International Journal of Analytical, Experimental and Finite Element Analysis (IJAEFEA), Issue. 1, Vol. 6, March 2019
e-ISSN: 2394-5141, p-ISSN: 2394-5133, pp 12 - 15
DOI: 10.26706/IJAEFEA.1.6.20190304

An Efficient System for Transmission of Data over Network using QKD

Harshal Choukhe[1]
harshalchoukhe1234@gmail.com

Shitan Dhir[2]
shitan819@gmail.com

Mahesh Punde[3]
mkpunde95@gmail.com

Kanchan Kukde[4]
Kanchankukdej19@gmail.com

Kiran Birgodiya[5]
kiranbirgodiya@gmail.com

Ruchira Selote[6]
Ruchira1302@gmail.com

Suryodaya College of
Engineering and Technology,
Nagpur, India.

Abstract— **Most of the web based applications requires a security for the data. Providing security to the data is a process known as cryptography, which consists of encryption and decryption process. Most of the conventional cryptographic algorithms used in the environments of communication network, based on mathematical models and computational assumptions, are unsafe and apt by many attackers. Problems associated with private-key encryption process is, firstly it depends entirely on the secrecy of the key, secondly it requires two parties who initially shares no secret information to exchange a secret key and an eavesdropper can snoop secret key as it is being exchanged. In Public-key encryption there is no key distribution problem; however, security relies on unproven mathematical assumptions such as the difficulty in factoring large integers. To overcome above mentioned limitations associated with both approaches, we have designed an approach to augment private key encryption with quantum key distribution. Experimental results showed that proposed approach outperforms better than existing approaches.**

Index terms: *Ciphertext, Plaintext, AES, SHA, Quantum Key distribution (QKD)*

I. INTRODUCTION

Computation of Quantum depends on quantum physics for communication and quantum cryptography in order to securely transfer of the information between two parities. Two parties can generate a key with particular characteristics and make the use it for secure transfer of the information between them. Nowadays, user data gets highest priority in the field of data communication on internet. The data must be communicated securely so as to keep the internet usage reliable. For this security of data, several techniques have been introduced. Cryptography, water marking, steganography, etc. are the some popular techniques. Each of these techniques has some problems associated with them. In case of conventional cryptographic approach, the sender either uses the transposition cipher or substitution cipher. In recent years quantum cryptography has been the object of a strong activity and rapid progress [2] and now it is extending its activities into pre-competitive research and in commercial products. A classical cryptographer finds the Quantum Key Distribution (QKD) could be an interesting cryptographic primitive[3]. Identifying methodological and in details cryptographic implications of Quantum Key Distribution is complex task as it requires a combination of knowledge

That usually belongs to separate academic communities, ranging from classical cryptography to the foundations of quantum mechanics and network security [4].

A QKD system consists of a quantum channel and a classical channel. The quantum channel is only used to transmit qbits (single photons) and must consist of a transparent optical path (fiber, free-space and optical switches, no routers, amplifiers or copper). It is a lossy and probabilistic channel. The classical channel can be a conventional IP channel (not necessarily optical), but depending on system design it may need to be dedicated and closely tied to the quantum channel for timing requirements.

Quantum key distribution (QKD), a novel cryptographic technique for secure distribution of secret keys between two parties (traditionally named Alice and Bob), is the first successful quantum technology to emerge from quantum information science. QKD employs quantum states to encode and transmit secure key bits. The security of QKD is guaranteed by fundamental properties of quantum mechanical systems. Intuitively, any intermediate measurement of a quantum state disturbs that state.

II. OBJECTIVES AND PROBLEM DEHFINATION

Problems associated with private-key encryption process is, firstly it depends entirely on the secrecy of the key, secondly it requires two parties who initially shares no secret information to exchange a secret key and an eavesdropper can passively snoop secret key as it's being exchanged. In Public-key encryption there is no key distribution problem; however, security relies on unproven mathematical assumptions such as the difficulty in factoring large integers. To overcome above mentioned limitations associated with both approaches. We have proposed an approach to augment private key encryption with quantum key distribution.

The proposed protocol takes advantage of the current public key cryptography protocols and the physical features of the quantum channels. It provides authentication and confidentiality.

The main purpose of the proposed protocol is to ensure that a secret key is delivered to the communicating parties in a secure manner. It eliminates the inefficiency introduced by preceding quantum key distribution protocols, which requires that the sender and the receiver communicate over the quantum channel for many rounds just to agree on a basis for the quantum communication, up to 20 rounds in the protocol proposed.

Authentication mechanism is provided using SHA-1 algorithm. SHA-1 is nothing but the cryptographic algorithm. It delivers authentication as well as data integrity. This algorithm is works for a message of size < 264 bits. And it creates a 160-bit (20 byte) output message. SHA-1 or Secure Hash Algorithm 1 is a cryptographic hash function which takes an input and produces a 160-bit (20-byte) hash value. We have been able to eliminate this by having the user who's requesting the communication session to generate a random basis, a random nonce, and to send it to the receiver over a classical channel.

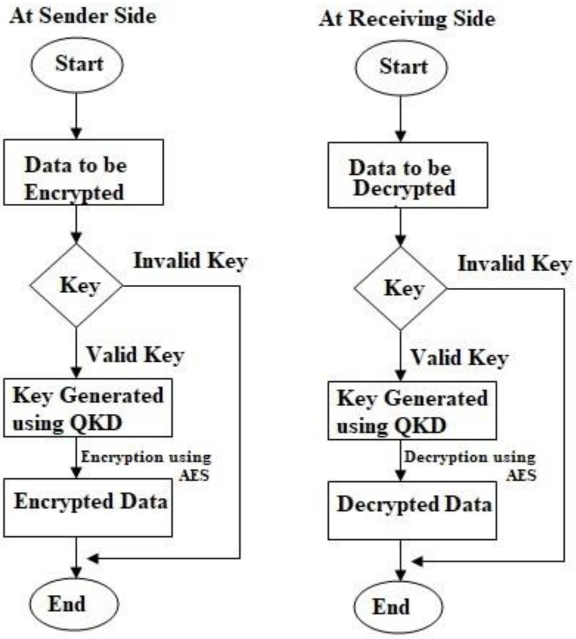


Figure 1.Data Flow Diagram for Encryption and Decryption process.

User want to send data to others, user needs to go through the AES encryption process. At destination end, user needs to decrypt the data with same algorithm.

AES is a symmetric key algorithm. Therefore it refers similar key for both encryption and decryption procedure. It operates on fixed size of data i.e. 128 bits. But, in AES key sizes are varying i.e. 128, 192 and 256 bit which is depends on how many rounds are cover under AES. The data is delivered through N stages for encryption. And these stages are shuffle as per the key size. Fort 10 stages key size is 128 bit. If the stages are 12 and 14 then key sizes are 192 and 256 separately.

The receiver, let consider Bob, should be able to verify that the message is indeed from sender consider Alice because he can decrypt it using Alice's private key

PRAlice. He should be confident that the message is secured because it’s encrypted using his public key *PUBob* and could only be decrypted using his private key *PRBob*, which no one knows but him.

When Alice receives the session key generated, *KSession*, by Bob she receives it over the quantum channel encoded using the random basis she has generated earlier at the beginning of the session. She received the original Nonce that she has also created along with the random basis. She should be confident that the session key *KSession* has been generated by Bob because it has the Nonce she sent to Bob earlier.

III. Proposed Methodology

Following figure shows block diagram of proposed work. The operation of this algorithm begins with the reading an input data (original data) from user that needs to be encrypted send or validated. The user can enter the data of any kind. Then process of Encryption is applied on the data. Once data is encrypted it is send over the network to the receiver. Receivers then decrypt the data according to QKD approach.

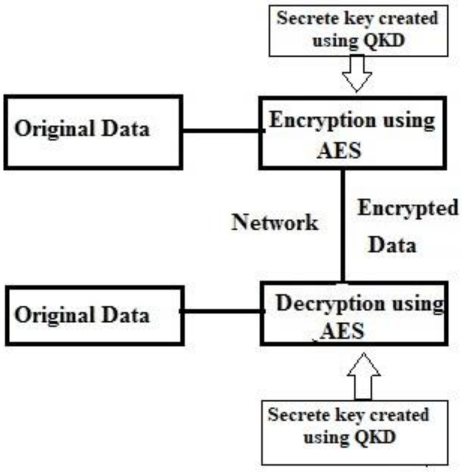


Figure 2. Block diagram of proposed methodology.

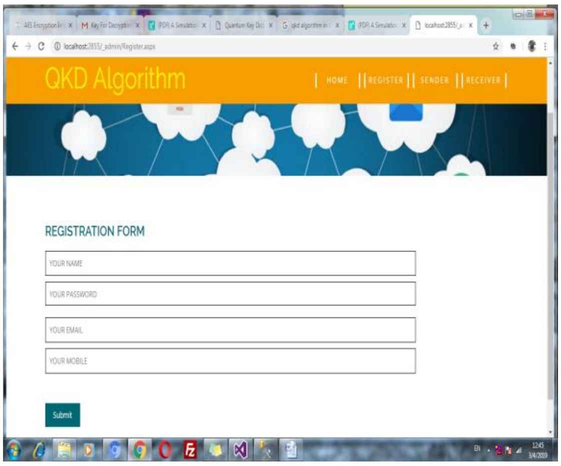
IV. Implementation

This is homepage for the project. It consist of registration, sender login and receiver login menus.

Next step is registration process. User needs to register by submitting necessary credentials. Once user completed with registration process, user can login to the proposed system.

QKD Algorithm
| HOME || REGISTER || SENDER || RECEIVER |
Transmission Of Data Over Network
With QKD Algorithm

Figure 3: Homepage of the project.



REGISTRATION FORM

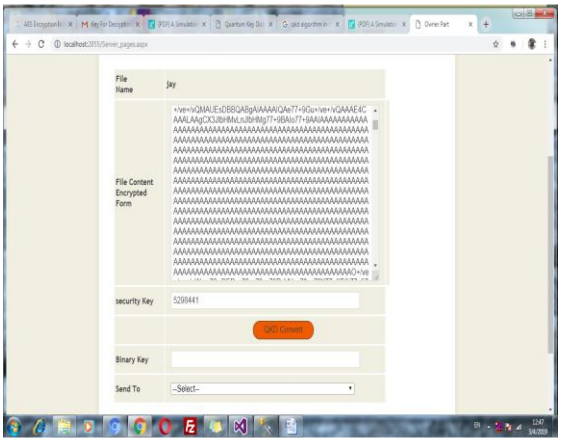
YOUR NAME

YOUR PASSWORD

YOUR EMAIL

YOUR MOBILE

Figure 4: Registration Process

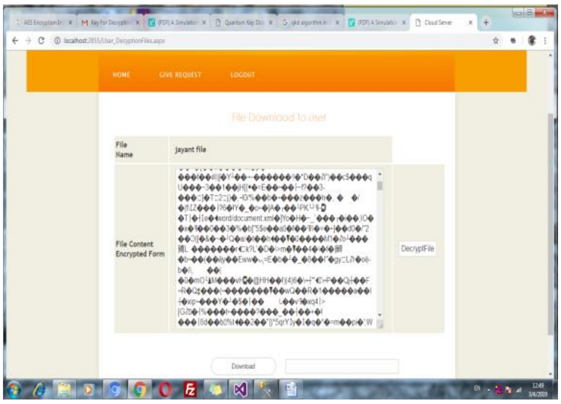


File Name	jay
File Content Encrypted Form	+/ve+/vQMAUEsDBBQABgAIAAAAIQAe77+9Gu+/ve+/vQAAAE4C AAALAAgCX3JlbHMvLnJlbHMg77+9BAIo77+9AAIAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAO+/ve
security Key	5298441
Binary Key	
Send To	--Select--

Figure 5: Encryption Process

Once user logged in to the system, user can proceed with encryption process with auto generated secret key using QKD.

At destination end user needs to decrypt the data using same secret key.



localhost:2855/User_DecryptionFiles.aspx

File Download to user

File Name	jayant file
File Content Encrypted Form	[illegible]

Figure 6: Decryption Process

V. Conclusions

We have proposed a quantum key distribution protocol that takes advantages of the strength provided by quantum channels. The proposed protocol also takes advantages of the public key cryptography. This protocol eliminates the unwanted redundancy introduced in previous protocols. Experimental results showed that proposed approach outperforms better than previously available algorithms.

The future work will focus on integrating a new kind of quantum memory that overcomes the limited storage time. The possibilities of transmitting confidential information securely and without fear of interception or interference could open up a realm of new possibilities.

References

[1] Mikio Fujiwara, Tomoyasu Domeki, Shiho Moriai, and Masahide Sasaki, *"Highly Secure Network Switches with Quantum Key Distribution Systems"*, International Journal of Network Security, Vol.17, No.1, PP.34–39, Jan. 2015.

[2] C. Elliott, A. Colvin, D. Pearson, O. Pikalo, J. Schlafer, , and H. Yeh, *"Current status of the DARPA quantum network,"* in Quantum Information and Computation III, pp. 138–149. SPIE, 2005.

[3] Sanchez-Avilaf&R. Sanchez-Reillot,TheRijndael Block Cipher (AES Proposal): A Comparison with DES, Universidad Politecnica de Madrid, 28040 Madrid, Spain.

[4] TianqiZhou,JianShen ,XiongLi,Chen Wang and Jun Shen,"*Quantum Cryptography for the Future Internet andthe Security Analysis"*Chinese Academy of Sciences, Beijing, China3Hunan University of Science and Technology, Xiangtan,China.

[5] J. Aditya, P. Shankar Rao," *Quantum Cryptography"* Dept of CSE, Andhra University,AndraPradesh,India.

[6] Richard J. Hughes,D. M. Alde, P. Dyer, G. G. Luther, G. L. Morgan and M. Schauer,"*Quantum Cryptography*" University of California Physics Division Los Alamos National Laboratory Los Alamos, NM 87545,USA.

[7] Mart Haitjema,"*A Survey of the Prominent Quantum Key Distribution Protocols*"University of Washington,USA.

[8] Alan Mink, Sheila Frankel and Ray Perlner*," Quantum Key Distribution (QKD) andCommodity Security Protocols: Introduction and Integration*"National Institute of Standards and Technology (NIST),100 Bureau Dr., Gaithersburg, MD 20899.

[9] R. D. Sharma and A. De, *"A new secure model for quantum key distribution protocol,"* in Industrial and Information Systems (ICIIS), 2011 6th IEEE International Conference on. IEEE, 2011, pp. 462–466.

[10] N. S. Yanofsky and M. A. Mannucci, Quantum computing for computer scientists. Cambridge University Press Cambridge, 2008, vol. 20.

[11] M. D. H. Kulkarni, *"Research directions in quantum cryptography and quantum key distribution,"* International Journal of Scientific and Research Publications, vol. 2, no. 6, June 2012.