Prevention of Authentication Problems Using Quantum Cryptography

Ch Lokesh Kumar[1] Dr Balarengadurai chinnaiah[2]

[1]UG Scholar, Department of CSE, Marri Laxman Reddy Institute of Technology and Management, Hyderabad

[2]Professor, Department of CSE, Marri Laxman Reddy Institute of Technology and Management, Hyderabad

Abstract- In this paper, we focus on prevention of authentication problems using quantum cryptography. Active attacks and passive attacks were the major problems in the process of authentication. Here we are using the quantum cryptography along with classical cryptography which enhances the overall security of the system. Polarization and photons are the key features of quantum cryptography. From the results we found that authentication problems were significantly reduced.

Keyword- Cryptography; Polarization; Photons; Quantum Cryptography.

I. INTRODUCTION

Cryptography is a technique used to transform the messages secretly. It provides secure communication between the adversaries. Classical cryptography uses simple mathematical methods to provide security and there is possibility for many attacks such as replay attacks, man in the middle attacks, and passive attacks. Quantum cryptography uses quantum mechanical properties to perform cryptography tasks. It solves replay and passive attacks, and also reduces the number of rounds for communication. In Chapter II we talk about literature survey and its problems. In Chapter III we discuss about security threats and its types. Proposed system and its advantages are illustrated in Chapter IV. Chapter V deals with performance analysis and we conclude in Chapter VI.

II. LITERATURE SURVEY

In [1], authors proposed that in large networks security is provided based on QKDP by relating classical cryptography and quantum cryptography. Their works include, securing replay and eavesdropping attacks. Effectiveness is enhanced in their proposed conventions by giving minimum number of rounds among Quantum Key Distribution (QKD).In [2] quantum cryptography to understand authentication strongly universal hash functions are studied. Vulnerabilities related to man-in-the-middle attacks are studied. Authentication lifetime is used to estimate the encrypted tags. This recommends crude measures like utilizing additional key for additional validation, diminishing data leakage, and changing secret hash function every now and again. Additionally investigate thoughts are given to utilize less key-consuming verification with solid security. In [3], as in [1, 4] authors focus on developing a secure model for huge networks. Here, they collaborate both classical cryptography and quantum cryptography. QKD framework with network design and services that provides security is discussed here. A session key is used to share the secret keys repeatedly for a long time. This model can resist from replay attacks and passive attacks effectively. In [5], as in classical cryptography the methods used currently are unsafe and liable to passive attacks, and these attacks can be solved by quantum cryptography. The combination of implicit and explicit QKDP are proposed by combining both classical cryptography and quantum cryptography to provide secured transmission between the participants. In [6], the idea of multi-server is recommended that clients are conveyed in parallel with numerous servers with the end goal of authentication. This presents a two server system that directly interacts to user and is visible to service server. In this, Classical Key Exchange (CKE) and QKD models are used. In [7], this project explains the basic principles of quantum cryptography and how these apply to QKD. In this BB84 protocol is explained in detail and compare to traditional cryptography system. Here two types of cryptographic algorithms are explained that is Symmetric key encryption and asymmetric key encryption. The above authors convey their knowledge on quantum cryptography and our project is designed to overcome the problems mentioned above.

III. SECURITY THREATS

Providing security is the primary goal of exchanging data. The concept of cryptography is evolved in order to provide secure communication between the host and the client, but as the technology growing everything is getting digitalized. Digital data is vulnerable to cyber attacks. In terms of exchanging data we have some attacks like Man-in-the-middle attack, Passive attack and Replay attack. In Man-in-the-middle Attack as the name suggests that the attacker secretly stoles the information and possibly alters the communication between two parties who believe that they directly communicate with each other, Where as in Passive attacks the purpose is solely to gain information about the target and no data is changed on the target. Sometimes it may possible for several vulnerabilities and in Replay attacks the valid data transmission is maliciously or fraudulently repeated or de1ayed.

A. Types of Attacks

- Man-in-the-middle attack
- Passive attack
- Replay attack

a. Man-in-the-middle Attack*:* As the name suggests that the attacker secretly stoles the information and possibly alters the communication between two parties who believe that they directly communicate with each other. The above is illustrated in the Fig 1.

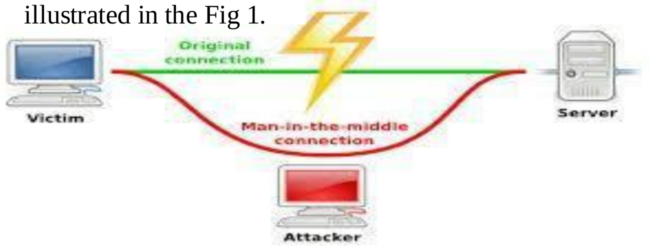

Fig.1: Man-in-the-middle Attack

b. Passive Attack: The purpose of this attack is solely to gain information about the target and no data is changed on the target. Sometimes it may possible for several vulnerabilities as shown in Fig 2.

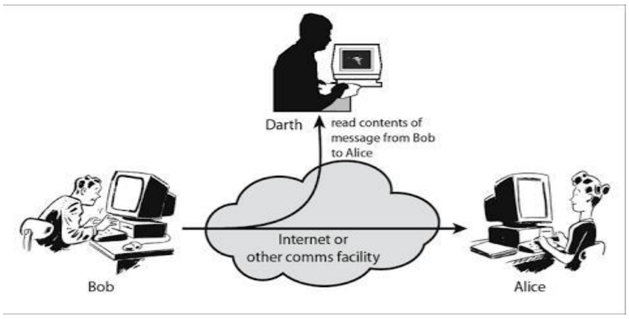
Darth
read contents of message from Bob to Alice
Internet or other comms facility
Bob
Alice

Fig.2: Passive Attack

c. Replay Attack: In this attack the valid data transmission is maliciously or fraudulently repeated or de1ayed as described in Fig 3.

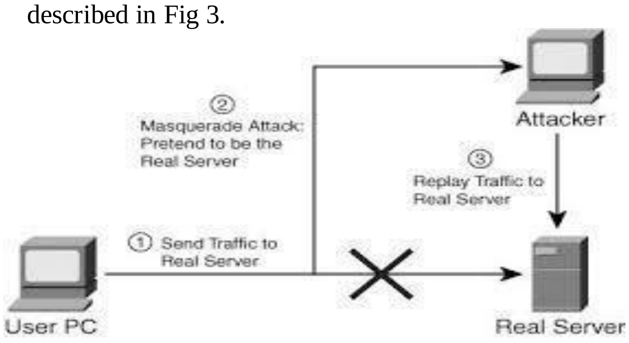
②
Masquerade Attack: Pretend to be the Real Server
Attacker
③
Replay Traffic to Real Server
① Send Traffic to Real Server
User PC
Real Server

Fig.3: Replay Attack

IV. PROPOSED SYSTEM

Quantum cryptography uses quantum mechanical properties to perform cryptography tasks. It solves replay and passive attacks, and also reduces the number of rounds for communication. In this, quantum mechanical properties like photons and polarization are used to provide security. The orientation of the photons is shown in the Fig 4.

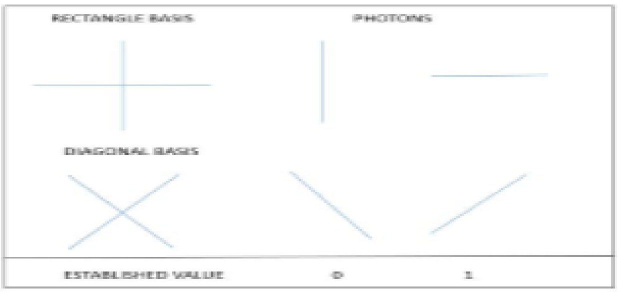

Fig.4: Photons and Polarization

In this integrated classical cryptography and quantum cryptography, the participant and trusted center agree their polarization by using pre-share secret key. These secret key with random string can be used to produce another encryption key to encode session key at the time of key distribution.

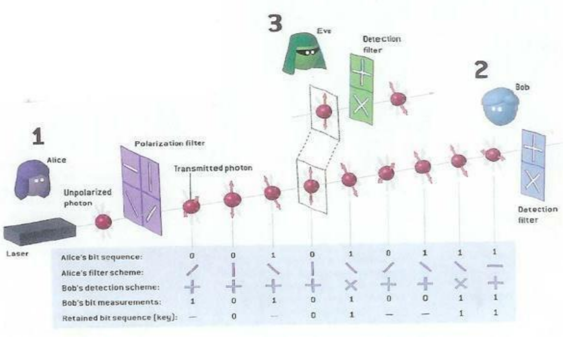

Fig.5: Quantum Key distribution

Even if session keys are transmitted the same polarization of qubits could not be received by the receiver. It presents implicit user authentication and explicit user authentication.

The implicit user authentication ensures that confidentiality is only possible to accepted user. After secure communication using session key, explicit user authentication is possible. Additionally digital signatures are added at explicit mutual authentication. The following describes the notation of the integration process. Presently, this project can be applied on .txt format files only. In future our project should be developed in such a way that it supports different formats in order to transfer files using Quantum Key Distribution Protocol (QKDP's). And the interface and user friendliness is not up to the mark in the current project. Usability with variety of formats and interface being enhanced will be in done in the coming future.

V. PERFORMANCE ANALYSIS

Integrating the classical and quantum cryptography by using three parties authenticated key distribution protocols to provide best security and authentication and to overcome the disadvantages of classical cryptography by using quantum cryptography. Sending data by providing hashing function, random number, key distribution and quantum key generation and by also generating session key and secret key.

VI. CONCLUSION

Using quantum cryptography authentication is provided and also reduced the large number of communication rounds. Quantum cryptography solves problem of large number of rounds for communication and secret-key distribution.

Proposed model is more effective as compared to other, particularly with digital signatures and quantum channels and it provides efficient key verification and user authentication.

VII. REFERENCES

[1]. Tzonelih Hwang, Kuo-Chang Lee, and Chuan-Ming Li, "Provably Secure Three-Party Authenticated Quantum Key Distribution Protocols", IEEE Transactions on Dependable and Secure Computing, pp. 71-80, Vol. 4, No. 1, March2007.

[2]. Aysajan Abidin, "Weaknesses of Authentication in Quantum Cryptography and Strongly Universal Hash Functions," Linköping studies in science and technology, 2010.

[3]. Tasleem et al., "Hybrid Approach: Combining Classical Cryptography and QKD for Password Authentication," International Journal of Computer Science & Communication Networks, Vol. 2, No. 4, pp. 512- 515 (55).

[4]. C. H. Bennett, "Quantum Cryptography Using any Two orthogonal States, "Physical Rev.Letters, vol.68,no. 3121, 1992.

[5]. Dr. G. Ananda Rao et al., "Three Party Authentication Key Distributed Protocols Using Implicit and Explicit Quantum Cryptography", Indian Journal of Computer Science and Engineering, pp.143-145, Vol. 2, No. 2, May 2011.

[6]. T. S. Thangavel and A. Krishnan, "Integrated Quantum and Classical Key Scheme for Two Servers Password Authentication," Journal of Computer Science, Vol. 6, No. 12, pp. 1396- 1405, 2010.

[7]. G.Li, "Efficient Network Authentication Protocols: Lower Bounds and Optimal Implementations," Distributed Computing, vol. 9, no. 3, pp. 131-145,1995.Computational Science and Its Applications (ICCSA'04), pp. 645-654,2004.