Cloud Computing Security Threat with Quantum Key Distribution Defense Model

Roszelinda Khalid and Zuriati Ahmad Zukarnain  
University Putra Malaysia  
Faculty of Computer Science and Information Technology,  
University Putra Malaysia, 43300, Selangor, Malaysia  
roszelinda@hotmail.com, zuriati@upm.edu.my

ABSTRACT

Cloud computing offer the cost-effective and flexibility to the user. However, the security threat is a main concern for user to place their data in the cloud. Data that stored and shares through cloud have to be confidential and restricted. Information leakage, men in the middle attack are the two main issues that make information stored in the cloud insecure.

Widely authentication method used is the classical approach like Public Key Infrastructure (PKI). This approach is workable in order to provide a secure environment within the cloud clients. The existing of Certificate Authority that act as controller they can verify the legal user. However, in certain circumstances, this approach cannot solve the issue such as stealing the identity. In this paper we are proposing a model that use quantum mechanical theory. This theory is supporting the no cloning theory. It used the power of light and a single photon to provide an authentication key.

Throughout this paper, we also do a literature on various security threats, and authentication method in cloud. Then, we are introducing a quantum defense model as a solution of the listed threats. We proposed new cloud authentication architecture for cloud computing environment. A new cloud authentication environment that implements quantum mechanics is proven that can gain more trust with less time of computation in cloud communications.

KEYWORDS

Quantum key distribution, authentication, security threat

1 INTRODUCTION

Reliability is compulsory when transferring information via a communication channel. Situation where the information leaks while transferring the information is a crucial situation especially when it is high profile information.

Trust, security and identity are always the issues in any service that provides Internet, but in cloud computing additional issue arise like control over data location. Handling and maintaining data in clouds is still a challenging issue. Due to its intrinsic resource- sharing and low-maintenance characteristics cloud computing has become the alternative in Information Technology. In cloud computing, the cloud service providers (CSPs), such as Amazon, are able to deliver various services to cloud users with the help of powerful data centers. Users can enjoy high-quality services and save significant investments on their local infrastructures By migrating the local data management systems into cloud servers. Data storage is one of the services provided by cloud. On the type of services needed by the
client, vendors provide 3 types of cloud models [1].

1.1 Private Clouds

In private clouds, the services and infrastructure are maintained privately in their own network. We can see that the security level is tight due to the size of network infrastructure they are monitoring. From the cost perspective, the cloud service client still has to subscribe the software and infrastructure services to reduce the cost.

1.2 Public Clouds

Public cloud provides an off-site over the Internet for its services and infrastructure. These types of network have sustainable efficiency in terms of resource sharing.

1.3 Hybrid Clouds

Hybrid clouds are the combination of a variety of public and private options in cloud with many providers. Lacking aspects in hybrid clouds is the cloud provides and attackers expose to disclose the real identity of the user.

Structure of this paper directed as follows; Section 2 introduces the basic threat in cloud; Section 3 explore authentication in cloud; Section 4 gives the literature review of the whole idea in cloud authentication by implementing quantum mechanics; Section 5 discusses our proposed methods; in Section 6 results and Section 7 conclusion.

2 THREATS IN CLOUD

This section gives an explanation on three types server attacks in cloud.

2.1 Unknown Server Attack

The services that are accessible from the public are implementing the client server network. This situation is actually exposed to the server to get attack from the client side. Chances of client to get access to the server are high.

![Figure 1: Malicious Server Attack](image)

Figure 1 shows the possibility on how the attacker may launch attacks to the victim server. Attacker will command client to generate unauthorized request to the server. The victim server without knowing the real situation will respond to it. The problem is, what if the request is coming from the attacker. Of course the victim server still will respond to it and finally the attacker are manage to own the victim server.

2.2 Finger Printing Server Attack

Finger printing server attack is usually happened in a log file. System administrator may notice if there is some abnormal situation in his log file. It happens when a client login to the server, then it will trace in the log file. When the client left the system, the log will delete his activity. However, if the login is from an attacker server, his log will not going to delete.
Figure 2 is the scenario of fingerprinting attack; Scan 1 is the size of the default log file before a user logs in. Scan 2 is the size of the log file after the session is killed. If size of file from Scan 2 is larger and Scan 1, it shows that the logs are still in the log file. The user has not logged out of the session. It supposed to be the size like Scan 1.

2.3 Distributed Denial of Service (DDOS) Attack

DDOS is an effort to make the entire network collapsed. By commanding a number of client to launch an attack by flooding the network bandwidth.

It also likes assigning zombies’ computer that control by an attack like Figure 3 to attack a specific server. This incident will incur lot of financial cost to restore the system like before.

3 Concept of Authentication in Cloud

Whether is a classical network or cloud network the authentication phase is being a hot debate. Authentication is an initial phase, before the information gets access. The main objective is how this kind of network, promise us that the information can be secure to be stored. Authentication is a process, where we verify the user who is going to use our system or access our information is legal and authorized user.

Figure 4 shows the basic concept of authentication in cloud. The user may request login to the system by his credentials. This could be their user name and password. Specify server will verify the credentials given and match it with the registered data in the server. If it is match then data in cloud can be assess.

4 LITERATURES OF EXISTING METHODS

Section 4 gives a literature review of the existing techniques for security issues in cloud computing. In paper [2] the authors highlight the security barriers in cloud computing is the process validation. The initial phase in process validation is authentication. It is become the prior point to convince the users in adopting cloud-computing technology.

Authentication and authorization in cloud is discussed in [3]. All the model of cloud infrastructure is included. Authentication mechanism is dedicated to verify and confirming the identity of clients, before they get access to cloud resources. Most well
known mechanism is password-based authentication. This mechanism is quite old fashion and most attackers already knew how to hack it. Most of the users, feels that this is weak mechanism to be implement in cloud network.

For improvement and high security aspect, authentication has been injected with additional aspect like public keys, X.509 certificates and implementation of cryptography such as RSA.

Authorization is giving privileges to the user for accessing data in cloud. It also includes data protection. Many cloud providers provides access control for users. In the scenario like cloud network, for giving an authorization could be tedious work. This is because; it could be many different cloud clients and each function for each access control needs to be different.

Model for secure multi-owner data sharing for dynamic groups in cloud name MONA [4] has been proposed. This proposed model is securing the information from any suspicious identity in the cloud. It applies the group signature scheme for privacy. However, because it is called as group signature, if one of the users does the alteration of the data, nobody could verify it. It just can be trace as group. What about, one of the group members is the traitor.

5 PROPOSED METHODOLOGY

In the previous section we have list 3 types of issues regarding to security and authentication in cloud. We are proposing an emerging technology to be implement in the defense model. Quantum key distribution (QKD) has been an impressive diversity of application in communication security.

This 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 is allow the same key is distributed to different parties based on quantum mechanism [5]. 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. Our scheme is using the QKD BB84 protocol. BB84 protocol is the first known quantum key distribution scheme, named after the original paper by Bennett and Brassard, published in 1984 [6]. It 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.

In our analysis it will involve entropies to quantitatively characterize problems in quantum information processing and quantum cryptography. In the case of many independent and identical instances of a task the von Neumann entropy is the relevant measure. In order to go beyond this restriction, we use smooth min- and max-entropies introduce by Renner [7]. The key for this proposed authentication of multiparty system using QKD protocol. Hence it will be 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.
Figure 5 is our proposed model for cloud authentication process with quantum mechanics. We use quantum key distribution method for initiating the authentication phase. Here we are using the strength of light to transfer a key in a single photon. In our model, the key in single photon will change in binary form. This will identify it as an initial key. This process will happen in quantum channel. Quantum key distribution and quantum channel is only dedicated for exchanging and distribute a key only for the purpose of authentication and authorization. After the authentication phase via quantum channel is successful, only then the process of transferring the information in the cloud network begin.

6 RESULTS

By applying a tight finite key in quantum key distribution, the problem of the man in the middle attack can be solved. We can see the result in figure 6. The information leakage is reducing by the length of key. This result also considers the interference that might occur such as noise. From the result it can gain trust from user, that their information will be secure enough be in in the cloud.

Figure 7: Time calculation for quantum key generation

In comparing the enhanced scheme with the existing scheme there is a high impact on the proposed method. Our proposed method also could reduce the time for key generation. Key generation is important to pursue the grant access. It is depend on the initial key size. We measure the key size between 5000 bits and 10000 bits. And the time taken is between 49ms to 250ms. The result is impressive even though there are addition phase need to go through compare to the current scheme. This explanation is referring to Figure 7.

7 CONCLUSIONS

In general, the current authentication scheme being used is still relatively backward methods especially in cloud environment. Many of the key aspects of authentication can’t guarantee effective control, especially in data transmission via a public channel. In this paper we are introducing a new scheme that can be adopt in multiparty communication dedicated
for cloud infrastructure. From the result we can see there is a significant result on reducing the error rate. We hope with the proposed scheme it can achieve the practical feasibility and simplicity in MQKD, a standard cryptographic like authentication scheme is designed. The simulation results show that our proposed protocol provides authentication of the clients is acceptable response to error rate and time. In addition, our results show that the proposed scheme could reduce amount of information leak and also less time consuming for generate a key.

REFERENCES


