QKD Communication Protocol for Authentication Mechanism

Associate Prof.Dr.Zuriati Ahmad Zukarnain
Department of Communication Technology and Networks, Faculty of Computer Science and Information Technology

Abstract

A unique communication protocol is proposed for Authentication Mechanism in replacing the key distribution technique based on public key infrastructure to achieve unconditional security in cloud. Cloud infrastructure provides many benefits in terms of low cost and accessibility of data. Ensuring the security aspect is a major factor in the cloud infrastructure. Today authentication to grant the communication are achieving through cryptography. Many encryption and decryption techniques are in place and ready to use in cloud computing technology. Many researchers have proposed a method by implementing RSA algorithm, and Public Key Infrastructure to ensure the security of data transfer in cloud computing. However, due to some circumstances, this algorithm or cryptography technique still cannot guarantee it is secure.

Besides the issue on reliably transmitting classical information through classical channel, which is focus on cloud network. Quantum key distribution has been an impressive diversity of application in communication security. Quantum key distribution is actually also known as part of Quantum Cryptography (QC). It is grow into the field in current world and has a potential as advanced technology. The idea is mainly on managing a secret key for a secure communication process in the cloud. As a secret key management of key distribution the protocol involved are Cloud Client Authentication Scheme, Multiparty QKD (MQKD) that perform initial task in quantum key distribution, then quantum cloud authentication.

The QKD protocol is believed to be able to detect any eavesdropping activities and provide an effective security. The Quantum Key Distribution (QKD) protocol used the concept of Multiparty QKD (MQKD), which allow the same key is distributed to different parties based on quantum mechanism. A quantum key server generates a secret key that may strengthen the security aspects. A quantum key distribution key scheme is imposed in the cloud network to secure the top-secret message or information and capture the eavesdropper. The existence of quantum key storage between the cloud provider and cloud client may guarantee the integrity of communication process that ensure the party is authenticated and the communication cannot be intercept. The established QKD BB84 protocol is the first known quantum key distribution scheme that allows two parties; as standard convention that Alice as sender and Bob as receiver, to establish a secret shared key using polarized photons qubits. Eve is presented as eavesdropper.

The quantum information processing is analyzed using Entropy Measurement such as Shannon Entropy, Mutual Information and Von Neumann Entropy. This asymptotic finite key analysis will produce minimum and maximum entropy. Hence an enhanced tight finite scheme analysis to evaluate the efficiency of the proposed protocol. The qubit error rate is the important indicator to detect the insider and outsider attacks during authentication.