Chapter 4
CCCE:
Cryptographic Cloud Computing Environment Based On Quantum Computations

Omer K. Jasim
Al-Ma'arif University College, Iraq

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

Safia Abbas
Ain Shams University, Egypt

Abdel-Badeeh M. Salem
Ain Shams University, Egypt

ABSTRACT

Cloud computing technology is a modern emerging trend in the distributed computing technology that is rapidly gaining popularity in network communication field. Despite the advantages that the cloud platforms bolstered, it suffers from many security issues such as secure communication, consumer authentication, and intrusion caused by attacks. These security issues relevant to customer data filtering and lost the connection at any time. In order to address these issues, this chapter, introduces an innovative cloud computing cryptographic environment, that entails both Quantum Cryptography-as-service and Quantum Advanced Encryption Standard. CCCE poses more secure data transmission channels by provisioning secret key among cloud's instances and consumers. In addition, the QCaaS solves the key generation and key distribution problems that emerged through the online negotiation between the communication parties. It is important to note that the CCCE solves the distance limitation coverage problem that is stemmed from the quantum state property.

INTRODUCTION

In this era, computing is categorized according to their usage pattern. Parallel Computing, Sequential Computing, and Distributed Computing are a well-known form of computing technologies (Sunita & Seema, 2013). In general, distributed computing involved in many communication systems to solve a large scale communication problems. The growing of high-speed broadband networks and the rapid growth of the Internet changed the network communication way. Thus, the new trends of distributed computing

DOI: 10.4018/978-1-4666-9834-5.ch004

technology require integration between distributed computing systems and networking communication systems (Aidan, Hans, Patrick, and Damian, 2012). This integration allows computer networks to be involved in a distributed computing environment as full participants in other sharing computing resources such as CPU capacity and memory/disk space.

Emerging trends in distributed computing paradigm include grid computing, utility computing and cloud computing (Sunita & Seema, 2013). These emerging distributed computing together with the development of networking technologies are changing the entire computing paradigm toward a new trend in distributed computing. This chapter describes the emerging technology in distributed computing which known as cloud computing.

Cloud computing is a specialized form of grid and utility computing, and that takes grid computing style when the dynamic connection service and the virtual resources service are available through the internet. In addition, any cloud architecture consisting of many layers (Service Platform Infrastructure layers-SPI) such as the infrastructure as a service (IaaS), the platform as a service (PaaS), the Software as a Service (SaaS) and some others collectively as a services (*aaS). These services layers offer numerous roles as reducing the hardware costs, providing the reliability of each consumer and provisioning resources on-demand (Chander & Yogesh, 2013; Mohammad, John, & Ingo, 2010).

SPI layers and Service Level Agreements (SLA) provide communication between cloud services provider (CSP) and consumers using cloud networks. Since cloud computing environment is a virtual and dynamic, it requires a scalable hardware that supports the virtualization technology and data transformation remotely. Data transformations remotely expose the whole cloud environment to various attacks (Faiza, 2012; Mather & Kumaraswamy, 2012). Therefore, a secure communication is an essential prerequisite for opening cloud environment as a robust and feasible solution (Kumaraswamy, 2012). Many distinct cloud security groups discussed the security vulnerabilities in the cloud computing and classified the possible vulnerabilities into cloud characteristics-related and security controls- related (Omer, Safia, El-Sayed & Abdel-Badeeh, 2014).

Despite different groups try to solve the security challenges in cloud computing, many gaps and threads are still uncovered or handled. Accordingly, the cryptographic tools are installed and developed in many cloud computing environments. These tools require a long-term secret key to guaranteeing the encryption/decryption process, which in turn, considered a valuable target for various attacks (Doelitzsch, Reich, Kahl & Clarke, 2011).

In the cloud computing environment, deploying such long-secret key for any modern encryption algorithm (symmetric or asymmetric) ensures the data confidentiality (prevention of unauthorized disclosure of information), integrity (change in the data), and availability (readiness of correctional services) (CSA, 2012, Omer, Safia, El-Sayed & Abdel-Badeeh, 2013). Despite the solvable problems based such long secret key, the key management and distribution problems still disclosed.

Quantum Key Distribution (QKD) addresses these problems in distributed computing and negotiation mechanism. It can preserve data privacy when users interact with remote computing centers remotely (Doelitzscher, Reich, Knahl & Clarke, 2011; Dabrowski, Mills, & orphan, 2011).

This chapter presents a robust cloud cryptographic environment that completely depends on quantum computations and a newly developed symmetric encryption algorithm. In addition, this chapter introduces an innovative CCCE, which poses more secured data transmission by provisioning secret key among cloud's instances based on QCaaS layer. Finally, this chapter solves the distance limitation coverage problem, by measures the randomness of qubits based on the NIST and DIEHARD test suite algorithms (Juan S., 2012; Andrew, Juan, James, Miles, Elaine and Stefan, 2013).

Related Content