ICIC Express Letters
Part B: Applications
Volume **11**, Number **3**, March **2020**

ICIC International ©2020 ISSN 2185-2766
pp. **279–288**

ENHANCEMENT OF QUANTUM KEY DISTRIBUTION PROTOCOL FOR DATA SECURITY IN CLOUD ENVIRONMENT

Yasser Hassen Jassem* and Alharith Abdulkareem Abdullah

College of Information Technology
Babylon University
Babil 51001, Iraq
*Corresponding author: yasserhassen000@yahoo.com; alharith@itnet.uobabylon.edu.iq

Received September 2019; accepted December 2019

Abstract. *There are many different techniques that have been developed to improve security of confidentiality of the user's data in the cloud storage. The assurance of confidentiality of the data stored in cloud storage and the exchange of data and sharing a key that is used to encrypt the data between two parties has been a major concern in the recent years due to the increased use of the cloud services. Also, to more security, we need to store the key away from the cloud and need data encryption in way that cannot break by the high computing like quantum computer. In this paper, we proposed a system that encrypts client's data by an encryption algorithm, by using a key that is generated from Enhancement BB84 protocol, the data can be decoded only with the authenticated user that grants the key from Quantum Key Distribution Server (QKDS) over quantum channel and decrypts the data uploaded to the cloud. The simulation results show that our proposed system was effective in producing more security and less time in the process of data encryption and it provides a security for confidentiality of the user's data in the cloud.*

Keywords: Cryptography, Quantum cryptography, Quantum key distribution, Enhancement BB84 protocol, Cloud computing

1. **Introduction.** Cloud computing is a technology that uses central remote servers and Internet to handle data and applications. The cloud computing technology allows for much more efficient computing by centralizing processing, storage, memory and bandwidth. Moving data to cloud provides great convenience to overcome the difficulty of hardware management [1].

Many organizations and companies have a larger dependency on cloud computing services for their operations in the daily work. Increasingly, amount of data in terabytes is daily being stored in the cloud computing (cloud storage) for access in an easy manner. Due to constantly changing and unpredictable nature of operational environments where cloud services are running there, the security systems encounter significant challenges to secure their data with strong capabilities to make sure that data is protected. Since 2004, data breaches have been increased, exposing confidentiality of the user data in cloud computing. There is an increasing need for user's confidentiality protection [2].

Many surveys or researches in the cloud computing show many reasons that lead most large organizations or companies to depend on the services of the cloud computing. These reasons include reducing the cost of the infrastructure, and fast, and easy access to the applications of the clients that use the services of the cloud computing. The cloud computing is generated from the technologies recently found. There are many challenges in security, which include Reliability and Data Privacy, Confidentiality of Communication/Computation, Data Integrity as well as Authorization and Authentication [1].

DOI: 10.24507/icicelb.11.03.279

The using quantum key distribution protocol with cloud storage environment is very important. The aim of quantum key distribution is to distribute a key to create an encryption that is absolutely unbreakable and key distribution schemes that are non-interceptable [3,4]. In the process of protecting data from unauthorized access, securing of data exchange between two parties has been a major concern in the recent years. By using the quantum, the communication security will be strongly based on the strong features of the quantum cryptography because the quantum key distribution protocol can uncover any eavesdropper activity and supply an effective security even if the data that is sent out to the cloud storage is encrypted, the cloud service providers will have access to it, so the privacy guarantees of the user decrease. For that reason, in this paper we proposed a way that ensures security for the data of the user on cloud computing.

Our proposed system, encrypts the data of the client (owner data) by an encryption algorithm, uses hybrid algorithms of these three encryption algorithms (Triple Data Encryption Algorithm (3DES), Advanced Encryption Standard (AES), Rivest Cipher 4 (RC4)), by using quantum key distribution that is generated from the Enhancement BB84 (EBB84) protocol [5], then after encrypting and uploading the data to the cloud (in our work using Dropbox cloud Storage), the data can be decoded only with the authenticated user who requests certificate from the client side (owner data) to grant the key from the Quantum Key Distribution Server (QKDS) over quantum channel, when the user gets the key from QKDS that can decrypt the data on the user side after downloading it from the cloud. The whole proposed model is shown in Figure 1 as the following.

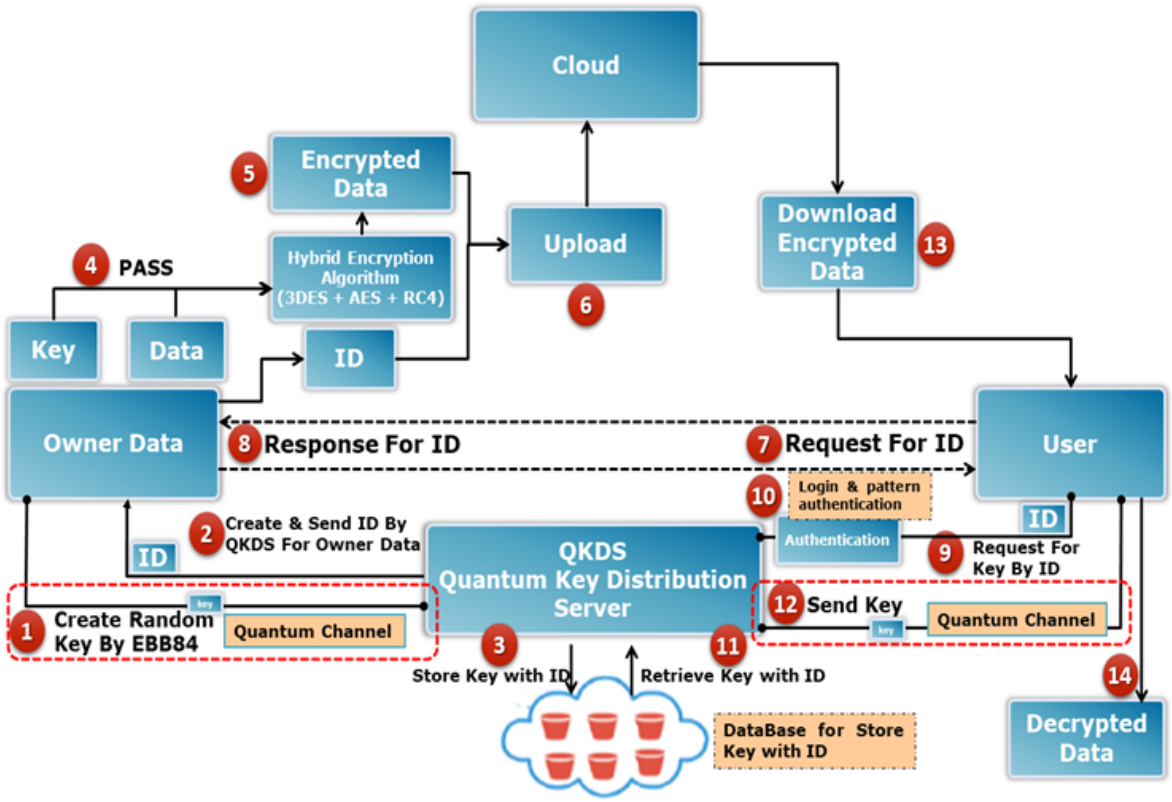

FIGURE 1. The proposed model

2. **Related Work.** There are many researches concerned with using the general quantum cryptography with the cloud environment such as the following researches.

Zukarnain and Khalid in [6] present a new scheme that can be adopted in multi-party communications allocated to cloud infrastructure. The results of this proposed scheme show that they are huge in terms of error rate. The proposed scheme can be capable to

implement with any quantum key distribution protocol and that it will have the ability to authenticate legitimate users.

In [1] Gabriel et al. have proposed a new integration of post quantum cryptography with steganography to ensure that the security of cloud communications are protected strongly in the era of classical computing as well as in the age of computing quantum.

Again in [7] Khalid and Zukarnain produced a new scheme in security of the cloud architecture. A new cloud security environment that implements the QKD (BB84 protocol) proved to be able to gain greater confidence and less time for computation of the cloud computing communications.

In [8] Sharma and Kalra proposed AES algorithm with quantum cryptography. The quantum with AES creates complex encryption keys that are very difficult to predict by the adversary compared with the encryption keys that are produced by AES.

The researchers in [9] proposed a novel schema that takes advantage of the quantum mechanisms to protect the storage of the cloud and the data dynamics. The proposed new schema addresses three parties, namely a cloud server, a data owner, and a trusted client who have provably secure communications with our proposed scheme. The results of the proposed scheme also revealed the success and failure rates with the private cloud computing and public cloud computing respectively.

Tobin et al. discovered in [10] the vulnerability in cloud computing and a solution has been proposed for this security vulnerability by creating an additional security layer using One Time Pad (OTP) random number generator, where the data is encrypted at the client and then uploaded to the cloud computing.

In [11] Zhou et al. clarify the problems of controlling access in the cloud that are handled through the embrace of the techniques of quantum. The proposed scheme has many advantages that make it better than many other proposed systems currently proposed in the same field and proposed for the same purpose.

The researchers in [12] introduced a new idea dealing with the quantum encryption capable of creating encryption codes that are unbreakable with key distribution schemes, which cannot be intercepted.

3. **Proposed Model.**

There are many security problems that cloud computing is suffering from, and they are growing continuously, and cannot ensure the confidentiality of the user's data. Client data in some cloud computing are not encrypted by the cloud service providers while others encrypt the client data, like in iCloud. However, the cloud computing is still successfully attacked, and generally our proposed system (solution), encrypts the data of the client (owner data) and uploads the data to the cloud then the encrypted data can be downloaded from the cloud and decrypted by the user as shown in Figure 1.

A simple model proposed has six components: Data Owner, General Encryption Algorithm (Triple Data Encryption Algorithm (3DES), Advanced Encryption Standard (AES), Rivest Cipher 4 (RC4) and hybrid of all these algorithms are used in this model), Quantum Key Distribution protocol, Quantum Key Distribution Server (QKDS), Cloud and User.

Whole process of proposed model can be described in detail as follows.

- **Step 1 and Step 2:** This process is done by completing the quantum connection between owner data and the QKDS to exchange quantum key that can be used in the next level of our proposed model.
- **Step 3:** Save key in database on QKDS to retrieve the key when it is requested, storing key is done through database() function. ID that is stored in database is agreed by the owner data and the QKDS and it is represented by the first ten of the basis that randomly generated by the QKDS and then transmitted to the owner data.

- **Step 4 and Step 5:** There are a multiple encryption algorithms that can be used to encrypt data (any encryption algorithm can be used to encrypt data), we use some of these algorithms that are suitable for that purpose. The algorithms we use are: Hybrid of these three algorithms (3DES, AES, RC4) to show that any encryption algorithm can be achieved with our work, so we used these three algorithms together. This process is achieved by passing the random generated key from EBB84 protocol to the hybrid encryption algorithm and encryption the data through the Encryptionmethod() function.
- **Step 6:** The uploading process aims to upload the encrypted data to the storage of cloud. Use Dropbox cloud in our work because it is more widely used than some other clouds. With temboo server that is a software toolkit for digital transformation that makes easy access for APIs and temboo is "a scalable, fault-tolerant environment for running and managing smart code snippets that we call Choreos. Choreos can call APIs, simplify the OAuth process". So, use temboo to create an application on Dropbox cloud functions to upload encrypted data with ID through upload() function.
- **Step 7 and Step 8:** User needs to get ID from owner data to grant the key that is achieved over authenticated classical channel (that can be done through any secure way).
- **Step 9 and Step 10:** Once user got the ID that connected to the QKDS to begin exchange key between them. At the first, there are some authentications required to begin process.
- **Step 11:** For more security and to guarantee the key is found in our database, some values (like: generated random bits, owner data's basis) are saved in the database using to compare with the user's ID to authenticate the process. So, once user granted authentication, the process is achieved by searching in database depending on user's ID to check if the key is found in database or not. If the key is found in database, the next step (exchange key) will begin.
- **Step 12:** When the previous step completed and checking that the key is found in our database, this step starts by the QKDS to begin quantum connection to exchange key with user. The quantum connection is done with EBB84 protocol which generates a random key and sends it to the user.
- **Step 13 and Step 14:** Once user gets the key from QKDS, it can download the encrypted data from the cloud and begin the process of decrypting the encrypted data to get the original data and use it for his purpose.

The whole steps of the proposed system summarized in a flow chart that explain each step of the proposed system are shown in Figure 2.

4. **Simulation Results.** The execution of the whole simulation of the proposed system includes the following.

1) execution of the 3DES algorithm.
2) execution of the AES algorithm.
3) execution of the RC4 algorithm.
4) execution of the hybrid algorithm of the three previous algorithms.
5) Full Time Owner X Server Q-Connection.
6) Full Time User X Server Q-Connection.
7) Full Time Execution for all Simulation.
8) Time of Uploading File to the Cloud.

Also, it includes the efficiency and the Quantum Bit Error Rate (QBER) for all tests and another result that are found in the simulation as shown in Table 1.

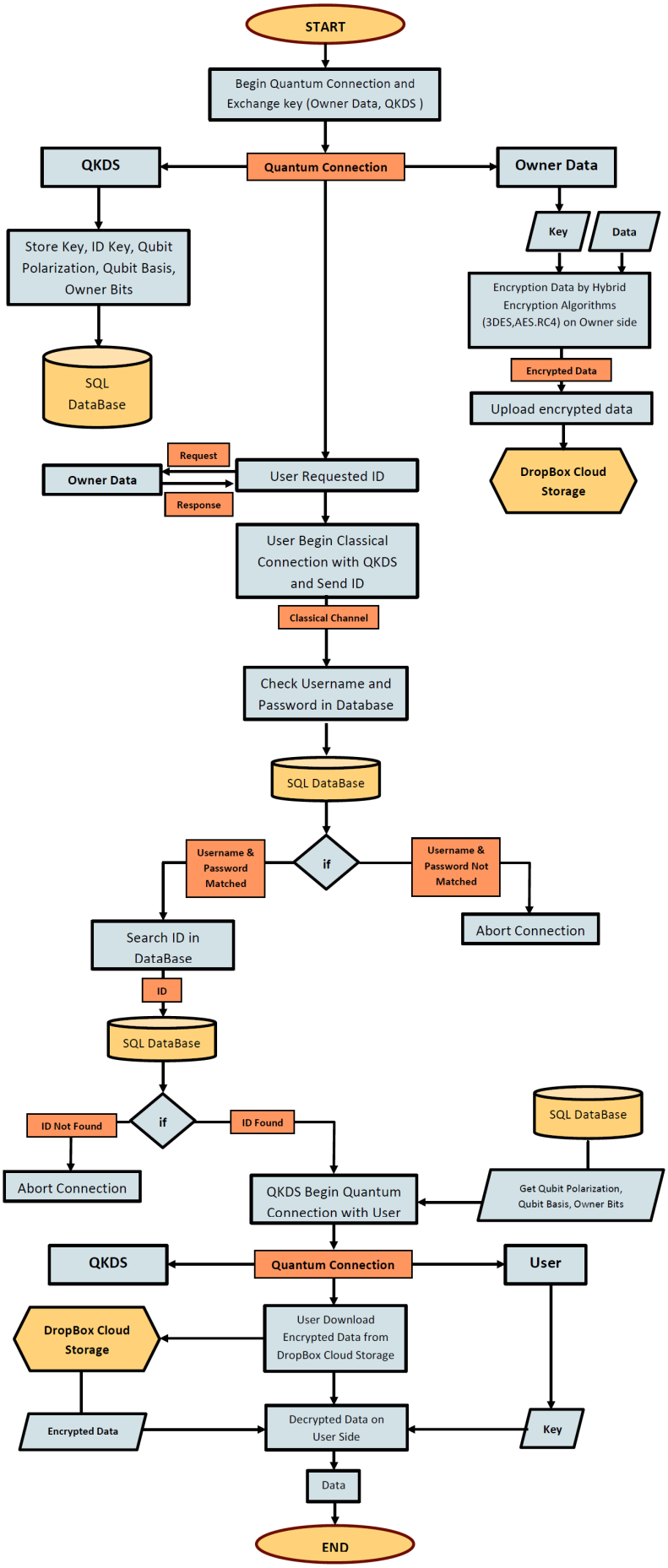

FIGURE 2. Flow chart of the proposed model

TABLE 1. Result of execution simulation of the proposed system

TRY	TRY TIMES	Full Time Owner X Server Q-CONNECTION	Used Bit Number	Throughput Key Length	Wanted Percentage	KEY Percentage (EFFICIENCY)	TIME OF STORE KEY + ID IN DB	3DES ENC + DEC Full Time	AES ENC + DEC Full Time	CR4 ENC + DEC Full Time	3ALG ENC + DEC Full Time	UPLOAD TIME	CLASSICAL CONNECTION	Full Time User X Server Q-CONNECTION	FULL TIME EXECUTION	EFFICIENCY	QBER
TRY 1	1219	8552 ms	1024	565	55%	55.17%	911 ms	12 ms	15 ms	8 ms	35 ms	2809 ms	25069 ms	11069 ms	54830 ms	55.17%	0.448
TRY 2	73	3506 ms	512	284	55%	55.46%	547 ms	16 ms	9 ms	12 ms	37 ms	2767 ms	24502 ms	10317 ms	44327 ms	55.46%	0.445
TRY 3	10	3476 ms	256	142	55%	55.46%	489 ms	17 ms	9 ms	13 ms	39 ms	3066 ms	24012 ms	10705 ms	44833 ms	55.46%	0.445
TRY 4	414	4333 ms	1024	585	57%	57.16%	716 ms	25 ms	15 ms	12 ms	52 ms	3001 ms	19241 ms	9804 ms	41512 ms	57.16%	0.428
TRY 5	20	6039 ms	512	309	59%	60.44%	1831 ms	9 ms	4 ms	7 ms	20 ms	2627 ms	21464 ms	13318 ms	55331 ms	60.44%	0.396
TRY 6	910	3939 ms	256	162	62%	63.28%	487 ms	15 ms	8 ms	9 ms	32 ms	2601 ms	22194 ms	10914 ms	42531 ms	63.28%	0.367
S. D.	441	4974.1 ms	–	312.3	–	56.828%	830.1 ms	15.66 ms	10.0 ms	10.16 ms	35.83 ms	2811.83 ms	22747 ms	11021.16 ms	47227.33 ms	56.828%	0.421

As we see in Table 1, the AES encryption algorithm is the best in depending on the time parameter and the average of execution time for all of the 6 tests in Table 1 for the AES encryption algorithm is (10.0 ms), then come the RC4 encryption algorithms with average time (10.16 ms), and at last the 3DES encryption algorithms come with average time (15.66 ms).

In the proposed system, we use hybrid encryption algorithm of all these three algorithms to make the encryption so strong and to protect the encrypted data from breaking and decrypting by the unauthorized access by attacker or by cloud provider service.

Although the time of the hybrid encryption algorithms is higher than the other three encryption algorithms, we used it to ensure high security for the data uploaded to the cloud. There is another comparison for the three encryption algorithms with calculating the results of the comparison between encryption algorithms and uploaded time for files with different sizes. That can be seen in Table 2.

Table 2. Comparison between encryption algorithms and uploaded time for files with different sizes

FILE SIZE	Used Bit Number	Throughput Key Length	3DES ENC + DEC Full Time	AES ENC + DEC Full Time	CR4 ENC + DEC Full Time	3ALG ENC + DEC Full Time	UPLOAD TIME TO DROPBOX
10 k	1024 bits	565 bits	110 ms	110 ms	115 ms	335 ms	5156 ms
1.2 M	1024 bits	582 bits	1507 ms	1026 ms	1187 ms	3720 ms	44101 ms
10 k	512 bits	287 bits	39 ms	30 ms	36 ms	105 ms	2677 ms
1.2 M	512 bits	292 bits	1483 ms	877 ms	834 ms	3195 ms	23929 ms
10 k	256 bits	141 bits	57 ms	31 ms	26 ms	114 ms	2890 ms
1.2 M	256 bits	142 bits	1478 ms	801 ms	771 ms	3051 ms	25691 ms
STANDARD DEVIATION	–	335 bits	779.0 ms	479.1 ms	494.8 ms	1753.3 ms	17407.3 ms

In Table 2 above, we implement these algorithms with different sizes of the file that are wanted to be encrypted to measure the time of the encryption algorithms in our proposed system.

Also, we can show that time of the AES encryption algorithm is the best in comparison with the other two encryption algorithms.

5. **Evaluating of the Proposed System.** We evaluate our proposed system by comparing the result of implementation of the system with other systems related to our work.

In the research of Tobin et al. [10] they use OTP random number generator to create the key and pass it to the user over classical channel to use the key after getting the encrypted data from the cloud.

In our proposed system we used a QKD protocol (EBB84 that is Enhancement protocol of the original BB84 protocol) [5] that is creating very strong random key with very good randomness that passes to encryption algorithm, and exchange of key over quantum channel is ensured high security due to capabilities in detecting any eavesdropping. The randomness of the key generated by the quantum key distribution protocol is better than that generated by OTP random number generator.

From comparing the result of Tobin et al.'s paper [10] and the result of our work, it appears that the result of our paper is better than result of [10] as shown in Table 3.

In the paper of Sharma and Kalra [8] they use generated key from QKD protocol and pass it to AES algorithm.

Figure 3 shows results of run time analysis of the quantum AES-256 different key sizes of our proposed system. Figure 4 represents the running time of symmetric key algorithms and the proposed scheme for the related paper [8]. It is evident from Figures 3 and 4 that quantum AES-256 of our work is more efficient than the proposed scheme for the related paper [8] and other classical AES encryption algorithms. Furthermore, in our proposed

TABLE 3. NIST (random numbers test) results of simulations of OTP random number generator and our work

Statistical Test	P-value simulation OTP	P-value simulation EBB84	Passed/Fail
Frequency Test	$P = 0.503$	$P = 0.622$	Pass
Block Frequency	$P = 0.216$	$P = 0.622$	Pass
Runs	$P = 0.508$	$P = 0.976$	Pass
Approximate Entropy	$P = 0.201$	$P = 1.000$	Pass
Cumulative Sums	$P = 0.563$	$P = 0.351$	Pass
Discrete Fourier Transform	N/A (Fail)	$P = 0.462$	Pass

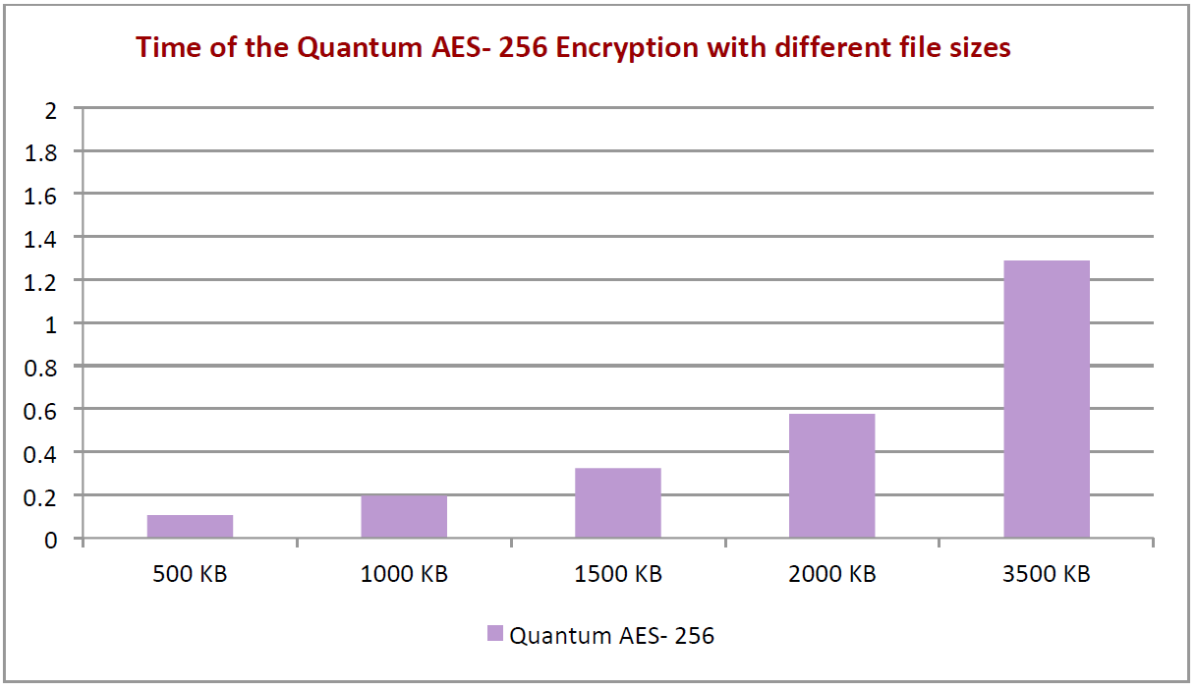

FIGURE 3. Time of the encryption different file sizes by AES with quantum key

system, we used the same way but not only with AES algorithm, we used it with hybrid algorithms (RC4, AES, 3DES).

Also, in the paper of Zhou et al. [11] the key and the certificate are sent to user by owner data and another copy of it stored in the cloud. So, this way will not ensure the confidentiality of the user's data.

In our proposed system, we built something new called a Quantum Key Distribution Server (QKDS) as a third party and it is responsible for exchanging key between owner data and user, while the data is stored in the cloud storage.

Our simulation needs some additions to finish perfectly and completely. Although it serves well enough to show the principle and how it works, there is a lot that can be added. The simplest is Adding Eve to be beneficial for our simulation. With Eve implemented, we would be able to test different security metrics of the protocol, such as how many bits on average Alice and Bob would need to share to detect Eve. From there we could test the other numerous modes of attack, and compare the security of this protocol with others either currently in use, or that have been used in the past.

Despite not having Eve, our simulation still demonstrates the basic idea and functionality of the EBB84 quantum key distribution protocol.

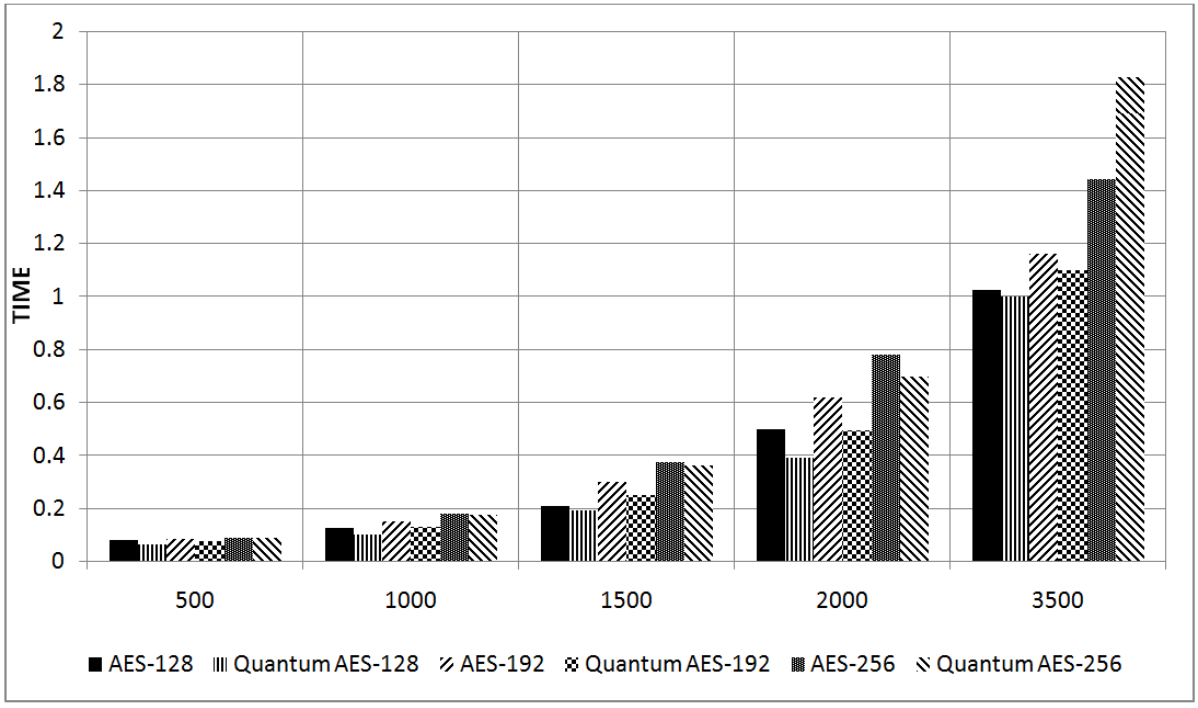

FIGURE 4. Comparison of AES and quantum AES of ([8])

Finally, from the results of three evaluation processes, it can be said that our proposed system was effective in producing more security and less time in the process of data encryption and it provides a high security for confidentiality of the user's data. Also, we provided a way to exchange the key between the owner data and the user over the quantum channel through Quantum Key Distribution Server (QKDS).

6. **Conclusion.** The simulator for the quantum encryption and quantum key distribution in the security of data of the user stored in the cloud storage is dealt with in our proposed system. Poor cloud security and more data breach were detected. So, we proposed a solution for this problem that created an extra level of security using Quantum Cryptography (QC) and the Quantum Key Distribution (QKD).

It also integrates the classical encryption algorithms (3DES, AES, RC4) with QKD that guarantee an unmatched level of security. This integration is applied for high security. The simulation results show that the quantum key distribution protocol produces complex and perfect keys, which are difficult to predict by adversary compared with keys generated by the AES itself.

Furthermore, the proposed system provides a way to exchange the key between the owner data and the user over the quantum channel through Quantum Key Distribution Server (QKDS).

So, our proposed system is considered effective to guarantee both the confidentiality of the user's data in cloud computing and exchange of the key between the owner data and the user through QKDS in a safe way.

REFERENCES

[1] A. J. Gabriel, B. K. Alese, A. O. Adetunmbi and O. S. Adewale, Post-quantum crystography based security framework for cloud computing, *Journal of Internet Technology and Secured Transactions*, vol.3, no.4, pp.344-350, 2014.

[2] L. Sim, S. Ren, S. Keoh and K. Aung, A cloud authentication protocol using one-time pad, *IEEE Region 10 Conference (TENCON)*, Singapore, pp.2513-2516, 2016.

[3] H. C. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, *Proc. of the IEEE International Conference on Computers, Systems and Signal Processing*, vol.175, pp.175-179, 1984.

[4] H. C. Bennett, F. Bessette, G. Brassard, L. Salvail and J. Smolin, Experimental quantum cryptography, *Journal of Cryptology*, vol.5, no.1, pp.3-28, 1992.

[5] A. A. Abdullah and Y. H. Jassem, Enhancement of quantum key distribution protocol BB84, *Journal of Computational and Theoretical Nanoscience*, vol.16, no.3, pp.1143-1159, 2019.

[6] Z. A. Zukarnain and R. Khalid, Quantum key distribution approach for cloud authentication: Enhance tight finite key, *International conference on Computer Science and Information Systems (ICSIS'2014)*, Dubai, UAE, pp.28-33, 2014.

[7] R. Khalid and Z. A. Zukarnain, Cloud computing security threat with quantum key distribution defense model, *Proc. of the 3rd International Conference on Green Computing, Technology and Innovation (ICGCTI2015)*, Malaysia, pp.49-54, 2015.

[8] G. Sharma and S. Kalra, A novel scheme for data security in cloud computing using quantum cryptography, *Proc. of the International Conference on Advances in Information Communication Technology & Computing*, Bikaner, India, 2016.

[9] G. Murali and R. S. Prasad, CloudQKDP: Quantum key distribution protocol for cloud computing, *International Conference on Information Communication and Embedded System (ICICES 2016)*, 2016.

[10] P. Tobin, L. Tobin, M. McKeever and J. Blackledge, On the development of a one-time pad generator for personalising cloud security, *The 8th International Conference on Cloud Computing, GRIDs and Virtualization*, Ireland, pp.73-78, 2017.

[11] L. Zhou Q. Wang, X. Sun, P. Kulicki and A. Castiglione, Quantum technique for access control in cloud computing II: Encryption and key distribution, *Journal of Network and Computer Applications*, 2017.

[12] P. H. Sureshkumar, A. Pramitha and R. Rajesh, The quantum key distribution (QKD) based security enhanced cloud data center connectivity, *International Journal of Latest Trends in Engineering and Technology*, vol.7, no.4, pp.378-382, 2016.