A Novel Scheme for Data Security in Cloud Computing using Quantum Cryptography

Geeta Sharma
Department of Computer Science and Engineering
Guru Nanak Dev University, Regional Campus
Jalandhar, Punjab, India
gsharma3210@gmail.com

Sheetal Kalra
Department of Computer Science and Engineering
Guru Nanak Dev University, Regional Campus
Jalandhar, Punjab, India
sheetal.kalra@gmail.com

ABSTRACT
Cloud computing manifests exceptional capacity to facilitate easy to manage, cost effective, flexible and powerful resources across the internet. Due to maximum and shared utilization of utilization of resources, cloud computing enhances the capabilities of resources. There is a dire need for data security in the wake of the increasing capabilities of attackers and high magnitude of sensitive data. Cryptography is employed to ensure secrecy and authentication of data. Conventional information assurance methods are facing increasing technological advances such as radical developments in mathematics, potential to perform big computations and the prospects of wide-ranging quantum computations. Quantum cryptography is a promising solution towards absolute security in cryptosystems. This paper proposes integration of Advanced Encryption Standard (AES) algorithm with quantum cryptography. The proposed scheme is robust and meets essential security requirements. The simulation results show that the Quantum AES produces complex keys which are hard to predict by adversaries than the keys generated by the AES itself.

Keywords
AES; Cryptography; Quantum Key Distribution; Symmetric Algorithm;

1. INTRODUCTION
Cloud computing is a substantial transition from classical computing that believes in dispensing of resources than having personal devices [1]. It dispenses data to user in a cost effective and flexible manner. The sharing of resources, incorporates software, hardware and storage. Cloud computing provides several services such as PaaS, SaaS, IaaS, MaaS, SecaaS [2]. Cloud computing proliferates the abilities of the hardware resources by sharing and optimal application. With the vast growth of internet and network applications, the amount of data being shared and dependence on these communication channels has expanded manifold. Thus, the need for data security is stronger than ever.

AICTC '16, August 12-13, 2016, Bikaner, India
© 2016 ACM. ISBN 978-1-4503-4213-1/16/08…$15.00
DOI: http://dx.doi.org/10.1145/2979779.2979816

As the data owner has no actual control of data in cloud computing, cryptography is the best way to secure sensitive data. Cryptography is a study of techniques to securely transmit data in the absence of a secure channel. Classical encryption techniques have certain inherent weaknesses in terms of security [3, 4]. To achieve data secrecy, several encryption techniques are extensively used. Asymmetric encryption algorithms are much slower than symmetric encryption algorithms as they demand more computational processing power [5]. The growth of quantum cryptography was propounded by the flaws of conventional cryptography classified as one-time pad systems, public key and private key systems [6]. With the improvement in computational power, classical cryptography and key management techniques based on computational complexity are rendered vulnerable to brute force, hacking and cryptanalytic attacks. It is for this reason that efforts have been made for more than a decade to establish a new basis for cryptography science in communication networks. These efforts have resulted in the emergence of quantum cryptography technology. The security of quantum cryptography is built on the uncertainty in quantum phenomenon. Quantum cryptography is the only means of providing secure communication regardless of computational power. Quantum Key Distribution (QKD) depicts one of the most notable practical applications of quantum information theory.
The concept of quantum cryptography is not to replace the existing cryptography, but instead it gives room for a more secure transfer of keys which are used in the process of encoding and decoding. It necessitates that the strategies must be evolved to generate a practical quantum cryptosystem which would enhance the speed of cryptographic communication. The paper proposes a scheme that ensures balancing speed and security by the means of integrating quantum with classical cryptography methods. QKD ensures tremendous security advantages as compared to the classical key distribution. Firstly, warranted by the laws of quantum mechanics, an intruder cannot imitate the qubits in transmission. Secondly, computational efficiency does not ease the task of an eavesdropper as a key generated using QKD process is unconditionally safe. Thirdly, in contrast to traditional key distribution schemes that relies on computational complexity to secure the key, QKD employs inherent properties of quantum mechanics to achieve security. Fourthly, property of QKD permits communicating parties to detect if there is an eavesdropper observing the transmission.

The paper is arranged as follows. Limitations of classical cryptography have been discussed in section 2 of the paper. In section 3, preliminaries of quantum key distribution have been discussed. In section 4, related work in the field of symmetric key cryptography has been discussed. In section 5, a novel scheme integrating AES with QKD has been proposed. In section 6,

experimental results of the proposed scheme have been shown. Finally, section 7 concludes the paper.

2. LIMITATIONS OF CLASSICAL CRYPTOGRAPHY

Classical cryptography relies on achieving security through computational complexity. It employs one way mathematical operations, which makes the reverse process of revealing encrypted data nearly an impossible job. If an intruder has unconditional computational power, then classical cryptography cannot protect data. Classical cryptography has the following limitations:

a) Key distribution problem: Classical cryptography does not provide any means to communicate the key securely. It is impossible to send key using physical medium as it is impractical. Additionally, it is not possible to verify whether the key was intercepted and its contents were copied by an adversary. Public key encryption emerged as a solution to the problem, but these encryption algorithms cannot be employed to encrypt data of large size and are too slow.

b) Growth in computing technology: With the emergence of quantum computers that can perform operations and calculations at a speed that no current technology could possibly achieve. The encrypted code that would take a trillion years to break conventional computers could be cracked in much less time. As the keys can be cracked easily, encryption algorithms are of no use as they can be readily decrypted once the key is compromised.

c) Eavesdropping: The act of capturing packets from the network, which are transmitted by other entities and getting unauthorized access to sensitive information such as password or any confidential information is known as eavesdropping. In classical cryptography, the sender and the receiver of information will have absolutely no idea that they are being hacked. These limitations could be easily tackled by switching over to quantum cryptography. Specifically, man-in-the-middle attack might be dangerous in transmitting sensitive information. QKD uses the source of light to operate in a linear and circular polarization. If an eavesdropper tries to intercept light particle, light signals will be destroyed

d) Authentication: Classical cryptography provides no mechanism to verify the integrity of the message. Quantum cryptography ensures that no eavesdropper can observe the qubits without introducing disturbance which would be detected. As all eavesdropping could be detected, quantum cryptography is considered more secure mean for distributing key.

3. PRELIMINARIES OF QUANTUM KEY DISTRIBUTION

Quantum cryptography ensures secure communication between two parties across optical networks. The Heisenberg uncertainty principle states that information being transmitted on the quantum channel could be spied only by measuring it, which introduces a disturbance in the system. The quantum state cannot be measured without disturbing it. In quantum cryptography, there are two channels: an optical channel and a public channel. Optical channel transmits photons between communicating parties. Public channel is employed to discuss the basis of photons. Light emitted from a light emitting source from the sender will pass either through diagonal or vertical polarizer. If vertical polarizer photon movement is in 90º then bit value becomes 1 and if photon movement is in 0º, then bit value will be 0. In case of diagonal polarizer photon movement is in 45º bit value will be 1 and if photon movement is in 135º bit value becomes 0. Light waves are propagated as discrete quanta called photons. Photons are given angular momentum known as spin. A spin carries the polarization photon may or may not pass through the polarizer using a detector. On the receiver side also having polarizer and it polarizes the photon. If both the sender and receiver entities are using same polarizer, then match occurred and that bit value becomes one of the bits of the key. The following steps show encoding process in BB84.

Step 1. Sender produces photons by randomly choosing among 0◦, 45◦, 90◦ and 135◦ angles and sends them in a sequence using quantum channel. He records 0 for 0◦ or 45◦ photon and 1 for 90◦ or 135◦. The random sequence is formed using H, V, D, A denoting horizontal, vertical, 45◦ and 135◦ respectively. Thus, sequences becomes as:

x++x+xx+x++++x+x++xxxx++x++++xx+xx+++x++x++++xx...
VVVHAVAAVAHVHDDVDDHHAAAVHDHVVDVDADVD
AAHVDHHHVA...
1110111110100001000111100011010101011010100011...

Step 2. The receiver has a rectangular analyzer and a diagonal analyzer. The receiver chooses random analyzer to measure the photons and records analyzer employed along with the measurement of the photon. He records 0 for 0◦ or 45◦ photon and 1 for 90◦ or 135◦. Randomly applying analyzers, sequences thus, becomes as:0

xxx++xx+++x+++xxxx++x++xxx+++x+xxxxxx++xx...
DVAHADAAVVHDHHDHAVDAHHVHVHVDDADHVVDV
AAADADHHDH...
0110101111000000110101001010100100111011110100000

Step 3. Both parties transmit photons using public channel. They discuss basis used to measure the photons.

Sender to receiver:
xx ++x+xxxx++xx+++xxx++xx++xx++x+xx...
Receiver to sender:
xxx+++x+++xx++++x++xxx++x+++x+...

Step 4. Now, both parties distill key by dropping photons in following case: (i) If the receiver detects no polarized photon. (ii) If there is dissimilarity in basis used by sender and analyzer used by the receiver. Now, they have arbitrary sequence 0's and 1's which is opted as a secret key:

Sender: 1100110011101000101001110001110001111011011
xxx+x++xx+x++xxx++xx+++xx++++xxx+x+x+++...
Receiver: xxx+xxxx+++x++x+x+++xx+++xx++++x+++x+xxxx
1110001101001100000101001110101111011010011
Hence, the refined key is 101111000001100100101. If there is no failure in detection, the length of the keys will be halved of the length of sequences taken at the beginning.

4. RELATED WORK

Advanced Encryption Standard (AES) and Data Encryption Standard (DES) are widely employed symmetric algorithms to achieve secrecy of the data. Mandal et al. [7] analyzed AES and DES to verify the accuracy of performance based on time taken, level of encryption and memory consumed.

In Subasree and Sakthivel [8], presents security algorithm architecture. The algorithm employs ECC, MD5, and RSA but has certain weaknesses. Firstly, the information is encrypted using asymmetric algorithms which are much slower than symmetric

algorithms. Secondly, if an eavesdropper is able to reveal private key, the whole messages can be read.

In Dubal et al. [9] security algorithm architecture, data is encrypted with a key generated by ECDH. From the previous studies, it is clear that the security algorithms that depend on asymmetric encryption algorithms such as [8] and [9] have critical weak points as they are slow when compared to symmetric algorithms and takes large power to encrypt all plaintext by public key.

In Zhu [10], a hybrid algorithm architecture is purposed. The message is encrypted with symmetric algorithm and the key and digital signature belonged to symmetric encryption are encrypted with asymmetric key algorithm. The algorithm suffers from a low security level because the message is encrypted in a single phase which leads to low complexity.

5. PROPOSED SCHEME

Several schemes are being proposed which provide data security, but integrating QKD with classical cryptography is a novel scheme and guarantees high security. This combination of QKD protocols, and classical cryptography is computationally inexpensive. QKD can be used to provide absolute security to the sender and the receiver. The user can achieve both absolute as well as practical security. To achieve absolute security, one-time pad algorithm is integrated with QKD. It achieves unconditional security for highly confidential messages. But to achieve faster and practical security, the symmetric key is integrated with QKD. Symmetric key cryptography algorithms require lesser execution time. As a consequence, these algorithms are commonly used for long messages. AES is the fastest block cipher and is selected for practical security.

5.1. Achieving absolute security

One-time pad [11] was purposed by Gilbert Vernam in 1917. One-time pad ensures perfect secrecy and is not breakable because of the two reasons. Firstly, the encryption key is a random number and secondly, the key is used exactly once. The scheme is also more attractive as it is easy to encrypt and decrypt. It generates ciphertext C using operation C=P $\oplus$ K, where P is plaintext, K is key and $\oplus$ is XOR operation.

Information-theoretic security can only be proved using one-time pad encryption scheme. Therefore, it is obvious to integrate the one-time pad scheme with QKD. This integration provides high security. In this perspective, integrating one-time pad with QKD gives an empirical solution for transmitting data securely. Long term security is required in several applications such as securing a medical database, government or high intensity strategic and defense records, industrial data protection [12].

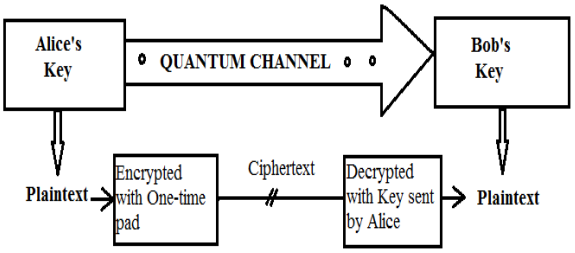

Figure 1. Integrating one-time pad with quantum cryptography

Figure 1 shows how quantum cryptography can be used to send an encrypted message using one-time pad encryption technique. It performs operations such as XOR, binary addition on the plaintext with the key to construct the encrypted message. A similar addition of the encrypted message and the key at the receiver's side decrypts the original message or plaintext. But one-time pad ensures secrecy of data with certain probability.

5.1.1. Limitations of one-time pad

Although one-time pad achieves the high security, it has certain limitations also. These limitations restrict the area of application of one-time pad.

a) The length of the key used in this scheme must be of the same length as the plaintext. Hence, in one-time pad, the rate of communication will be the same as the key-sharing rate.

b) The key should never be reused. It should be used just for once. Thus, drives name one-time pad. Consider two messages m_1, m_2 which are encrypted using the same key K. Ciphertexts generated as:

$Ct_1 = m_1 \oplus K$

$Ct_2 = m_2 \oplus K$

Ct_1, Ct_2 are transmitted. An intruder can simply take addition modulus 2 of generated ciphertexts Ct_1 , Ct_2 to get hint i.e. non-trivial information.

$Ct_1 \oplus Ct_2 = (m_1 \oplus K) \oplus (m_2 \oplus K)$

$Ct_1 \oplus Ct_2 = (m_1 \oplus m_2)$

c) One- time pad suits for shorter messages only. As the length of the key should be of the same length as of plaintext, this will surely reduce the efficiency of the system.

But for absolute security, these limitations are of no concern as quantum cryptography can effectively distribute sufficient material to make the one time pad feasible for short, but highly confidential messages.

5.2. Achieving practical security

One-time pad is very slow method and may not fit into applications where transmission speed is the highest priority. In applications where transmission speed is not to be compromised and only generated key need to be sent with absolute security, a combination of quantum cryptography with symmetric key encryption will be of choice. AES is a block cipher symmetric algorithm developed by NIST in 1977 and supersedes DES. In purposed scheme, AES is employed. Table 1 shows different parameters of AES. For faster execution of encryption, AES algorithm is used with key size of 128 bits as increase in key size will directly increase encryption or decryption time.

Table 1. AES parameters

Key Size(in bits)	Rounds	Cipher Type
128	10	Block
198	12	Block
256	14	Block

Figure 2 depicts the architecture of quantum cryptography integrated with symmetric key algorithm. Private keys are sent using a stream of photons. Key is encoded in each photon and is represented by either 0 or 1. The key can be encoded into either the relative phase of the photon or the polarization. Quantum Key Distribution (QKD) protocols like BB84 is used to transfer secret key between users.

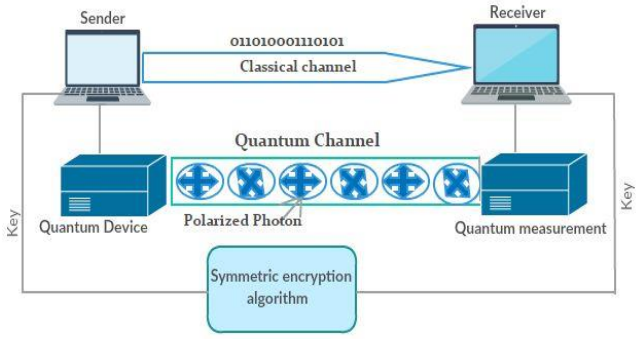

Figure 2. Architecture of quantum cryptography integrated with symmetric key algorithm

5.2.1. Integration methodology for symmetric key algorithm

To be more specific several modes can be specified. These are: dynamic key changing mode and fixed key mode. (i) In dynamic key changing mode, key is updated every time when a quantum cryptosystem generates a key of the same length. A fresh key is generated and used for encryption/decryption process and it is used only once for every data file. Figure 3 shows flowchart of dynamic key changing mode. (ii) Unlike dynamic key changing mode, the shared key is fixed for a certain length of time. A timestamp is fixed and fixed key is used again until the timestamp expires. Flowchart of fixed key mode is shown in Figure 4.

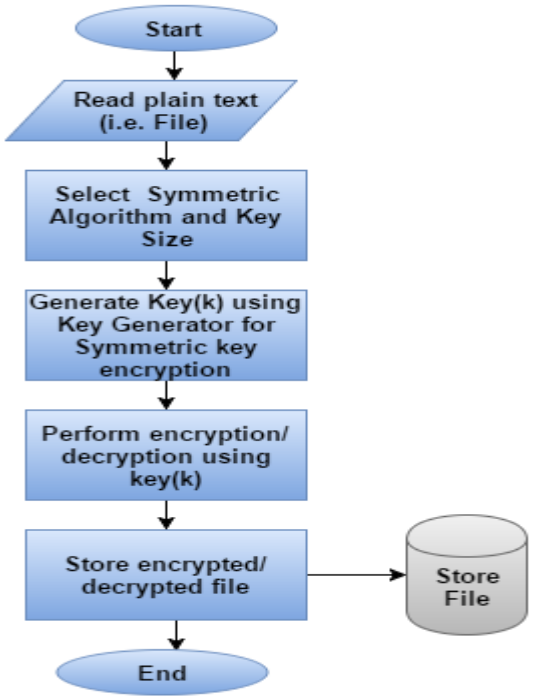

Figure 3. Flowchart of dynamic key mode

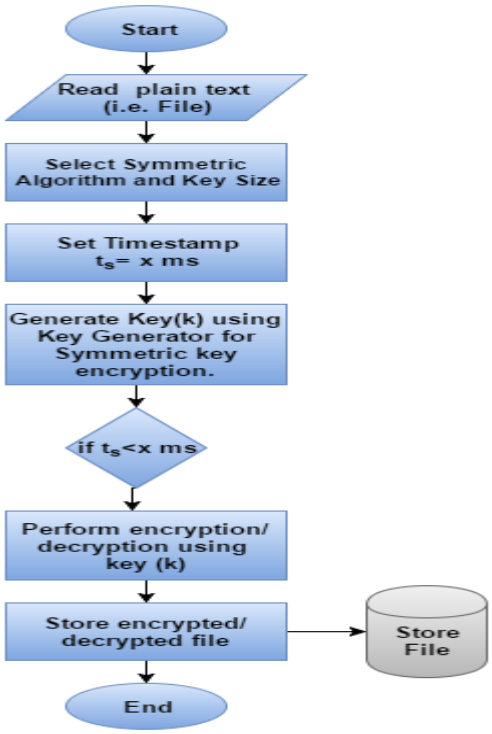

Figure 4. Flowchart of fixed key changing mode

5.2.2. Quantum AES architecture

The Quantum AES integrates AES with QKD to achieve high security for cloud computing environment [13]. The enhanced version of AES, i.e. Quantum AES employs the key generated by QKD to encrypt and decrypt data as shown in Figure 5. As QKD works on Heisenberg uncertainty principle rather than the complicated mathematical computations for developing the key, the cipher is resistant to any attack and hard to be cracked [14] [15].

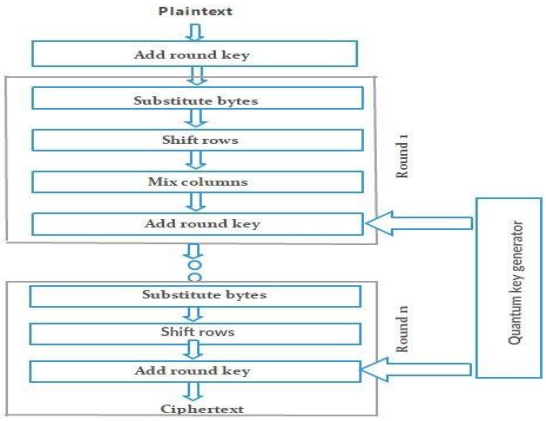

Figure 5. Quantum AES round

The steps to integrate the AES with quantum cryptography are as follows:

Step1: Key (k) generated by quantum key generator is sent through a quantum channel using BB84 protocol.

Step2: Receiver measures bits received from the quantum channel with his own selected bases. Receiver announces the bases to sender via public channels to verify the compatibility of the generated key.

Step3: For practical security, key length of 128 bits is selected for the encryption process.

Step4: Final key k_q is used to encrypt or decrypt data using AES.

Step5: Encrypt the first block of input data D_1-128bits using k_{q_1} which is generated by QKD round r_1.

$$E(D_1 \oplus k_{q_1}) = M_1$$

Step6: Similarly, encrypt the rest of blocks of input data by stages using k_{q_n} key which is generated using QKD round r_n where n can take value 10, 12, 14.

$$E(D_1 \oplus k_{q_n}) = M_n$$

Step7: As a receiver decrypts the encrypted message using following procedure.

$$D(M_n \oplus k_{q_n}) = D_n$$

6. EXPERIMENTAL RESULTS

In this section, the symmetric key algorithm AES and the purposed Quantum AES have been implemented for different key sizes. The experiment is performed on Core i7 (4.20GHz). Figure 6 shows the running time of the AES. AES is given with different sizes of input files and running time is measured in milliseconds.

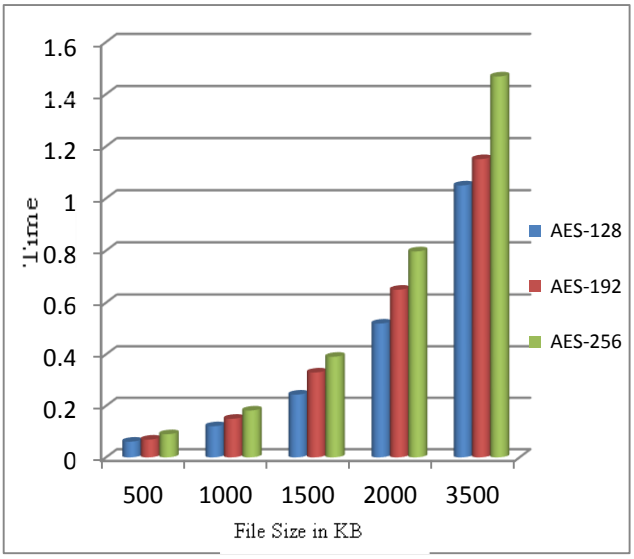

Figure 6. Running time for AES

From result, it is evident that increase in the size of file results in increase in time to encrypt that file. Conclusions drawn from the implementation are (i) AES is implemented easily. (ii) Running time increases with increase in input file size.

Figure 7 shows the running time of the Quantum AES. The size of input files given to Quantum AES is taken as 500kb, 1000kb, 1500kb, 2000kb, and 3500kb and running time is measured in milliseconds. When compared with classical AES, Quantum AES shows a higher degree of security.

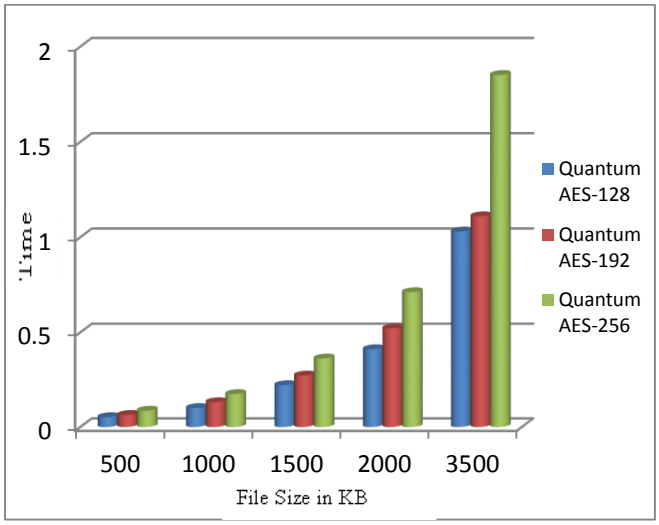

Figure 7. Running time for Quantum AES without key generation time

6.1. Comparative analysis

Figure 8 shows results of run time analysis of the AES and Quantum AES for different key sizes. Figure 9 represents the running time of symmetric key algorithms and the proposed scheme. It is evident from Figure 9 that Quantum AES is more efficient than other encryption algorithms such as AES, DES, 3DES and RC4.

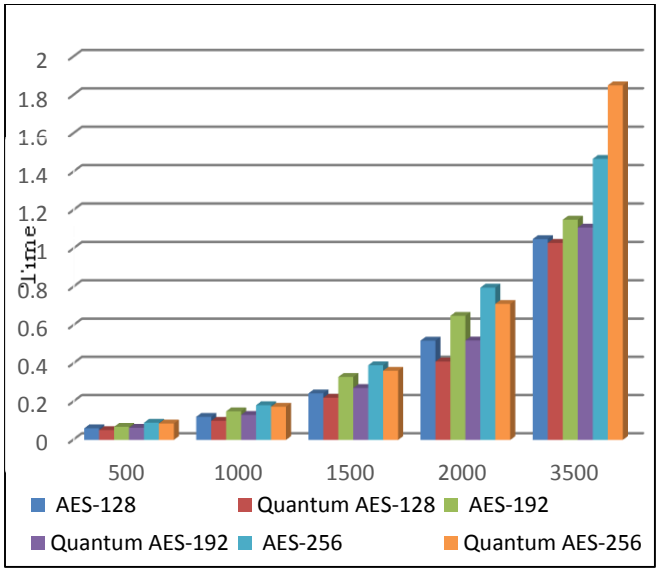

Figure 8. Comparison of AES and Quantum AES

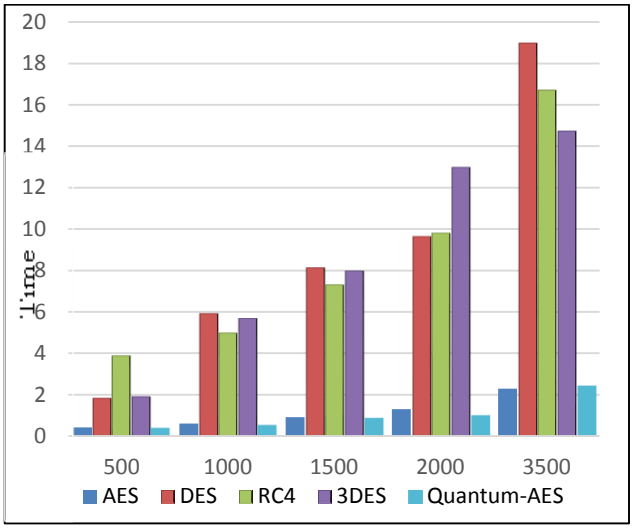

Figure 9. Comparison of Quantum AES and other symmetric key algorithms

7. CONCLUSION

This paper integrates high speed AES algorithm with QKD which ensures an unprecedented level of security. This technique is applicable particularly for high security demanding applications such as nuclear power stations, nuclear weapon sites, government agencies, military and security forces. The proposed scheme ensures balanced speed and security by the means of integrating QKD with classical cryptography methods. The simulation results show that the Quantum AES produces complex keys which are hard to predict by adversaries than the keys generated by the AES itself. In future, Quantum AES will be tested against quantum and algebraic attacks.

8. REFERENCES

[1] Duan, Q. et al. 2012. A Survey on Service-Oriented Network Virtualization Toward Convergence of Networking and Cloud Computing. *IEEE Transactions on Network and Service Management*. 9, 4 (2012), 373-392.

[2] Marwaha, M. and Bedi, R. 2013. Applying Encryption Algorithm for Data Security and Privacy in Cloud Computing. *International Journal of Computer Science Issues (IJCSI)*. 10, 1 (2013), 367.

[3] Ajay Kakkar, M.L. Singh Dr., P.K. Bansal Dr. Efficient key mechanisms in multin-ode network for secured data transmission, Int. J. Eng. Sci. Technol, 2 (5), 2010, pp. 14787–795.

[4] Schneier, B. 1996. *Applied cryptography*. Wiley..

[5] Daemen, J. and Rijmen, V. The Design of Rijndael: AES—The Advanced Encryption Standard of Information Security and Cryptography. 22, Springer Verlag, Berlin, (2002), 231-240.

[6] Rothe, J. 2002. Some facets of complexity theory and cryptography: A five-lecture tutorial. *CSUR*. 34, 4 (2002), 504-549.

[7] A.K. Mandal, C. Parkash, A. Tiwari, Performance of cryptographic algorithms: DES and AES, in: IEEE Students' Conference on Electrical, Electronics and Computer Science, 2012, pp.1-5.

[8] Subasree, S., Sakthivel, N.K. Design of a new security protocol using hybrid cryptography algorithms. IJRRAS 2 (2), 2010, pp.95–103.

[9] Dubal, M.J., Mahesh, T.R., Ghosh, P.A. Design of a new security protocol using hybrid cryptography architecture. In: Proceedings of 3rd International Conference on Electronics Computer Technology (ICECT), vol. 5, India, 2011.

[10] Zhu, S. Research of hybrid cipher algorithm application to hydraulic information transmission. In: Proceedings of International Conference on Electronics, Communications and Control (ICECC), China, 2011.

[11] G.R. Blakley. "One Time Pads Are Key Safeguarding Schemes, Not Cryptosystems Fast Key Safeguarding Schemes (Threshold Schemes) Exist.", Proceedings of 1980 IEEE Symposium on Secuirty and Privacy, 1980, pp.108-113.

[12] D. Stebila, M. Mosca, N. Lütkenhaus. The Case for Quantum Key Distribution, 2009. eprint arxiv: quant-ph/0902.2839.

[13] Omer K. Jasim, Safia Abbas, El-Sayed M. El-Horbaty and Abdel-Badeeh M. Salem. A Comparative Study between Modern Encryption Algorithms based On Cloud Computing Environment‖, the 8th International Conference for Internet Technology and Secured Transactions (ICITST-2013), UK,2013, pp.536-541.

[14] Broadbent, Anne and Christian Schaffner. "Quantum Cryptography Beyond Quantum Key Distribution". *Designs, Codes and Cryptography* 78.1 (2015): 351-382. Web.

[15] Mailloux, Logan O. et al. "Performance Evaluations Of Quantum Key Distribution System Architectures". *IEEE Security & Privacy* 13.1 (2015): 30-40. Web.