# Chapter 52
# Cryptographic Cloud Computing Environment as a More Trusted Communication Environment

**Omer K. Jasim**
*Alma'arif University College, Iraq*

**Safia Abbas**
*Ain Shams University, Egypt*

**El-Sayed M. El-Horbaty**
*Ain Shams University, Egypt*

**Abdel-Badeeh M. Salem**
*Ain Shams University, Egypt*

## ABSTRACT

*Cloud Communication Environment is an internet-based computing, where shared resources, software, and information are provided with computers and devices on-demand. They guarantee a way to share distributed resources and services that belong to different organizations. In order to develop cloud computing applications, security and trust to share data through distributed resources must be assured. This paper offers a study of the different mechanisms used in open cloud environments such as keys generation and management, and encryption/decryption algorithms. In addition, the paper proposes a new cryptographic environment, annotated as "CCCE" that deploys the combination between quantum key distribution mechanisms (QKD) and advanced encryption standard (AES), and demonstrates how quantum mechanics can be applied to improve computation.*

DOI: 10.4018/978-1-5225-8176-5.ch052

## INTRODUCTION

Recently, Cloud computing (CC) (Ateniese, Kamara, 2012) has widely been applied in several industrial fields such as Google, Facebook, Amazon, and (e-business, e-learning... etc.) and is considered a new communication technique that combines multiple disciplines such as parallel computing, distributed computing and grid computing. In return, it provides Virtualization, utility computing, and other multiple services for client enterprise (Ateniese, Kamara, 2012; CCA, 2013).

Basically, cloud computing main principles are based on sharing resources among separately distributed servers and individual clients. This sharing is performed by enabling free accessing of the stored files and data for all clients (CSA, 2013).

Despite the free data accessing is considered an advantage; it has several drawbacks such that any cloud client can manipulate any file transferred through cloud communication. Consequently, many companies have explored the critical areas in a CC environment.

CSA (2013) is an example of those companies, which delivers a package that contains cloud provider, clients and considers the security model. The CSA security model has the ability to interrupt the intruder, who is responsible for destroying and interrupting the original data files and communications.

Later on, the security guarantee issue in cloud communication environment has become a challenge and which attract many studies, such as Hail et al. (1999), who discuss the technical security issues arising from side channel - attacks, browser attacks, browsers' related attacks, and authentication attacks.

Moreover, Jensen et al. (2009) discuss the security vulnerabilities existing in the cloud platform. They grouped the possible vulnerabilities into technology-related, cloud characteristics-related and security controls- related.

In spite of different studies' attempts to solve the security problem in cloud communications, many gaps and threads are still uncovered or handled. In the meantime, all proposed attempts consider the main three building modules in the cloud communication architecture [see Figure 1]. However, none of these attempts care about the whole performance of the interaction between the constituent modules, which in turn, caused data transformation delaying (IDC, 2011; John, Ingo, 2010) and provide a high chance for the attackers to discover the main encryption key and intrude the data streams in the transferred files.

This paper proposed a secured cloud computing environment annotated as "CCCE" in which, a hybrid technique is used in the encryption and decryption processes. The proposed hybrid technique combines the Advanced Encryption Standard Algorithm (AES) and QKD that generates the keys used for the encryption process randomly.

The rest of the paper is organized as follows: the second section shows the CC architecture and implication security, the third section describes the CC precaution, the various types of attacks that threaten the CC data transformation are discussed in the fourth section, the models of cloud encryption files are explained in the fifth section, the sixth section proposes the CCCE architecture and discusses in detail its main building modules including an illustrative example that represents the main functions used through the interaction between the main modules, the seventh section provides the analytical analysis for the proposed model and finally, the eighth section presents the conclusion.