized confession. It can be used to provide security for data storage to protect its integrity while storing data on Cloud paradigm. Cryptographic key management is the most important element of cryptographic system as effective use of cryptographic system requires proper management of cryptographic key. To date, cryptographic key security has been ensured to protect it from vulnerability and security breaches. However, the use of cryptographic key in online or Cloud based applications has prompted large fraction of information security attacks since the consumer of Cloud does not have access to the physical storage servers.

Cloud Security Alliance (CSA), the global leaders in Cloud security, has identified that the cryptographic key management at Cloud is a challenge.

They recommended that cryptographic keys should be stored on enterprise domain due to their sensitive nature. However, searching of encrypted data from a large data set is problematic on Cloud storage while cryptographic keys are stored at enterprise premises. Furthermore, these limitations of encrypted data restrict Cloud users and they cannot utilize all benefits of Cloud paradigm. All these concerns require a strong cryptographic key management system that can reduce the intricacy of operation on Cloud stored data by processing them on same platform.

This research provides an effective and robust security protocol for symmetric cryptographic key management in Cloud that attempts to resolve the above mentioned issues. This thesis contributes in following aspects;

- ***Secure Data Storage on Cloud:*** This part of research offer a mechanism for secure storage of sensitive data on Cloud. This storage scheme can be further utilized in any type of data storage. Using secure protocol user can share cryptographic key with Cloud to manipulate encrypted data.

- ***Symmetric Cryptographic Key as Cloud Service:*** Our second part of research provide symmetric cryptographic key as Cloud service and user may embed this service in other utilities such as mobile/PDAs digital signature utilities etc.

- ***Secure Data Access:*** On the fly computation of cryptographic key will ensure key access security.

Proposed protocol is based on secret splitting and use enhanced Shamir's algorithm for cryptographic key splitting. Furthermore, this protocol distributes cryptographic key components to various Cloud servers. That ensures cryptographic key protection, even if the security on one of the Cloud server is compromised. All data transfer between Clouds is done through pkcs#7 protocol, that provides data enveloping and de-enveloping during data travelling in insecure environment. In addition to this, SSL protocol is also used which connect end user browser to an application server securely.

The proposed protocol is validated using Scyther validation tool used to analyze security protocols. Furthermore, we have also evaluated our protocol using NIST defined qualitative criteria.