Three-Party Authentication using Quantum Key Distribution Protocols

Kalamani P[1],Sujith nair.P[2], Kiran.J[3], Srinivas.D[4], Adithya prabhu[5]

[1]Assistant Professor, *Department of Computer Science & Engineering, Sri Sairam College of Engineering, Bengaluru.*

[2345]*UG Scholars, Department of Computer Science & Engineering, Sri Sairam College of Engineering, Bengaluru.*

ABSTRACT-- This project presents Quantum Key Distribution Protocols (QKDPs) to safeguard security in massive networks, by mistreatment DES algorithmic rule for secret writing and decryption of .txt file. In this project, secure communication between the sender and also the receiver is being created attainable through a trusted center by mistreatment secret key authentication. The trustworthy Center distributes a quantum key to each the sender and also the receiver when the verification of the secret key. The sender encrypts the info and sends to the receiver side solely when getting the quantum key from the Trusted Center. Similarly the decoding method happens. RSA algorithmic rule is getting used for quantum key distribution. and the input txt file is retrieved on the receiver aspect.

I INTRODUCTION

Authentication is the process which allows a sender and receiver of information to validate each other. If the sender and receiver of information cannot properly authenticate each other, there is no trust in the activities or information provided by either party. Authentication can involve highly complex and secure methods or can be very simple.

Various authentication methods like password, finger print, handprint, retina pattern, etc. are used. In this methodology, sometimes it will reject valid user and accepts invalid user. So people are not comfortable with these approaches.

The simplest form of authentication is the transmission of a shared password between entities wishing to authenticate each other. In classical cryptography, three-way key distribution protocols utilize challenge response mechanisms or timestamps to forestall replay attacks .However, challenge response mechanisms need at least 2 communication rounds between the TC and participants.

The timestamp approach desires the idea of clock synchronization that isn't sensible in distributed systems. Furthermore, classical cryptography cannot find the existence of passive attacks like eavesdropping.

II LITERATURE REVIEW

Different authentication techniques are used for communication. Nowadays, biometric authentication is popular. The advantages and disadvantages of various biometric authentication technique is discussed in [1].This paper addresses the actors affecting various authentication techniques[2].Graphical password authentication techniques are discussed in[3].To provide the efficient way of authentication, an integration of physical biometric approach is used. Minutiae mapping is introduced to extract the finger, iris and palm print and RC4, DWT algorithm for encryption and hiding the information[4].

In quantum cryptography, quantum key distribution protocols (QKDPs) use quantum mechanisms to distribute session keys and public discussions to test for eavesdroppers and verify the correctness of a session key.However, public discussions need extra communication rounds between a sender and receiver and price precious qubits. By contrast, classical cryptography provides convenient techniques that enable economical key verification and user authentication.

The advantages of each the classical and quantum cryptography are utilized within the projected QKDP. The advantages of proposed system are :a)Man within the middle attacks will be prevented, eavesdropping will be detected, and replay attacks will be avoided simply.b)User authentication and session key verification will be accomplished in one step while not public discussions between a sender and receiver.c)The secret key pre-shared by a TC and a user will be a long term

III METHODOLOGY

The proposed methodology using quantum key distribution protocols contains the following modules:

1. Sender Module.

2. Trusted Center Module and
3. Receiver Module.

A. *Sender Module*

This module has three sub-modules.They are,

1. Registration
2. Login
3. Send data

B. Trusted Center Module

- Secret Key Verification
- Session Key Generation
- Qubit Generation
- Quantum Key Generation

To generate the quantum key using the qubit and the session key which depends on the qubit combination such as,

1. If the value is 0 and 0, then 1/0.707(p[0]+p[1])

2. If the value is 1 and 0, then 1/0.707(p[0]-p[1])

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

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

- Key Distribution

C.Receiver Module

This module has three sub-modules. They are,

1. Registration
2. Login
3. Receive data

The Use case Diagram for Quantum key Generation is shown in fig 3.1. For Encryption & Decryption, DES(Data Encryption Standard) algorithm is used and for key generation RSA algorithm is used.

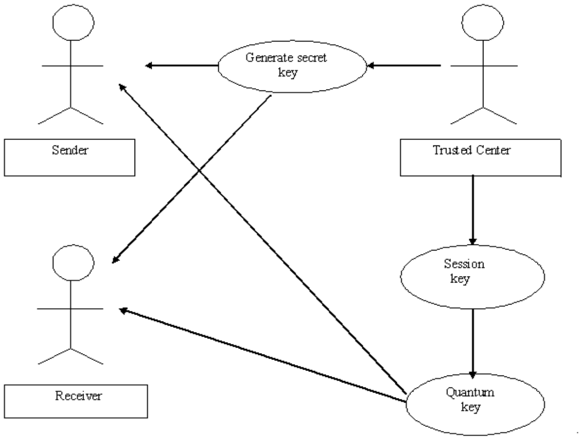


Figure 3.1: Use case Diagram – Quantum key Generation

DES algorithm:

The basic operations are DES Encryption. It includes

a)Initial permutation

b)Details of a single round

c)Sub-Key generation

DES Decryption uses the same procedure as encryption, except that the application of the Sub-Keys is reversed.

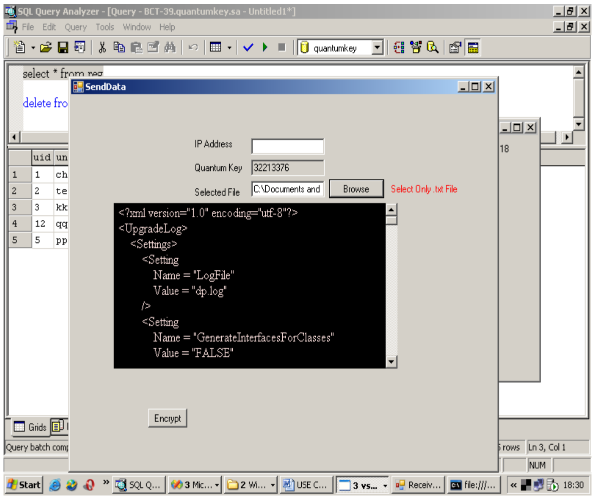
RSA algorithm:

Key Generation

1. Select p ,q where both p and q both prime, p≠q
2. Calculate n=p*q
3. Calculate Ø(n)=(p-1)(q-1)
4. Select integer e where gcd (Ø(n),e)=1; 1<e<Ø(n)
5. Calculate d where d= e^-1 mod Ø(n)
6. Public key KU={e ,n}
7. Private key KR={d ,n}

After the registration of sender and receiver esecret key is generation should be done.After that quantum key generation should be done

on both the sides.



uid	un
1	ch
2	te
3	kk
12	qq
5	pp

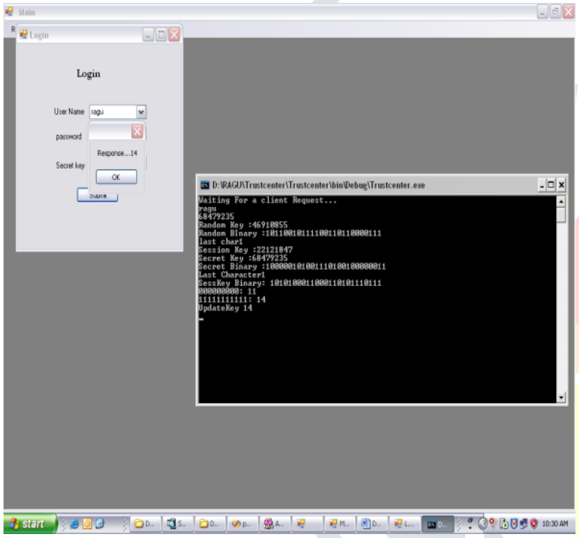
IP Address

Quantum Key 32213376

Selected File C:\Documents and Browse Select Only .txt File

```
<?xml version="1.0" encoding="utf-8"?>
<UpgradeLog>
  <Settings>
    <Setting
      Name = "LogFile"
      Value = "dp.log"
    />
    <Setting
      Name = "GenerateInterfacesForClasses"
      Value = "FALSE"
```

Fig 3.2: Quantum Key Generation (After both sender and receiver logged in)



User Name ragu

password

Secret key

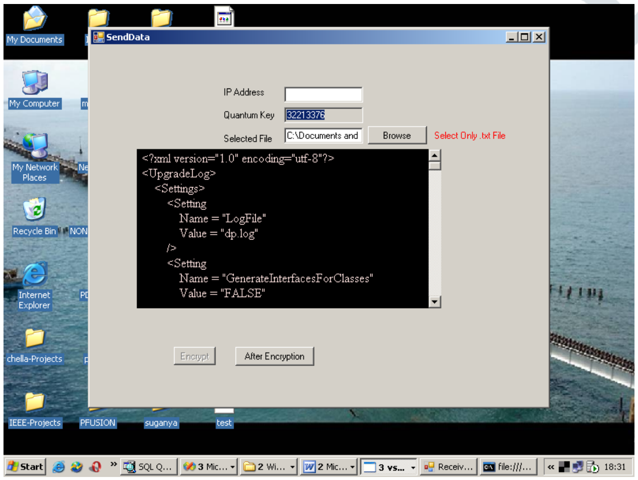
Response...14

D:\RAGU\Trustcenter\Trustcenter\bin\Debug\Trustcenter.exe

```
Waiting For a client Request...
ragu
68479235
Random Key :46910855
Random BInary :10110010111100110110000111
last char1
Session Key :22121847
Secret Key :68479235
Secret Binary :100000101001110100100000011
Last Character1
SessKey Binary: 1010100011000110101110111
000000000: 11
11111111111: 14
UpdateKey 14
_
```

Fig 3.3 Path name of the .txt file and the Ip address of the local system

Data to be Encrypted



IP Address

Quantum Key 32213376

Selected File C:\Documents and Browse Select Only .txt File

```
<?xml version="1.0" encoding="utf-8"?>
<UpgradeLog>
  <Settings>
    <Setting
      Name = "LogFile"
      Value = "dp.log"
    />
    <Setting
      Name = "GenerateInterfacesForClasses"
      Value = "FALSE"
```

Fig 3.4 Data to be Encrypted

IV CONCLUSION AND FUTURE ENHANCESMENT

Compared with classical three-party key distribution protocols, the proposed QKDPs easily resist replay and passive attacks. Compared with other QKDPs, the proposed schemes efficiently achieve key verification and user authentication and preserve a long-term secret key between the TC and each user. Additionally, the proposed QKDPs have fewer communication rounds than other protocols. By combining the advantages of classical cryptography with quantum cryptography, this work presents a new direction in designing QKDPs.The whole project can be enhanced for secure communication between two systems in a local area network through the trusted center which can be a third system in the local area network.

V REFERENCES

1. Bhattacharyya, Debnath & Ranjan, Rahul & Alisherov, Farkhod & Minkyu, Choi. (2009). Biometric Authentication: A Review. International Journal of u- and e- Service, Science and Technology.

2. K. Sharmila, V. Janaki and A. Nagaraju : A Survey on User Authentication Techniques", Orient. J. Comp. Sci. & Technol., Vol. 10(2), 513-519 (2017).

3. Sayli Chavan et al, International Journal of Computer Science and Mobile Computing, Vol.4 Issue.4, April- 2015, pg. 324-329.

4. Malathi.R, Jeberson Retna Raj.R, “An Integrated Approach of Physical Biometric Authentication System”,presented in International Conference on Computational Modeling and Security (CMS 2016) and published in Elsevier.

5. G. Li, “Efficient Network Authentication Protocols: Lower Bounds and Optimal Implementations,” Distributed Computing, vol. 9, no. 3, pp. 131-145, 1995.

6. M. Bellare and P. Rogaway, “Provably Secure Session Key Distribution: The Three Party Case,” Proc. 27th ACM Symp. Theory of Computing, pp. 57-66, 1995.