International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 04 Issue: 09 | Sept -2020 ISSN: 2582-3930

Three Party Authentication Key Distributed Protocols Using Implicit and Explicit Quantum Cryptography

[1] Mohamed Rashik.H, [2]Sabari Ramachandran. M, [3]Bala Subramanian. N, [4]Mohamed Rafi. M

[1]Final year MCA, Mohamed Sathak Engineering College, Kilakarai

[2]Assistant Professor, Dept of MCA, Mohamed Sathak Engineering College, Kilakarai

[3]Associate Professor, Dept of MCA, Mohamed Sathak Engineering College, Kilakarai

[4]Professor, HOD, Dept of MCA, Mohamed Sathak Engineering College, Kilakarai

ABSTRACT:

Since the beginning of time, there has always been a truffle between the code makers and the code breakers. Today, communicating mission-critical information in a secure way is more challenging than ever. The attacks can come from inside or outside the organization. They can target our infrastructure, our applications, or our financial assets. They can be launched by a spy from a foreign government, a hostile competitor, or a trusted business associate. Today, the war rages on, as organizations search for a way to ensure absolute security of high-value information exchanges. Quantum Key Distribution (QKD) solves key distribution and management problems that have been the bane of cryptographers for centuries. QKD offers the most secure cryptographic solution ever, providing protection from both internal and external threats.QKD is not meant to replace existing encryption technologies like Secure Socket Layer and the Public Key Infrastructure. Instead, QKD represents a new hybrid model which combines QKD and classical data encryption to deliver a more secure system. Customer ROI is based on the increase in overall system security. We have proposed a quantum key distribution system, QPN that solves these real-world security needs. In this white journal we present this as an example of a QKD system, that uses photon polarization to encode the qubits, to explain and provides a good overview.

1. INTRODUCTION

Computer networks are typically a shared resource used by many applications for many different purposes. Sometimes the data transmitted between application processes is confidential, and the applications would prefer that others be unable to read it. For example, when purchasing a product over the WWW (World Wide Web), users sometimes transmits their credit card numbers over the network. This is a dangerous thing to do since it is easy for a hacker to eavesdrop on the network and read all the packets that fly by. Therefore, users sometimes want to encrypt the messages they send, with the goal of keeping anyone who is eavesdropping on the channel from being able to read the contents of the message. The idea of encryption is simple enough. The sender applies an encryption functions to the original plain text message, the resulting cipher text message is sent over the network, and the receiver applies a reverse function known as the decryption to recover the original plain text.

The encryption/decryption process generally depends on a secret key shared between the sender and the receiver. When a suitable combination of a key and an encryption algorithm is used, it is sufficiently difficult for an eavesdropper to break the cipher text, and the sender and the receiver can rest assured that their communication is secure. The familiar use of cryptography is designed to ensure privacy-preventing the unauthorized release of information and privacy. It also is used to support other equally important services, including authentication (verifying the identity of the remote participant) and integrity (making sure that the message has not been altered).

In the Journal development concern, when they want to share the data with others, intruder may hack the data, intrude the data. To mitigate this problem, forwarded data and sender of the data will be audited. The sender submits the secret key to the trusted center (TC), then the TC will verify the secret key and Authenticate to the corresponding sender and gets the session key from TC, else TC doesn't allow the user Transmission. The message is encrypted by the received session key and appends the qubit with that encrypted message, then transmits the whole information to the corresponding receiver. Verify the secret key received from the user and authenticate the corresponding user for the secure transmission.

It is a shared secret key which is used to for encryption and decryption. The size of session key is 8 bits. This session key is generated from pseudo random prime number and exponential values of random number. To get the secret key and random string, then convert it into hex-code and then convert it into binary, find the least bit of the two binary values and get the quantum bit of 0

and 1. To generate the quantum key using the qubit and session key this depends on the qubit combinations,

It's a technique to encrypt the session key by using the master key and store all the values to TC storage. It distributes the original session key and qubit to the sender for encrypting the message. It also distributes the key and qubitto the corresponding receiver to decrypt the received messages. It receives the encrypted message with hashed session key and qubit, then verifies the qubit with TC and generates the master key and reverses the hash, the session key and also reverse hash the session key from sender then compare the session key which improve the key authentication. Then finally decrypt the message using session key and show it to the user.

2. PROBLEM DESCRIPTION

In classical cryptography, three-party key Distribution protocols utilize challenges Response mechanisms or timestamps to Prevent replay attacks.

Classic cryptography cannot detect the existence of passive Attacks such as eavesdropping. Identifies the security threads in the message, but not the security threads in the session key.

3. PLANNED DESIGN

Sender

a) Secret key Authentication

The sender submits the secret key to the trusted center (TC), then the TC will verify the secret key and Authenticate to the corresponding sender and gets the session key from TC, else TC doesn't allow the user Transmission.

b) Encryption

The message is encrypted by the received session key and appends the qubit with that encrypted message, then transmits the whole information to the corresponding receiver.

Trusted Center

Secret Key Verification

Verify the secret key received from the user and authenticate the corresponding user for the secure transmission.

a) Session Key Generation

It is a shared secret key which is used to for encryption and decryption. The size of session key is 8 bits. This session key is generated from pseudo random prime number and exponential values of random number.

Qubit Generation

To get the secret key and random string, then convert it into hex-code and then convert it into binary, find the least bit of the two binary values and get the quantum bit of 0 and 1. To generate the quantum key using the qubit and session key this depends on the qubit combinations,

i. If the value is 0 and 0, then $1/\sqrt{2}(p[0] + p[1])$.

ii. If the value is 1 and 0, then $1/\sqrt{2}(p[0] - p[1])$.

iii. If the value is 0 and 1, then p[0].

iv. If the value is 1 and 1, then p[1].

a)Hashing

It's a technique to encrypt the session key by using the master key and store all the values to TC storage.

b)Key Distribution

It distributes the original session key and qubit to the sender for encrypting the message. It also distribute the key and qubit to the corresponding receiver to decrypt the received messages

Receiver

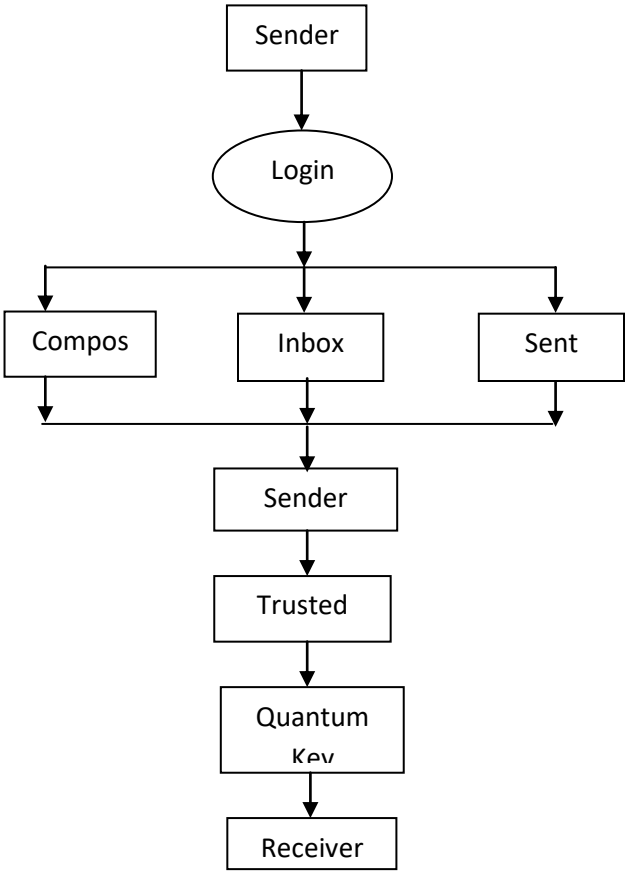
a) Secret key Authentication

It receives the encrypted message with hashed session key and qubit, then verifies the qubit with TC and generates the master key and reverses the hash, the session key and also reverse hash the session key from sender then compare the session key which improve the key authentication.

b)Decryption

Then finally decrypt the message using session key and show it to the user.

SYSTEM ARCHITECTURE



This work proposed quantum key distribution protocols (QKDPs) to safeguard security in large networks, ushering in new directions in classical and quantum cryptography. In quantum cryptography, quantum key distribution protocols (QKDPs) employ quantum mechanics to distribute session keys and public discussions to check for eavesdroppers and verify the correctness of a session key. By using Quantum Channel we can eliminate passive attacks like eavesdropping and therefore replay attacks. This in turn can be used to reduce communication rounds. Security against

such attacks as man-in-the-Middle, eavesdropping and replay,

* Efficiency is improved as the proposed Protocols contain the fewest number of Communication rounds among existing QKDPs,

* Two parties can share and use long-term Secret (repeatedly).

OPERATIONAL EXPENDITURE

We implement quantum key distribution protocols to safeguard security in large networks.

4. CONCLUSION

An Internet-based solution's feasibility is unquestionable as authorization can be provided for the secure access of information by asking the user for username and password and the ease of connecting a computer to the Internet makes the solution simple and efficient.

The user can send or receive message among the branches or camps. For the security purpose the senders message is encrypted and them stored in the appropriate users inbox. The receiver must decrypt it in order to read the original content of the message. The user can chat with members of the people. The primary goal of the system is to Provide the security to the users, the Security is provided by using Quantum mechanisms.

REFERENCES

[1] G.Li "Efficient network authentication protocols: Lower bounds and Optimal implementations", Distributed computing, Vol 9, No. 3 pp.1995.

[2] J.T.Kohi, "The evolution of the Kerberros Authentication Service" European conf. proc pp 295-313-1991. B.Nuemann and T. Ts'o "Kerberros" An authentication service for computer networks" IEEE comm., Vol 32, No.9 pp33-38 1994.

[3] W.Stallings, Cryptography and network security: principles and practice, prentice hall 2003.

[4] N. Linden, S. Popescu, B. Schumacher, and M. Westmoreland, "Reversibility of local transformations of multiparticle entanglement", quant-ph/9912039 W. Dür, J. I. Cirac, and R. Tarrach, "Separability and distillability of multiparticle quantum systems", Phys. Rev. Lett. 83, 3562 (1999)

[5] Ll. Masanes, R. Renner, M. Christandl, A. Winter, and J. Barrett, "Unconditional security of key distribution from causality constraints", quant-ph/0606049

[6] C. H. Bennett, G. Brassard, C. Crépeau, and M.-H. Skubiszewska, "Practical quantum oblivious transfer", Lecture Notes in Computer Science 576, 351 (1991)

[7] C. H. Bennett, P. W. Shor, J. A. Smolin, and A. V. Thapliyal, "Entanglement-assisted capacity of a quantum channel and the reverse Shannon theorem", Phys. Rev. Lett. 83, 3081 (1999)

[8] P. W. Shor, "Equivalence of additivity questions in quantum information theory", Commun. Math. Phys. 246, 453 (2004)

[9] M. B. Hastings, "A counterexample to additivity of minimum output entropy", Nature Physics 5, 255 (2009)

[10] Hammond, A., Citrano, A.: MagiQ Technologies Announces New., Next Generation Quantum Cryptography Solution. MagiQ Technologies, Inc. PR 617/ 661-8300 x201 617/ 758-4140 (March 28, 2005)

[11] Clifford Neuman, B., Ts‘o, T.: Kerberos: An Authentication Service for Computer Networks. IEEE Communications Magazine (September 1994) 0163-6804/94

[12] Blumenthal, D.J.: Photon Statistics and Basics of Propagation in Dielectric Media, ECE 228A (Fall 2007)

[13] Tompkins, F., Wolfe, P.J.: Bayesian filtering on the stiefel manifold. Harvard University

[14] García-Mata, G., Frahm, K.M.: Shor’s factorization algorithm with a single control qubit and imperfections, Université de Toulouse, France (December 12, 2008)

[15]Smith, G., Smolin, J.A.: Additive atson ©2008 IEEE.