A Novel Quantum Secure Data Sharing Protocol for Cloud Environment based on Cloud Service Provider

Umi Salma. B

[1]Department of Computer Science, Jazan University, Jazan, Saudi Arabia

Abstract: In the last two years group communication Services are more popular ever before in the history of internet because of Covid-19. Educational institutions and organizations fully depend on secured data sharing network's (proxy server). Secure file sharing in cloud environment is widely researching field for many researchers in order to transmit sender's data securely to receiver with the help of proxy server. Cloud data security is the main concern to the companies. Most of the malwares downloaded from cloud applications and from HTTPS- connection which are encrypted. Proxy re-encryption is a type of secured, trusted, confidential and safe data sharing process. Quantum technology is growing rapidly, the main outcome of quantum technologies are encryption and secret sharing between sender and receiver using proxy. In this paper, a proxy re-encryption protocol based on Quantum carriers and principle (PRPQCP) is proposed. Sender in the protocol should have the capacity to generate Bell states by executing Bell and Z basis quantifying and storing qubits, this will decrease receiver quantum need, prepared for better implementation. Proxy server without knowing the sender plain-text converts sender cipher-text data to cipher-text of receiver data. The receiver needs to have the ability to return and initialize Z-basis quantifying. One secret one time, conceptually executed mostly when similar information shared multiple times. The plain text hacking and cipher text hacking securities are realized. Outstanding-granularity secret file sharing is achieved.

Keywords: Proxy Server, Proxy-re-encryption, Cloud Environment, Quantum, Bell States

I. INTRODUCTION

In Covid-19 pandemic third party services are adopted widely by educational institutions, companies, industries, hospitals and government etc. Network applications such as Online Classes, Games, video conferences, built in Radio, Mobile TV Series, video calling, group chatting etc. The main concern is handling security in file sharing network during data transmitting between groups. This scheme explains how sender and receiver communicate in cloud environment with the help of proxy server (Cloud service provider) called Proxy re-encryption. Here we call Sender as delegator and Receiver as delegate. Sender stores his plain text data in cloud server in the form of cipher-text after encrypting. Even service provider doesn't know the plain text of the sender because the private key is with sender. Here Proxy play third party role which is very important for secure and safe data sharing. If sender wants to share his data to Receiver then the third party called proxy converts sender. Cipher - text sender data to cipher-text of receiver data without decrypting the sender cipher-text using sender private key. In this protocol sender should have the potentiality of generating Bell states, carry out Bell and Z – basis quantifying and storing qubits. The quantum needs of the receiver are minimized. The receiver required to have review and execute Z – basis quantifying. One time one pad is applied theoretically, when ever unique data shared many times. The against selection plain-text threat security and the against selection cipher-text threat security are realized. Fine-granularity secret information (data) sharing is successful achieved by using this scheme.

II. LITERATURE REVIEW

A. Quantum Secure Data Sharing Risk in Cloud

QKD Protocol using Bell's theorem to secure quantum key distribution, satisfies its security against any member attack by an attacker only restricted by the non-signaling condition [1]. Entropy accumulation method proposed which declares the full amount of cryptographic protocols with device independent quantum key sharing, while obtaining important optimal specifications. According to loophole-free Bell testes recommended that the obtained specification are accessible scientifically and satisfies theoretically experimentally demonstration of device independent cryptography [2]. Secret File Sharing Schemes evaluated with respect to data access, security and cost in the pay as you go paradigm [3]. Proposed group key agreement protocol which utiliing the state vectors of group members, generated random numbers determine the logical link among the group members and generates multiple cryptographic keys independently using local secret key [4]. Improved Semi Quantum Secret Sharing Protocol (SQSS) is more secure and efficient and satisfies the semi quantum condition [5]. CASMA deals with dynamic nature of IoT application by utilizing context aware security server, Surveyed, analyzed, compared and consolidates the previous work and appreciated their work towards IoT based on taxonomy and evaluation [6].

The analysis of alternative algorithms for key computation, encryption, decryption, and resource utilization using the suggested protocol reveals that RSA performs well with little files, whereas ElGamal and Paillier methods are better for larger files to be saved in cloud storage file sharing technique through Trusted Third Party (TTP) system, in order to overcome the existing symmetric key cryptography. TTP keeps confidentiality and integrity of the stored and received data [7]. Unidirectional proxy re-encryption method proposed and improved previous schemes by contributing collusion resilience and addressed the re-encryption key sharing issues further more [8]. QBDQ method based on oracle functioning and proved that it has more efficiency related to communication Entanglement and used oblivious sharing technique to resolve the issues of the client's privacy [9]. VSS method proposed to verify strong t-consistency of member; members use the sub polynomial of master secret key to make verification polynomial and utilize to verify master members [10]. XOR-based threshold secret SSS proposed, using XOR operations are used to make shares and recover the secret and it is easy to extend to multi secret method [11].

Classical and quantum secret sharing scheme proposed, its secure, easy availability against the quantum computation and eavesdropper attack [12]. Detected four kinds of noise on RSP method and compared with single qubit method and resolved long distance RSP [13]. Derived straight physical connection among the N parties MABK and CHSH inequality related to an offence of the CHSH inequality among one of the members (parties) and the remaining N-1. To identify multipartite complexity between N parties participated in the protocol and generated a common key [14]. Driver HQ public cloud infrastructure used to access the secure file as SaaS using PRNG algorithm to generate random numbers in sequence order each time when ever key generates [15]. Solved the issue by altering URDA with variable fragment lengths, As a result, all bits in revealed sequences are randomly distributed uniformly and independently [16]. Proposed GKMP based on mixed encryption and verification method applied to stop shared files from being attacked by the attacker [17]. Multi-secret sharing schemes (MSSSs) proposed by [18], [19]. Block chain-based authentication and dynamic group key agreement protocol proposed to authenticate left member and perform batch authentication which will decrease communication cost and computation. Solved single node failure problem using 4 setups to register user to join the group and used mathematics and prove if to increase the security and accuracy of proposed protocol [20].

Secure key Management System proposed in order to reduce the time during encryption and decryption key generation process [21]. A Dynamic Privacy Aggregate Key Re-Encryption (DPAK-RE) algorithm proposed to secure data security. Authenticate members can collect many groups of top secret keys and keep in a envelope at once all a single key and possibilities of keys are collected, later this collection of keys Re-encrypted and initiates the private key [22]. Introduced DNA based Random Key Generation and Management for OTP Encryption method to resolve OTP symmetric key initiation and sending issues with DNA, at the molecular level by generating DNA Bio-hiding secret key [23]. Enhanced and Secured RSA Key Generation Scheme (ESRKGS), in this algorithm four large prime numbers used with RSA to make more secure along factorized method [24]. DNA proxy re-encryption method generates three keys for the sender, in order to access data Proxy or Receiver. Sender encrypt data using his key and stores in cloud, if receiver need data then proxy re-encrypt he data using second key, receiver decrypt the data with help of third key [25]. Shimao et.al. Proposed Revocable and identity-based conditional proxy re-encryption scheme with ciphertext evolution (RIB-CPRE-CE) method proposed based on Xiong et al.'s identity based conditional proxy re-encryption method for efficient and secure data sharing in cloud. URKeyGen and UpReEnc used into the previous method to maintain cipher-text evolution and used to generate updated re-encryption keys [26].

III. METHODOLOGY

A. *Proposed Protocol*

The main aim of the proposed protocol: Sender and Receiver are both users of a cloud data centre. Sender binary information is $B \in \{0, 1\}^n$. Sender sends the cipher-text of B on the proxy (Service provider) data server. The cipher-text of B represented as $C_S \in \{0, 1\}^n$, where $C_S = B \oplus RN$, Random number initiated by sender with help of quantum random number generator is $RN \in \{0, 1\}^n$ and this generated RN is non-public to others. If sender want to share cipher-text B along with Receiver then they has to take proxy server help in order to complete securely. The basic process of this protocol as follows: initially sender sends conversion key $c_k \in \{0, 1\}^n$ to the Service provider (proxy server) in order to generate final conversion key $c_k^f \in \{0, 1\}^n$, using this final conversion key Proxy server changes senders cipher-text to Receiver cipher-text $C_R \in \{0, 1\}^n$, later receiver decrypts C_R to obtain plain-text B by utilizing his private key $K_R \in \{0, 1\}^n$. K_R can be acquired by accomplishing the beginning algorithm of the proposed mechanism, described in the definition 3 of section 3. proxy also don't know about plain-text B. the relation between receivers private key K_R and other variables described. Figure 1 gives detail information of the proposed protocol.

B. *Preliminaries*

- Definition 1: A Bell state is defined as a maximally entangled quantum state of two qubits has four states.

$$\emptyset^{\pm} = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle), \psi^{\pm} = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle) \quad (1)$$

This $\emptyset^{\pm} = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)$ bell states property that upon measuring the first qubit, one gets 2 possible results: 0 with probability 1/2, leaving $\emptyset^{\pm} = |00\rangle$. As a result, a measurement of the second qubit always gives the same result as the measurement of the first qubit. That is the measurement outcomes are correlated. Similarly, the Bell States $\psi^{\pm} = \frac{1}{\sqrt{2}}$ $(|01\rangle \pm |10\rangle)$ has the attributes beginning with the first qubit, one gets two desirable results: 0 along feasibility 1/2, quitting the post determining state $\psi^{\pm} = |01\rangle$ and 1 with feasibility 1/2, quitting $\psi^{\pm} = |10\rangle$. As a result, a determining of the second qubit regularly gives result in the inverse as the determining of the first qubit. The determining conclusion is associated.

- Definition 2: Z-basis $\{|0\rangle, |1\rangle\}$ determine is the determining of a qubit in the computational basis. This is a determining on a single qubit along result determined by the two determining operators $B_0 = |0\rangle\langle 0|$, $B_1 = |1\rangle\langle 1|$. the determining operators fulfill the requirement for completeness. Assume the state being calculated is $|\psi\rangle = \propto |0\rangle + \beta|1\rangle$. Then the chance of obtaining determined output 0 is p (0) $=| \propto |^2$. Likewise, the chance of obtaining the Determining result 1 is p (1) $= |\beta|^2$. The state after determining in the two cases is therefore $|0\rangle$ *or* $|1\rangle$.

Algorithm definition**:** When sender's message or information stored on proxy server is to be shared with Receiver, Sender is the delegator, Receiver is the delegate and the cloud service provider is proxy server. Sender formerly shared key $K \in \{0, 1\}^N$, with the cloud service provider by executing quantum key distribution protocol.

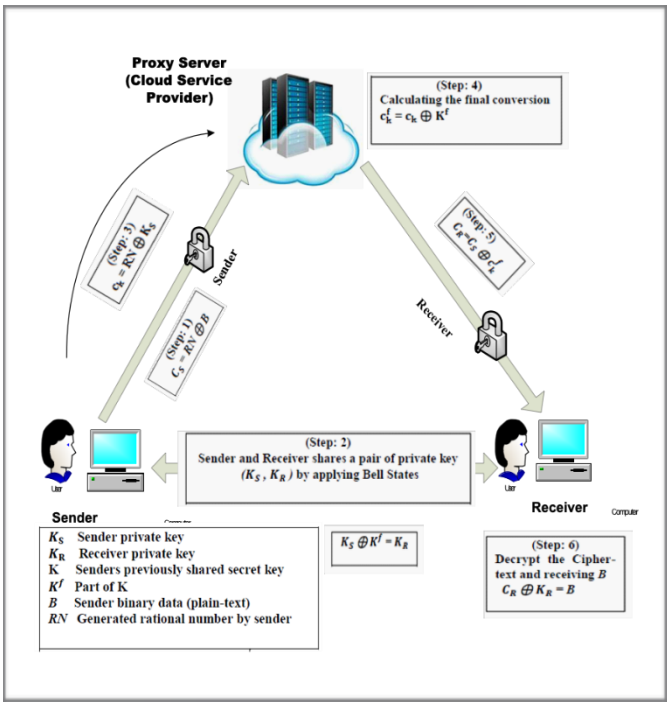

Figure 1: Structure of the proposed protocol

- Definition 3: The Initial Algorithm
  Initial (K): On inputting the secret key $K \in \{0, 1\}^n$, details of algorithm works as follows:
  1. Sender arranges N Bell states bestow to K. The arranging rule is: '0' to form state $\emptyset^+$ and '1' to form state ψ^-.
  2. Each Bell state is conserved by Sender by one particle and Receiver receives the other particle from Sender.
  3. Receiver randomly executes Z-basis $\{|0\rangle, |1\rangle\}$ and analyzes each particle received. Receiver saves the analysis results as $K_R \in \{0, 1\}^n$, where '0' implies result $|0\rangle$, and '1' implies $|1\rangle$.
  4. Sender executes joint Bell-basis analysis on repeated particles which received and reserved for the same particles. The protocol will continue if each analysis is consistent with the Bell state that was originally created or if the inconsistent ratio is less than the set threshold or else the protocol will be abolished.
  5. Sender registers the positions as P when the Sender does not receive particles and uses Z-basis to allot the registered particles. Sender saves the analyzed results as $K_S \in \{0, 1\}^n$, as per the rule: '0' for state $|0\rangle$ and '1' for state $|1\rangle$.
- Definition 4: Key Generation Algorithm
  KeyGen (K_S, RN): On adding sender's secret key K_S and a random number RN, this algorithm outputs key $c_k \in \{0, 1\}^n$, where $c_k = RN \oplus K_S$.
- Definition 5: Algorithm for generating re-encryption keys
  Re-keyGen (c_k): Proposed algorithm works as follows after adding the secret key c_k:
  1. Sender computer $c_k^f = Encrypt_k(c_k, P)$ and sends c_k^f to the cloud service provider (proxy). Here $Encrypt_k()$ may could be any same encryption algorithm excluding for XOR.
  2. The proxy server decrypts c_k^f with K to obtain c_k and P.
  3. According to P, the proxy server separates the reciprocal bits in K to get $K^f \in \{0, 1\}^n$
  4. The proxy server computers $c_k^f = c_k \oplus K^f + RN \oplus K_S \oplus K^f + RN \oplus K_R$, and obtains the final modification key $c_k^f \in \{0, 1\}^n$. Here, $K_s \oplus$
  $K^f = K_R$ is obtained as per Bell states properties.
- Definition 6: Encryption Algorithm
  Encrypt (RN, B): On inputting a random number RN and plain-text B, this algorithm outputs the cipher-text $C_S \in \{0, 1\}^n$, where $C_S = RN \oplus B$.
- Definition 7: Re-Encryption Algorithm
  Re-Encrypt (c_k^f, C_S): After inserting the final conversion key c_k^f and cipher-text C_S, the proposed algorithm executes the re-encryption cipher-text $C_R \in \{0, 1\}^n$, where $C_R = C_S \oplus c_k$.
- Definition 8: Decryption Algorithm

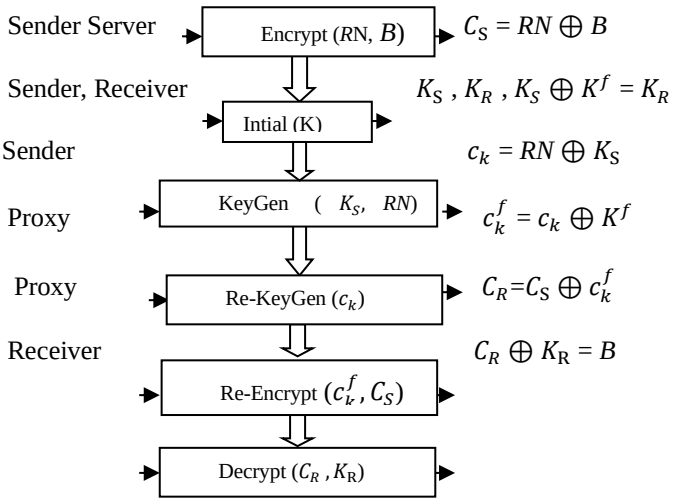

Figure 2: Algorithm Execution Process

Decrypt(C_R, K_R): After entering receiver's secret key K_R and cipher-text C_R, algorithm executes the plain-text *B*. Figure 2 algorithm execution process.

C. Protocol Security Proof

According to the below induction, the proposed protocol satisfies the consistency requirement:

Sender ⟶ the proxy

$$Encrypt_k(c_k, P)$$
$$C_s = RN \oplus$$

The proxy: $c_k, P = Decrypt_k(Encrypt_k(c_k, P)$

$$K^f = Extract(K, P)$$
$$c_k^f = c_k \oplus K^f$$

The proxy ⟶ Receiver: $C_R = C_S \oplus c_k^f$

Receiver: $C_R \oplus K_S = C_s \oplus c_k^f \oplus K_R = RN \oplus B \oplus c_k^f \oplus K_R = RN \oplus B \oplus RN \oplus K_R \oplus K_R = B$

In general, to prove the security of traditional cryptography proposal, the security goals are established first. After that, as per the attacker capability an attack model developed. The approach condition for dividing the idea is proposed to determine a tough mathematical obstacle.

In our proposed design, the sender's information is encrypted along with random number *RN* and saved on proxy (Cloud Service provider). If the sender is accepted or agreed to share information with requested user, then sender has to execute the protocol. According to the principles of quantum no-duplicate, unpredictability and complication, complication secure that the cipher-text re-encryption of the same shared information is different in each process, it means that on-time one-pad (one time one secret) is generated. Hence it's proved that the proposed protocol can withstand anti-selective plain-text attack without employing the standard reduction procedure, anti-selective plain-text attack and anti-selective cipher-text attack.

The principles of quantum no-duplicate, unpredictability and complication works on the protocol where it has the capacity to find or stop attackers from contradict quantum bearers. Section III *D* satisfies that if the surveillant aims to contradict quantum bearers with a high possibility, attacker's actions will be discovered. (Approximately 99.9 percent)

In addition, in the proposed protocol, proxy server knows only K^f the complication relationship among K_S and K_R, even proxy don't know the stored data and sender and receiver's relationship among K_S and K_R. Receiver knows only *P* andK_R. Therefore he is not able to know the stored data on proxy server (cloud service provider) without the re-encryption of cipher-text by the proxy server.

D. Security Analysis

Prevent Resend Attack: Eve may interrupt the particles that sender sends to the receiver and compare that data particles with Z-basis, later arranges some possible particles having unique state and send back to the receiver. Assume that every particles reserved by sender is revealed as packet 1, each particle sent to receiver is identified as particle 2, and each particle altered or modified by Eve is identified as particle e. Later, after Eve interrupt and comparing particles 2 with Z-basis, then the particle state 1 collapses, to $p_1 = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|$. The state of the particle repeated by the Receiver is

$p_e = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|$. The mixed state of particle *e* is: $p_{1e} = \frac{1}{4}|00\rangle\langle 00| + \frac{1}{4}|11\rangle\langle 11| + \frac{1}{4}|01\rangle\langle 01| + \frac{1}{4}|10\rangle\langle 10|$

(2)

If the beginning state of particle 1 and 2 is ψ^-, after eavesdropping detected the joint Bell-basis calculate the result on particle 1 and e is as follows:

$$\rho'_{1e} = \frac{1}{2}|\psi^+\rangle\langle\psi^+| + \frac{1}{2}|\psi^-\rangle\langle\psi^- \quad (3)$$

If the beginning state of particle 1 and 2 is $\emptyset^+$, after eavesdropping detected, the joint Bell-basis calculate the result on particle 1 and e is as follows:

$$\rho'_{1e} = \frac{1}{2}|\emptyset^+\rangle\langle\emptyset^+| + \frac{1}{2}|\emptyset^-\rangle\langle\emptyset^-| \quad (4)$$

Therefore, sender can detect Eve's eavesdropping on each qubit with possibility 1/2, and the total possibility that sender can identify Eve's eavesdropping is $1-(1/2)^n$, When n = 5, the possibility reaches 97%. The proposed protocol will be abolished, and the sender data that stored on the proxy server cannot be retrieved by the eavesdropper.

1) *Attack from Untrusted Source:* Repeated particle are used to detect eavesdropping attack, intercept-resend attack and source untrusted attack. Usually, in untrusted source attack, Eavesdroppers with superpowers will provide equipment for generating Bell states. Despite the fact that Sender believes a true Bell state is ready, what receiver actually receives may be a distinct state because the qualified device is maintained by Eve. That is to say, the source cannot be trusted. To steal Sender data, Eve might be able to use the servers to generate some non-caught up mixed states. States of |00⟩, |01, |10, |11⟩ or caught up states along a larger dimension like as GHZ states.

a) Eve prepares state $p_{12} = \frac{1}{2}|00\rangle\langle 00| + \frac{1}{2}|11\rangle\langle 11|$. Instead of $\emptyset^+$ and develops state

$p_{12} = \frac{1}{2}|01\rangle\langle 01| + \frac{1}{2}|10\rangle\langle 10|$. Instead of ψ^-.

In this manner, Eve will be knows sender's key K_S and Receiver's key K_R before eavesdropping detection. However, during the eavesdropping, Sender executes the join Bell-basis calculations on particle 1 and 2 and the following output will be received reciprocally:

$$\rho'_{12} = \frac{1}{2}|\emptyset^+\rangle\langle\emptyset^+| + \frac{1}{2}|\emptyset^-\rangle\langle\emptyset^-| \ \textit{or}$$

$$\rho'_{12} = \frac{1}{2}|\psi^+\rangle\langle\psi^+| + \frac{1}{2}|\psi^-\rangle\langle\psi^-| \quad (5)$$

Certainly, Sender will detect Eve's eavesdropping on every qubit with the possibility of 1/2, and the entire possibility that Sender identifies Eve's eavesdropping is $1-(1/2)^n$. Then, the protocol will get discontinue, and the Eve's eavesdropper will not be able to access any information which saved or stored on proxy server.

b) Eve prepares to connect the state:

$E_0, E_1 Or\ p_{123} = \frac{1}{2}|E_0\rangle\langle E_0| + \frac{1}{2}|E_1\rangle\langle E_1|$.

Instead of $\emptyset^+$, and prepares connect state

$E_2, E_3\ or\ p_{123} = \frac{1}{2}|E_2\rangle\langle E_2| + \frac{1}{2}|E_3\rangle\langle E_3|$ instead of ψ^-. Here,

$$E_0 = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle_{123} \quad E_1 = \frac{1}{\sqrt{2}}(|001\rangle + |110\rangle_{123}$$

$$E_2 = \frac{1}{\sqrt{2}}(|010\rangle + |101\rangle_{123}, E_3 = \frac{1}{\sqrt{2}}(|100\rangle + |011\rangle_{123} \quad (6)$$

Eve forwards particle 1 and 2 to Sender, and keeps particle 3 itself. When Receiver checks the received particle 2 with Z-basis, then the state of particle 1 and 3 collapse. As Eve Don't know on which stages receiver check and return, Eve never checks packet 3 on the non-return along Z-basis till receiver decides which states are returned. Although, by doing this, receiver will receive K_S *and* K_R but prior to that, to find eavesdropping Sender executes joint Bell-basis computation on particle 1 and 2.

If Eve prepares entangled state

$E_0, E_1 or\ p_{123} = \frac{1}{2}|E_0\rangle\langle E_0| + \frac{1}{2}|E_1\rangle\langle E_1|$

Instead of $\emptyset^+$, the measurement result is:

$$\rho'_{12} = \frac{1}{2}|\emptyset^+\rangle\langle\emptyset^+| + \frac{1}{2}|\emptyset^-\rangle\langle\emptyset^-| \quad (7)$$

If Eve prepare unsettle state

$E_2, E_3\ or\ p_{123} = \frac{1}{2}|E_2\rangle\langle E_2| + \frac{1}{2}|E_3\rangle\langle E_3|$

$$\rho'_{12} = \frac{1}{2}|\psi^+\rangle\langle\psi^+| + \frac{1}{2}|\psi^-\rangle\langle\psi^-| \quad (8)$$

Prior to Eve knows Sender key and Receiver key K_S and K_R, sender identifies the eavesdropping behavior of Eve with the possibility of $1 - (1/2)^n$. then the protocol discontinue and its sure that the eavesdropper unable to get any sender information which stored on proxy server (service provider).

2) Proxy Server Attack: In this our Proposed protocol the proxy server knows only the connection between Sender and Receiver key K_S and K_R and don't know the sender plain-text B because it encrypted by sender itself before stored in cloud server through $C_R = B \oplus K_R$. In other words only sender knows the random number which is encrypted the shared information B, although not possible to proxy server to know *B* through $C_S = RN \oplus B$. Assume if the proxy server is not trusted then proxy server is the eavesdropper as discussed in s, proxy has the authority of eavesdroppers and knows the K. whenever proxy server executes tackle-resend attacks with the help of *K* won't help proxy to successes in his attack. Then, sender detects eavesdroppers, the attack notification will be received by sender with the possibility $1 - (1/2)^n$ and the data stored by sender on cloud server or proxy server don't know by proxy itself. For trusted proxy server, proxy having the conversion key c_k and the final conversion key c_k^f, even though proxy unable to get plain-text of stored data by sender on cloud server. If the proxy is not trusted then its behavior will be identified with the possibility of 100 %. So it's proved that neither trusted nor untrusted proxy has the access to the sender plain-text which stored in cloud server.

IV. RESULT AND DISCUSSION

1) *Experimental Result*

The proposed protocol proved and extremely advantageous in Cloud Environment key management system (CEKMS). These keys play a vital role in attention to the domain network security. The previous analysis expanded network security and privacy depend upon the cloud environment (cloud computing) protocols. Evaluations are carried out on the experimental system. The

performance of the algorithm is evaluated taking into discretion the components like security and execution time as seen in Table1. The execution time of the proposed protocol is impressive in comparison to the existing protocols as show in Figure 3. PRPQCP protocol provides great security with regards to key encryption and decryption compared to existing protocols as seen in Figure 4.

2) *Discussion*

Continues decline and mutual data are commonly used to investigate quantum key sharing security, i.e. secret key deal by communication above the quantum approach. This section analyzes protocol's post-preparation from the viewpoint of mutual information. To process the key shared by sender and receiver typically compatible and to decrease the amount of data Eve knows, the protocol need to implement error settlement and secret elaboration. The packet which sent by sender and receiver may interrupt Eve and compares that packet with the Z-basis and sends back to receiver. In generally, Receiver compares with Z-basis state. The output of the Z-basis comparison is received as K_R . Eve's attack may not succeed in a little error because the packet comparison basis is unique with Receiver's. Assume bit error rate λ for the external factors excluding Eve's attack as mention above. To make error correction, needs to share more information of H2(λ) for every bit of error. After secret elaboration, security key rate is:

$$c \leq I(Y:X) - I(Y:E) = 1 - H_2(\lambda) - I(Y:E) \quad (9)$$

Eavesdropping detection protocol has to detect whether the sender and Receiver packets share the unsettled the state $\emptyset^+$or ψ^-, once unsettled state is confirmed from eavesdropping detection protocol, Eve unable to obtain the data of Receiver key K_R, as per the monogamy of nonlocal unsettled. Therefore, in our proposed protocol, I (Y: E) = 0.

$$c \leq 1 - H_2(\lambda) \quad (10)$$

Let's Assume the secret information B length is n, the length of c_k^f, K_S *and* K_R must be n bits in order to ensure that the confidential information can be transmitted successfully. Therefore, c_k, K_S *and* K_R length prior to error rectification and privacy boosting which is denoted as m must meet the following constraint

$$m \geq \frac{n}{1-H2(\lambda)} \quad (11)$$

The total number of Bell states executed in the beginning of the algorithm should satisfy:

$$N = 2m \geq \frac{2n}{1-H2(\lambda)} \quad (12)$$

Table 1 presents the data which is used to perform the analysis. Carried out four algorithms evaluation specifically Enhanced and Secured RSA key Generation Scheme (ESRKGS), DNA Proxy re-encryption, Dynamic Privacy Aggregate Key Re-Encryption (DPAK-RE), secure key Management System (SKMS) and proxy re-encryption protocol based on Quantum carriers and principle (PRPQCP)

S.No	No of Techniques	Execution Time (ms)	Security	
			Encryption (bits)	Decryption (bits)
1	(ESRKGS)	113.7	9000	9500
2	DNA Proxy re-encryption	112.56	5000	4500
3	DPAK-RE	350	8000	8000
4	SKMS	95.12	9500	9500
5	PRPQCP	93.05	9900	9900

Table 1: Techniques Performance comparison

Figure 3 shows the comparison and describes the KMS based on cryptography techniques execution with the access of ESRKGS, DNA, DPAK-RE, SKMS and proposed protocol PRPQCP. This proposed protocol is extremely effective and gives impressive execution time in compare to the response of the existing protocols.

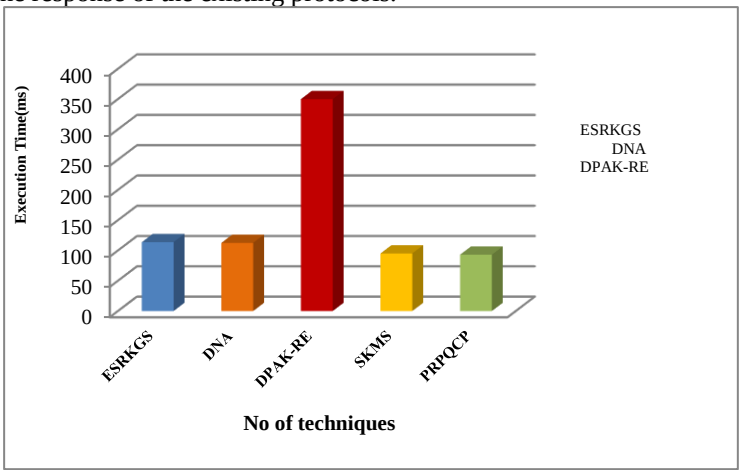

Fig 3: Execution time comparison

Figure 4 shows the comparison and describes the KMS based on cryptography techniques performance with the access of ESRKGS, DNA, DPAK-RE, SKMS and proposed protocol PRPQCP. This proposed protocol provides great security with regards to key Encryption and Decryption in compare to the existing protocols.

3) *Comparison with previous work*

The proposed protocol is compared with earlier proxy re-encryption methods in reference with [8], [12] this proposed protocol satisfied theoretically and implements applies one-time one-pad (one time one secret), mostly when unique information shared more than one times. In each information sharing task and generates a random number with Complication connection. It is assured from quantum non-cloning principles, unpredictable and complexity. The second layer cipher-text of the receiver may not reflect. As a result, the protocol understands anti-selection and anti-selective cipher-text attack, security without depending on complicated mathematical problems.

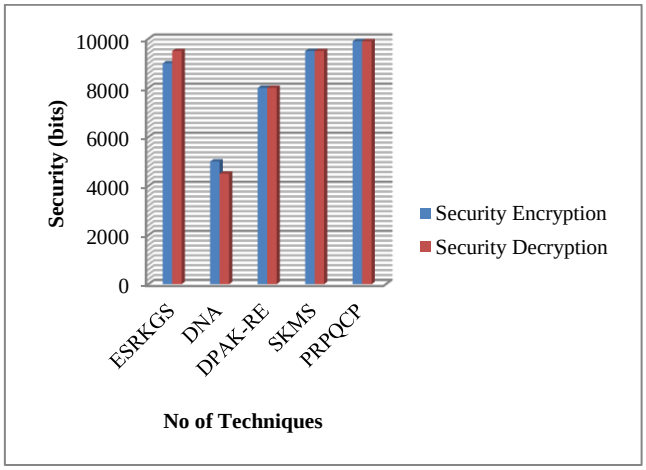

Fig 4: Security comparison between techniques

Compared our protocols with refs [8], [16], our proposed [26] protocol flexibly included secret data sharing at fine- grossness. By modifying c_k and the beginning point of shared information, the Sender can regulate the sharing grossness to the Receiver. The protocol, on the other hand, is vulnerable to the proxy server and Receiver's conspiratorial attack. Executing Bell and Z basis analysis and storing qubits. Receiver quantum capability is less: receiver must have the ability to execute Z basis analysis and return. Also compared proposed protocols with QSS protocols in refs [13], [14], [15], [20] our protocol makes it easier to implement. In refs [14], [15] more than one packet complexity states required being prepared, but this is much more difficult than processing Bell states. In ref [19] although both quantum secret and typical secret sharing prepared, Quantum Fourier transformations and a d-level quantum system, on the other hand, are required, which are more sophisticated and difficult to construct than our protocol. Protocol need to implement error settlement and secret elaboration. The packet which sent by sender and receiver may interrupt Eve and compares that packet with the Z-basis and sends back to receiver. In generally, Receiver selects randomly to give back the packet or Receiver compares with Z-basis state. The output of the Z-basis comparison is received as K_{R} . Eve's attack may not execute or succeed in a little error because the packet comparison basis is unique with Receiver's.

V. CONCLUSION

The proposed method of quantum cryptography protocol recognizes safe and secure information sharing on proxy server depend on proxy modification encryption. In the proposed system the block-resend attack, the untrusted source attack and proxy server attacks are analyzed. In the proposed protocol sender should have the capacity to execute Bell states by calculating Bell and Z basis comparison and saved qubits. Receiver quantum requirements are decreased and the receivers itself possess the ability to return and carry out Z-basis calculations, which satisfies partially quantum cryptography protocol condition. In information lost or stolen outline to make sure that normal key distributing after Sender sends packets to Receiver, Receiver has to declare which packets are lost or stolen, once done this sender discards the particular packets Prior to extracting K^f, sender and proxy server should discard the particular packet bits.

ACKNOWLEDGEMENTS

The researcher(s) would like to thank the Deanship of Scientific Research, Qassim University for funding the publication of the project.

REFERENCES

1. A. G. N. &. M. L. Acín, "From Bell's.theorem to secure quantum key distribution," *Phys Rev Lett*, pp. 97(12), 120405, 2006.
2. F. D. O. F. a. R. R. Arnon Friedman, "Practical device-independent quantum cryptography via entropy accumulation," *Nature Communications*, p. 9:459, 2018.
3. V. D. J. &. H. N. Attasena, "Secret sharing for cloud data security: a survey.," *The VLDB Journal*, pp. 26, 657–681, 2017.
4. M. K. S. Bilal, "A Secure Key Agreement Protocol for Dynamic Group," *Cluster computing, springer*, p. 20(4), 2017.
5. X. Z. S. B. &. C. Y. Gao, "Cryptanalysis and Improvement of the Semi-quantum Secret Sharing Protocol," *Int J Theor Phys*, pp. 56, 2512-2520, 2017.
6. A. W. a. O. A. E.-M. Hussein Harb, "Context Aware Group Key Management Model for Internet of Things," *The Seventeenth International Conference on Networks*, pp. 978-1-61208-625-5 34, 2018.

7. P. M. R. A. a. S. P. S. Indu, "Secure File Sharing Mechanism and Key Management for Mobile Cloud Computing Environment," *Indian Journal of Science and Technology*, p. 48, 2016.
8. H. R. D. S. L. a. K. C. Jian Weng, "chosen cipher-text secure bidirectional proxy re-encryption schemes without pairing," *Institutional Knowledge (InK) at Singapore Management University*, pp. 180,(24), 2010.
9. W. X. Y. Z. M. C. J. &. Y. C. Liu, "A novel quantum visual secret sharing scheme," *IEEE Access*, pp. 7, 114374–114384, 2019.
10. W. G. P. L. Z. C. H. &. Z. M. Liu, "A quantum-based database query scheme for privacy preservation in cloud environment," *Security and Communication Networks*, p. 10.1155, 2019.
11. Y. X. H. L. Y. C. N. &. Z. Y. Q. Liu, "Efficient (n, t, n) secret sharing schemes," *The Journal of Systems and Software*, pp. 1325-1332, 2012.
12. S. Mashhadi, "General secret sharing based on quantum Fourier transform," *Quantum Information Processing*, pp. 18,114, 2019.
13. Z. G. W. S. Y. W. M. M. S. L. &. W. X. J. Qu, "Effect of quantum noise on deterministic remote state preparation of an arbitrary two-particle state via various quantum entangled channels," *Quantum Information Processing*, pp. 16(306), 1–25, 2017.
14. J. M. G. &. W. S. Ribeiro, "Fully device-independent conference key agreement," *Phys Rev A*, pp. 97(2), 022307, 2018.
15. S. A. a. S. V. Y. Shakkeera Liaquath, "Secure key management system mobile cloud data storage," *International Journal of Engineering and Advanced Technology (IJEAT)*, p. 20(17):4835, 2019.
16. A. Shamir, "How to share a secret. Communication," *ACM*, pp. 22, 612–613, 1979.
17. S. h. B. Z. k. h. a. E. p. Shouyi Zhang, "Group Key Management Protocol for File Sharing on Cloud Storage.," *Digital Object Identifier*, p. 10.1109, 2017.
18. S. &. I. K. Takahashi, "Secret sharing scheme suitable for cloud computing," in *27th International Conference on Advanced Information Networking and Applications (AINA2013)*, IEEE 27th International Conference, 2013.
19. C. C. C. T. Y. &. H. M. S. Yang, "A (t, n) multi-secret sharing scheme," *Math. Comput*, pp. 151(2), 483–490, 2004.
20. F. L. H. D. M. T. J. Z. a. J. X. Zisang Xu, "A Blockchain-Based Authentication and Dynamic Group Key Agreement Protocol," *doi:10.3390/s20174835: Sensors*, pp. 20, 4835, 2020.
21. V. a. V. V. Pradeep. K, "Secure Key Management System in Cloud Environment for Client data," *IJEAT*, vol. 8, no. 5, pp. 1-7, 2019.
22. P. M. M. S. H. &. V. K. R. Reddy, "Secured Privacy Data using Multi Key Encryption in Cloud Storage," 2018.
23. X. L. M. S. Yunpeng Zhang, "DNA based Random Key Generation and Management for OTP Encryption," *BioSystems*, pp. 1-1, 2017.
24. P. V. M. M. K. N. M. Thangavel, "An Enhanced and Secured RSA Key Generation Scheme (ESRKGS)," *Elsevier, Journal of information security and applications*, pp. 1-8, 2014.
25. A. Elhadad, "Data sharing using proxy re-encryption based on DNA computing," *Springe, Soft Computing*, 2019.
26. S. D. R. V. K. H.-J. &. Yao and I.-H. Ra, "A novel revocable and identity-based conditional proxy re-encryption scheme with ciphertext evolution for Secure Cloud Data Sharing," *IEEE Access*, no. 42801–42816, p. 9, 2021.

Dr. Umi Salma. B is a Sr. Lecturer at the Faculty of Computer Science & Information technology Department, Jazan University, Jizan, Saudi Arabia. Dr. B. Umi Salma has completed her Ph.D in Computer Science, Master of Computer Application and M.PHIL Degree in Computer Science. Dr. B. Umi Salma has published research papers in International Journals such as Computer Science & Network Security, International journal of cryptography & Security, Information Journal on computer engineering & information Technology. She has also participated in various national conferences on cryptography and security and workshops on Network Security and Network Security in its Advance Applications organized by department of Computer Science & Engineering. She has also participated in International Conference on Emerging Trends and Computer Sciences on Computer Science & Mobile Applications organized by department of International Technology and was also presented conference papers in various conferences and awarded the best paper award at the IICET2015. She has interest in the area of Information Security, Cryptography and Network Security, Security in Computing.