International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-2, December 2019

Certificateless Bilinear Quantum Mutual Exclusive Signcryption for Data Security in Cloud

Kavitha K, Saravanan V

Abstract: ***Signcryption perform both encryption and signature verification simultaneously with minimum computational time and overhead when compared to that of the traditional signature model. Certificateless Sigcryption rectifies issues corresponding to the key escrow problem and hence reducing the key management in the traditional key cryptography in Cloud environment. There has been some Certificateless Signcryption methods proposed, most of which are proved secured using the proxy pairing operations. However, with proxy pairing found to be computationally difficult in understanding and with the discrete operation reducing the advantages gained from smaller key size, data security is said to be compromised. To address this issue, in this work, a method called, Bilinear Quantum Mutual Exclusive Signcryption (BQ-MES) for data security in cloud environment is presented based on quantum principles. The new method inherits the security of bilinear mapping along with quantum, which possesses lower computation complexity than proxy operations, employed in signcrypting data in cloud environment. In the BQ-MES method, only a designated authorized cloud user recovers the data stored in the cloud via cloud service provider by verifying the validity of a signcrypted data. This is performed using Mutually Exclusive Probability model. Experimental works are conducted on the parameters such as computational time, computational overhead and data security rate. By evaluating the performance with related schemes, results show that the data stored in cloud environment is secured using BQ-MES method and computationally efficient.***

Keywords**:** ***Certificateless Signcryption, Bilinear Mapping, Quantum, Mutual Exclusive, Cloud.***

I. INTRODUCTION

Cloud computing provides flexible access via internet-based computing to cloud users. As the communication between users pertaining to their data are performed via cloud environment, securitizing data remains the major concerns. To preserve the data, several authentication mechanisms have been designed in the recent years using certificateless signcryption for cloud environment.

A new cryptographic concept called Searchable Attribute Based Sign Cryption (SABSC) was proposed in [1] that supported fine-grained access control, data privacy, data authenticity, and data searchability. Besides, security was also said to be established with hybrid access policy. This was said to be achieved by applying Decisional Bilinear Diffie-Hellman Exponent hardness assumption, attained unforgeability based on the Computational Diffie-Hellman Exponent problem and ensured keyword secrecy based on the one-way hash function.

With this, the SABSC method achieved indispensable essential security requirements, such as data confidentiality, keyword secrecy, unforgeable with minimum time complexity. Despite data confidentiality and security achieved for data with minimum time complexity, the space complexity involved in cloud in performing the above said activities (i.e. data confidentiality, keyword secrecy, unforgeability) remained unaddressed. To reduce the space complexity involved, in this work, Bilinear Setup Mapping model is first used in the design of network and cloud computing environment.

Data security is a pertinent service in cloud computing. However, its comprehensive application is hampered by the apprehension of having a secure access to data without a violation on authentication and confidentiality. To address this problem, a novel data access control method that not only achieves authentication but also ensured confidentiality for cloud-based smart grid systems, called Certificate Less Signcryption with Proxy Re Encryption (CLS-PRE) was presented in [2].

The method initially stored the encrypted smart grid-related data in the cloud. Upon requirement of the data by the user, the data owner issued a delegation command to the cloud to perform data re-encryption. Therefore, the cloud here is not said to acquire any plaintext information on the data, where only authorized users are competent of data decryption. Both the integrity and authentication of data was said to be verified with minimum time and space complexity. However, data security was not said to be ensured. To provide data security between cloud users, a Quantum Key Generation model is designed, that entirely works on the principle of quantum theory. Besides, the Quantum Key Generation has the advantage of possessing secure solution to the key exchange problem and hence ensures data security in cloud environment. One of the most important services in cloud environment is data storage. The central constituent of data storage remains in the effective data storage, by providing measures for confidentiality and authorized access of data in cloud. In [3], a novel data access control mechanism was designed using an Identity Based Sign Cryption with proxy re-encryption, ensuring data security.

Revised Manuscript Received on December 30, 2019.
***** Correspondence Author
Kavitha.K*, Department of Computer Applications, Dr. N.G.P. Arts and Science College, Coimbatore, India. Email: kavitha.k@drngpasc.ac.in
Saravanan, V,Department of Information Technology, Hindusthan College of Arts and Science, Coimbatore, India. Email: vsreesaran@gmail.com.

Yet another data security model based on secure handover and certificateless signcryption was presented in [4]. Despite security measures included, the computational efficiency was not considered. To address this issue, a pairing free certificateless proxy signcryption based on elliptic curve cryptography was presented in [5], therefore improving computational efficiency.

Wireless Body Area Network (WBAN) also referred to as the mobile-health system is considered as one of the main book for remote patient monitoring. It is considered as a system to monitor the human body's health in a remote manner and also analyze the health status parameters in real time. In [6], an improved certificateless signcryption scheme based on elliptic curve discrete logarithm was designed to address the computational and communication cost involved in designing security proof model. Despite improvement found in computational and communication cost, the security remained one of the main concerns was not attended in [7], a provable secure cipher text policy attribute based encryption was designed. In [8], hash-based proxy signatures were used for cloud based health information exchange to provide security. However, the above said scheme measures only the data confidentiality. Certain other factors, like computational time, overhead are not considered. In fact, computational time, computational overhead are necessary for data security in cloud environment. The reason is that the cloud data receiver cannot be sure that received data is the same as the cloud sender data when the cloud data receiver gets the data from the cloud service provider. An unauthorized user in the cloud can even modify the stored data for some intentions. So it is important for the cloud data receiver to verify the integrity and source of received data.

In this paper, we solve this problem by proposing a Certifictaeless Signcryption scheme with bilinear mapping and quantum principles. With the two functions, first, the computational time and overhead incurred is said to be reduced and with the quantum principles, it remains difficult in changing the data by the unauthorized users. Different to the conventional model of public and private key system, our method not only allows the authorized user to decrypt the ciphertext but also allows it to verify the source and validity of the data via mutual exclusion probability function. Besides we also show how to use out method to insure the security of data in cloud environment by applying polarization principle. In summary, the contributions of the paper include the following:

- We develop a novel Bilinear Setup Mapping model that is computationally efficient and complicated math involved making only authorized user to extract data and ensuring data security.
- We use the proposed Quantum Key Distribution model to develop a novel public and private key generation that enables authenticated and authorized selective sharing of data via cloud service provider. The model exhibits several desirable features that include quantum properties providing data security via public and private key generated via third party public key generator, flexible specification of key generation policies compliance with agreements between cloud data owners and cloud data users.
- We perform a detailed security and performance analysis of the proposed method. Our computationally efficient analysis shows that the proposed Certificateless Signcryption method ensures data security in cloud environment. We compare the performance of the proposed method with other well known certificateless signcryption methods in the literature and find that the proposed method achieves the best performance while being provably secure.

The remainder of this paper is organized as follows. Section 2 discusses some preliminaries of the paper related to the certitificateless signcryption scheme applied in cloud. Section 3 introduces the network and presents the proposed method. Section 4 presents the experimental setup and Section 5 presents the performance evaluation containing computational time, computational overhead and data security. Finally, we draw a conclusion in Section 6.

II. RELATED WORKS

With the swift growth of cloud environment, more users are coming to propose moving both the huge significance of data storage and computation overhead to the cloud server in a cost-effective manner. Despite the advantages provided by using the cloud environment, secure data access control is still considered to be one of the most hindrances as the cloud server is not entirely trusted by the cloud user and the data stored in cloud may include certain amount of sensitive data or information.

In [9], attribute-based signcryption was designed without degrading the attribute privacy, balancing both the security aspects along with practical computation efficiency. Yet another computationally efficient method that outsourced the heavy computation to ciphertext transformed server was presented in [10]. Signcryption with equality test was proposed in [11] to provide both authentication and confidentiality in a simultaneous manner. Yet another certificateless online/offline signcryption method was designed in [12] to provide data security. Despite security, anonymity of user was not provided. To address this issue, a dynamic password-based two server authentication and key exchange mechanism was provided in [13], therefore ensuring robust and secure access to cloud services.

A policy controlled system with anonymity was designed in [14] that validated signature without revealing the signer identity, therefore ensuring both privacy and anonymity. Multi-receiver signcryption on the other hand requires message signcryption for large number of receiver. In [15], an efficient certificateless multi-receiver signcryption scheme was designed that signcrypted a message for any number of receivers, therefore guaranteeing non-repudiation.

Different security and privacy protection techniques were reviewed in [16] from both hardware and software aspects, therefore enhancing the data security. Data mining techniques were applied in [17] using Apriori algorithm to ensure security in cloud. An efficient and provable secure anonymous two factor authentication was designed in [18] for not only ensuring security but was also proved to be computationally efficient. However, the above schemes were not proven to be efficient in terms of cipher text retrieval schemes. To address this issue, an efficient cipher text retrieval instance with a designated tester was presented in [19]. With this the method was proven to be effective and efficient for retrieval of data in cloud environment.

A new and novel searchable revocable multi-data owner attribute-based encryption model based on hidden policy for secured cloud storage was presented in [20].

In conclusion, most of above work only considers the data confidentiality and ignores the data security and computational factors. However, the data security and computational factors are also necessary for data security in cloud environment since an adversary may modify the stored data for some intentions. This is our motivation of this paper.

III. BILINEAR QUANTUM MUTUAL EXCLUSIVE SIGNCRYPTION (BQ-MES)

Cloud environment involves an on-demand availability of computer system resources, specifically data securiyt, computing power, resource utilization and so on without the direct involvement of the user. However, the data stored in cloud is not said to be full proof in terms of security. Several security mechanisms have been provided by different research persons in various perspectives.

A proxy re-encryption model was designed in [1] for providing data confidentiality and security with minimum time complexity. However, the space complexity involved while ensuring data security remained a major concern. Yet another method using attribute-based signcryption was designed in [2] ensuring data integrity and authentication. Despite these two advantages, the data security measure was not considered. To address the above said issues like data security with minimum time and space complexity, in this work, a Bilinear Quantum Mutual Exclusive Signcryption (BQ-MES) method is designed. In this section, Bilinear Quantum Mutual Exclusive Signcryption (BQ-MES) for data security in cloud environment is designed. Figure 1 shows the block diagram of BQ-MES method.

As illustrated in the Figure 1, to start with a cloud environment is created based on the network and followed by which a cloud environment setup is designed consisting of 'n' number of cloud data owners 'CD_o' and cloud data users 'CD_u', a cloud service provider 'CSP' and third party public key generator 'TP_PKG' respectively. Next, the cloud data user initiates the process of data sharing with the other users of the

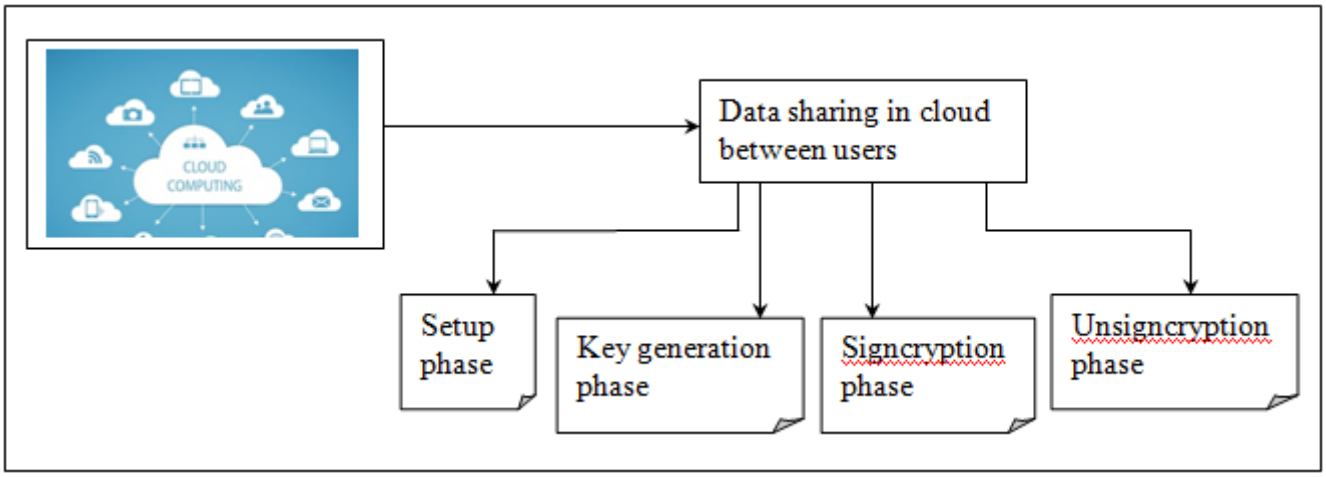

Fig. 1. Block diagram of Bilinear Quantum Mutual Exclusive Signcryption

cloud. Finally, during the data sharing over cloud, four steps are performed, setup phase, key generation phase, signcryption phase and unsigncryption phase. The BQ-MES method consists of the following steps.

A. Network model

Figure 2 given below illustrates the overview of the network model [3] for providing data security in cloud environment. The network model consists of four types of entities, a third party private key generator 'TP_PKG', a cloud data owner 'CD_o', a cloud data user 'CD_u' and a Cloud Service Provider 'CSP'. The 'TP_PKG' is responsible for signing up of the 'CD_o' and 'CD_u' respectively and produces the private keys for them.

The 'CD_o' transmit its data to the 'CSP' in an unreadable encrypted form. In other words, the 'CSP', do not know the real content of the transmitted data. It obtains the data from the cloud data owner and stores in the data center. If any other cloud user has to access the data, the cloud service provider along with the third party public key generator checks for the key (i.e. public and private key). Upon matching of the key, data is provided to the cloud user via the third party public key generator.

B. Bilinear Setup Mapping

The certificateless signcryption for data security in cloud environment is built on bilinear groups. The bilinear mapping involves a function that fuses components of two vector spaces to yield a component of a third vector space and is linear in each of its arguments. The purpose of using bilinear mapping in the setup phase is due to the minimum CPU usage occupied, besides the complicated math involved making extraction trivial and obtained only by following highly securitized format. In the setup phase, to start with a security parameter 'SeP' is taken as input. The third party private key generator 'TP_PKG', executes the Bilinear Setup Mapping algorithm to generate system parameters 'SyP' and a master key 'M_Key'. The pseudo code representation of Bilinear Setup Mapping is given below.

Algorithm1 Bilinear Setup Mapping algorithm

Input: Security Parameter 'SeP'
Output: System Parameter 'SyP', Master Key 'M_Key'
1: Initialize Security Parameter 'SeP' 2: Begin 3: Obtain bilinear group using (1), (2) and (3) 4: Publish system parameter and master key using (4) 5: Return (System Parameter 'SyP', Master Key 'M_Key') 6: End

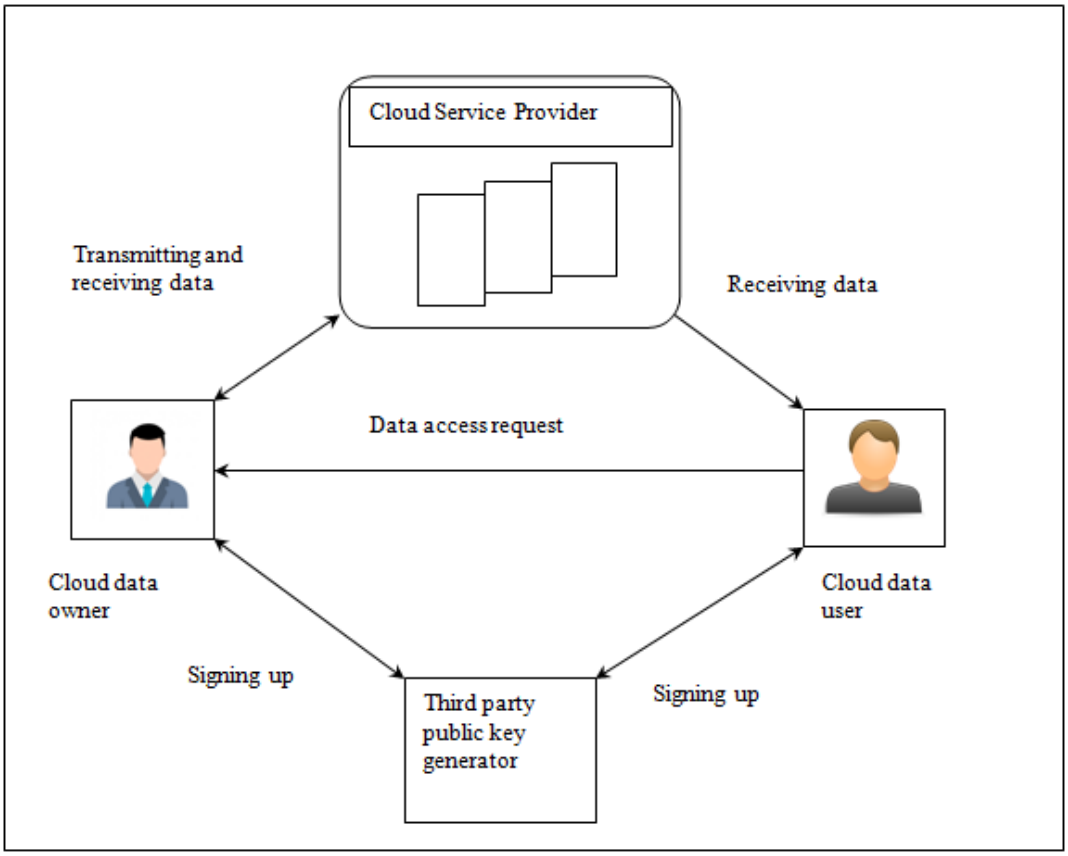

Fig. 2 Network model

As given in the above algorithm, the system parameters are said to be publicly available in the cloud environment, whereas the master key 'M_Key'' is maintained secretly by the third part private key generator. Let 'CG_1' and 'CG_2' and 'CG_t' represent the cyclic groups of the same order. Then a bilinear map from '$CG_1 * CG_2$' to 'CG_t' represents a function and is given below.

$$f: CG_1 * CG_2 \rightarrow CG_t \text{ such that for all} \quad (1)$$

$$a \in CG_1, b \in CG_2, p, q \in \mathbb{Z} \quad (2)$$

$$f(a^p, b^q) = f(a, b)^{pq} \quad (3)$$

With the above said bilinear mapping, the third party private key generator 'TP_PKG' obtains the system parameter as given below.

$$Setup(SeP) \rightarrow (params, M\_Key) \quad (4)$$

From the above equation (4), the common parameters '$params$' includes the data'D' to be stored in the cloud and the data space 'D_Space' occupied by it.

C. Quantum Key Generation

With the data to be stored in the cloud environment, based on bilinear mapping setup, in this section, key generation based on Quantum Key Distribution (QKD) model is presented. The QKD involves the process of extracting the key (i.e. public/private key) with the purpose of securely sharing data in cloud. The conventional key distribution strategy (i.e. partial private key) [1] depends on the strength of mathematical problems and assumptions on capabilities of users in cloud environment, where the security is said to be hindered by uncertain random number generator. All these aspects, especially, the sustained progress in quantum information processing, make it inevitable to securely distribute cryptographic keys. Quantum Key Distribution (QKD) provides solutions to these matters via underling quantum properties to store the data in a secured manner in cloud environment. The QKD encrypts the '$0s$' and '$1s$' of a digital signal (i.e. data) on individual particles of light, i.e., photons. Each type of a photon's spin denotes one piece of information, '0' or '1' for binary code. This code in turn utilizes strings of '$0s$' and '$1s$' to produce a logical message. Followed by which a binary code is said to be allocated to each photon. For example, a photon possessing a vertical spin is said to be assigned with '1' and a photon possessing a horizontal spin is said to be assigned with '0'.

The sender now sends the photons via randomly selected filters and records the polarization of each photon. Now, the sender knows what photon polarizations the receiver has to be received. Even, if the unauthorized cloud user detects the signal, the information present in the photons is quickly transformed, specifying both that an unauthorized user is trying to extract the data present in the cloud and the unauthorized user cannot obtain the data and hence is said to be secured. The pseudo code representation of Quantum Public and Private Key Generation is given below.

Input: Common parameters '$params$', identity of the cloud user 'ID_u'
Output: Users public/private key pair 'PB_{Key}, PR_{Key}'

1: Begin
2: For each System Parameter 'SyP' with identity 'ID_u'
//partial private key extraction
3: Perform partial private key extraction using (5)
4: Obtain two orthogonal states using (6)
5: Extract private key using (10)
//public key extraction
6: Extract public key using (11)
7: Return (users public/private key pair 'PB_{Key}, PR_{Key}')
8: End for
9: End

Algorithm 2 Quantum Public and Private Key Generation

As given in the above algorithm, with the objective of designing data security in cloud environment, Quantum Public and Private Key Generation are used. Three different processes are involved in the design of the above algorithm. They are partial private key generation, private key generation and public key generation. To start with partial private key generation is performed by the third party private key generator. The third party private key generator 'TP_PKG' runs this which takes as the common parameters '$params$', an identity of the cloud user 'ID_u' and outputs a Partial Private Key 'PPK_u'. Then the 'TP_PKG', send 'PPK_u', to the respective cloud user via a secure channel.

$$PPK_u \rightarrow extract-partial-private-key\left(params, M_{Key}, ID_u\right) \quad (5)$$

Based on the above partial private key, the full private key is obtained using the quantum principle. Here data is no longer encoded on the number of involved photons, but individual photons serve as carriers and quantum information and photons are encoded on their quantum properties, like polarization. Two orthogonal states like '$|0> and\ |1>$' encode the '0' and '1' values of the quantum bit (qubit), and is mathematically expressed as given below.

$$|\varphi>=\alpha|0>+\beta|1>, \alpha, \beta \in C_{Text}, |\alpha|^2+|\beta|^2=1 \quad (6)$$

From the above equation (6), a photon is utilized as a qubit and each polarization base is set to either horizontal or vertical to denote a canonical equilibrium system. In this work, the horizontally polarized photon denotes logic zero and is mathematically expressed as given below.

$$|0>=(1\ 0)^T \quad (7)$$

On the other hand, the vertically polarized photon denotes logic one and is mathematically expressed as given below.

$$|1>=(0\ 1)^T \quad (8)$$

$$|\varphi>=R(\theta_u)\ (|1>or\ |0>) \quad (9)$$

From the above equation (9), the private key is mathematically expressed as below.

$$PR_{Key}=extract-private-key\left(params, \varphi, PPK_u\right) \quad (10)$$

Given the common parameters '$params$', the partial private key 'PPK_u', the private key 'PR_{Key}', the cloud user with identity 'ID_u', the public key is expressed as below.

$$PB_{Key}=extract-public-key\left(params, PR_{Key}, PPK_u\right) \quad (11)$$

With the three keys generated above, i.e., partial private key, private key and public key, the process of data security in cloud environment is said to be proceeded by designing signcrypt and unsigncrypt that is described in the forthcoming section.

D.Bilinear Quantum Mutual Signcryption and Unsigncryption

Given the common parameters '$params$', the data 'D', and the public key 'PB_{Key}', the user with identity 'ID_u' and the full private key 'PR_{Key}', the cloud service provider runs this algorithm to generate the cipher text 'δ' as the output. This is mathematically expressed as given below.

$$\delta \rightarrow BQ-Signcrypt\left(params, D, PB_{Key}, ID_u, PR_{Key}\right) \quad (12)$$

Given the ciphertext 'δ', the sender's identity 'ID_u' and the public key 'PB_{Key}', the receiver with identity 'ID_{u1}' and the full private key 'PR_{Key1}', the cloud service provider runs this algorithm to unsigncrypt the ciphertext. This is mathematically expressed as given below.

$$D \rightarrow BQ-Unsigncrypt\left(params, \delta, ID_u, PB_{Key}, ID_{u1}, PR_{Key1}\right) \quad (13)$$

The pseudo code representation of Bilinear Quantum Mutual Signcryption and Unsigncryption is given below.

Input: Receivers private key 'pk_r', Sender public key 'pk_s', Cipher text 'C', identity of the cloud user 'ID_u'
Output: Data '$d_1, d_2, \ldots, d_n$'

1: Begin

2: For each cloud user 'ID_u'

3: Generate Signcryption using (12)

4: Return cipher text 'δ'

5: End for

6: If '$P(A/B) = 1$' then

7: Valid signature

8: Obtain the unsigncrypted original data using (13)

9: End if

10: If '$P(A/B) <> 1$' then

11: Invalid signature

12: End if

13: End

Algorithm 3 Bilinear Quantum Mutual Signcryption and Unsigncryption

As given in the above algorithm, after performing signcryption via bilinear quantum model, unsigncryption is performed. This is performed via Mutual Exclusive Probability model. In Mutual Exclusive Probability model, the probability of the receiver in the cloud environment is interpreted as the ratio of frequencies of outcomes where the statement is true to the total outcomes 'TO'. This is mathematically formulated as given below.

$$P(ID_u) = \frac{\{x: ID_u(x)\}}{\{x : TO\}} \quad (14)$$

The Mutual Exclusive Probability is then formulated as given below.

$$P(ID_u/ID_{u1}) = \frac{\{x:ID_{u1}(x) \wedge ID_u(x)\}}{\{x:ID_{u1}(x)\}} \quad (15)$$

From the equation (15), 'ID_u' refers to the signature (via private key) of cloud sender and 'ID_{u1}' refers to the signature of the cloud receiver node. Here, '$P(ID_u)$' and '$P(ID_{u1})$' refers to the probabilities of matching cloud sender signature 'ID_u' and 'ID_{u1}' without regard to each other. Here, '$P(ID_u/ID_{u1})$' represents the probability of cloud sender signature match with cloud receiver. On the other hand, '$P(ID_{u1}/ID_u)$' denotes the probability of cloud receiver signature match with cloud sender. If the result of '$P(ID_u/ID_{u1}) = 1$', then the signature of both the cloud sender and cloud receiver is valid and the original unsigncrypted data packet is obtained via the cloud service provider.

IV. EXPERIMENTAL SETUP

The experimental evaluation of the proposed Bilinear Quantum Mutual Exclusive Signcryption (BQ-MES) for data security in cloud environment and existing Searchable Attribute Based Sign Cryption (SABSC) [1] and Certificate Less Signcryption with Proxy Re Encryption (CLS-PRE) in [2] are implemented in Java Language with cloudsim simulator. The Amazon Access sample Dataset is taken from the UCI machine learning repository https://archive.ics.uci.edu/ml/datasets/Amazon+Access+Samples#. This is an anonymized sample of access provisioned within the company. This is a sparse data set which comprises a number of users and their authorized access. The file includes 4 types of attributes such as Person_Attribute, Resource_ID, Group_ID and System_Support_ID that is stored on the cloud server. Based on the user information, the cloud server performs authentication either 'remove_access' or 'add_access. This dataset is used to find the authorized user to access or store the data, services or resources to the cloud server. Otherwise, the cloud server removes access. Based on the attribute information, the secured access control is performed with the number of cloud users. The experimental results and the discussions are presented in the next section.

V. DISCUSSION

The experimental results and discussion of the proposed BQ-MES method and existing methods namely SABSC [1] and CLS-PRE [2] are discussed in this section with different parameters such as computational time, computational overhead and data security. The experimental result is compared with two state-of-the-art works based on the two-dimensional graphical representation. For each section, the mathematical calculation is provided showing the performance of the proposed method and the existing two methods.

A. Performance measure of computational time

The first performance metric used to measure the data security in cloud environment is computational time. Computational time though refers to the time consumed in performing certain task, in our work, lower the computational time, more swift the data is said to be stored in cloud and hence, lesser the data being intercepted by unauthorized users. Computational time here refers to the time consumed in performing a specific task. In this work, the computational time refers to the time consumed for establishing system setup and the time consumed for key generation towards data security in cloud environment.

$$CT = D * \{Time\,(f:) + Time\,[private\,key + public\,key]\} \quad (16)$$

From the above equation (16), computational time 'CT' is the summation of the time consumed in establishing the system setup '$f:$' and the time consumed in generating the key '$private\ key + public\ key$' respectively. The sample calculation for computational time using the proposed BQ-MES and existing SABSC [1], CLS-PRE [2] is given below.

Sample calculation for computational time

- **Proposed BQ-MES**: With '20' number of cloud user data to be stored in cloud environment, the time consumed in forming setup being '$0.015ms$' and the time consumed in key generation being '$0.023ms$', the computational time is measured as given below.

$$CT = 20 * [0.015ms + 0.023ms] = 0.76ms$$

- **Existing SABSC**: With '20' number of cloud user data to be stored in cloud environment, the time consumed in forming setup being '$0.018ms$' and the time consumed in key generation being '$0.029ms$', the computational time is measured as given below.

$$CT = 20 * [0.018ms + 0.029ms] = 0.94ms$$

- **Existing CLS-PRE**: With '20' number of cloud user data to be stored in cloud environment, the time consumed in forming setup being '$0.022ms$' and the time consumed in key generation being '$0.034ms$', the computational time is measured as given below.

$$CT = 20 * [0.022ms + 0.034ms] = 1.12ms$$

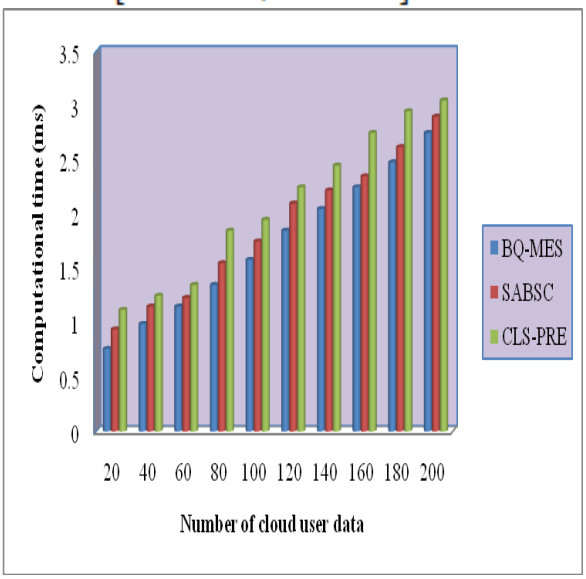

Fig. 3 Convergence graph of computational time

Figure 3 given above shows the convergence graph of computational time with respect to the different numbers of cloud user data. In the above figure, x axis represents the number of cloud user data in the range of 20 to 200 and y axis represents the computational time involved. With higher number of cloud user data involved in data storage, the time involved in private key generation increases. This is because with higher cloud user data, higher mathematical calculations are involved during public and private key generation. Therefore, the computational time involved is also said to be high. However, with the sample calculation given above, with '20' users considered for evaluation, the computational time was found to be '$0.76ms$' using BQ-MES method, '$0.94ms$' using SABSC and '$1.12ms$' using CLS-PRE method respectively. The computational time involved in ensuring data security was found to be lesser using BQ-MES method when compared to [1] and [2]. This is because of the application of Bilinear Setup Mapping. By applying this Bilinear Setup Mapping, fuses components of two vectors spaces resulting in a component of third vector space with linearity found in each of its arguments. With this, mapping between vector spaces is performed in a swift manner, therefore producing private key faster. Therefore, the computational time in ensuring data security is found to be lesser using BQ-MES by 10% compared to [1] and 19% compared to [2].

B. Performance measure of computational overhead

The second metric used in the work to evaluate the amount of data being secured in cloud environment is the computational overhead. Lower the computational overhead, higher is the amount of data being stored in cloud and hence higher is the data secured. Computational complexity here refers to the memory consumed in performing a task. In this work, the computational complexity refers to the memory consumed in establishing system setup and the memory consumed in key generation towards data security in cloud environment.

$$CC = D * \{Mem(f:) + Mem[private\ key + public\ key]\} \quad (17)$$

From the above equation (17), computational complexity 'CC' is the summation of the memory consumed in establishing the system setup '$f:$' and the memory consumed in generating the key '$private\ key + public\ key$' respectively. The sample calculation for computational complexity using the proposed BQ-MES and existing SABSC [1], CLS-PRE [2] is given below.

Sample calculation of computational complexity

- **Proposed BQ-MES**: With '20' number of cloud user data considered for experimentation, memory consumed in establishing the system setup being '$8KB$' and the memory consumed in key generation being '$12KB$', the computational overhead is measured as given below.

$$CC = 20 * [8KB + 12KB] = 400KB$$

- **Existing SABSC**: With '20' number of cloud user data considered for experimentation, memory consumed in establishing the system setup being '$10KB$' and the memory consumed in key generation being '$15KB$', the computational overhead is measured as given below.

$$CC = 20 * [10KB + 15KB] = 500KB$$

- **Existing CLS-PRE**: With '20' number of cloud user data considered for experimentation, memory consumed in establishing the system setup being '$13KB$' and the memory consumed in key generation being '$19KB$', the computational overhead is measured as given below.

$$CC = 20 * [13KB + 19KB] = 640KB$$

Figure 4 given below shows the performance graph of computational complexity. The horizontal axis represents 200 cloud user data to be stored in cloud. The vertical axis represents the computational complexity measured in terms of kilobytes (KB). Higher, the cloud user data to be stored in the cloud, higher is the computational complexity. However, from the simulations conducted with '20' cloud users' data, the computational complexity involved for the BQ-MES method was found to be '400', '500' using SABSC and '640' using CLS-PRE.

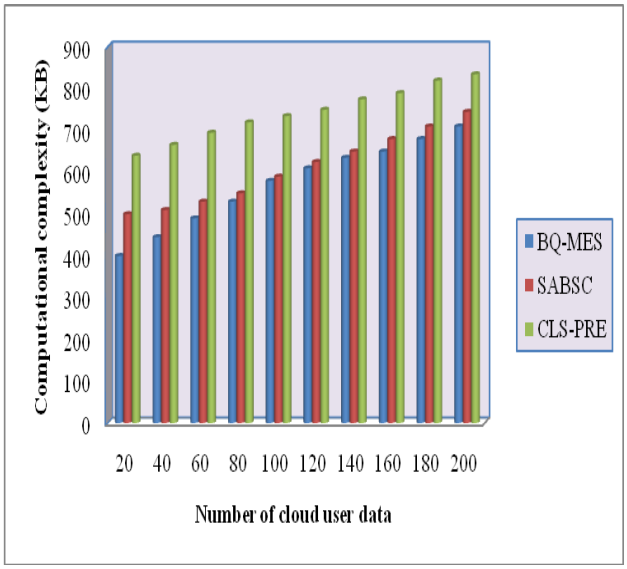

Fig. 4 Convergence graph of computational complexity

From the simulations, it is inferred that the computational complexity involved in data storage is found to be reduced using BQ-MES when compared to SABSC and CLS-PRE. This is because of the reason that minimum CPU usage is said to be occupied using bilinear mapping in the setup phase. Besides as the cyclic group of similar order considered and pairing is somewhat faster and hence, larger number of keys are said to be generated for larger number of cloud user data. Therefore, the computational complexity involved using BQ-MES method is found to be reduced by 6% compared to [1] and 23% compared to [2].

C. Performance measure of data security

Finally, data security in cloud environment is measured. Data in cloud environment is said to be secured if it is resistant to several attacks. There are several certificateless signcryption methods to prevent the data being tampered. Besides, there are several certificateless signcryption methods to test the security of a signcryption technique. In this work, mutual exclusive method is used that forms the ratio of analysis between cloud user's data sent to other cloud users without any modifications to the actual data sent by the cloud user. With this mutual exclusive analysis, the cloud data security 'CDS' is mathematically formulated as given below.

$$CDS = \sum_{i=1}^{n} \frac{CU_i[d_i(wm)]}{CU_i[d_i]} \qquad (18)$$

From the above equation (18), the cloud data security 'CDS', is measured on the basis of cloud users data sent to other cloud users without modification '$CU_i[d_i(wm)]$' to the overall cloud users data sent '$CU_i[d_i]$'. It is measured in terms of percentage (%). The sample calculations for cloud data security for the proposed BQ-MES method, existing SABSC [1] and CLS-PRE [2] are given below.

Sample calculation for cloud data security

- **Proposed BQ-MES**: With '20' cloud user data considered for evaluation, '18' cloud users data sent to other cloud users without modification, the cloud data security is measured as given below.

$$CDS = \frac{18}{20} * 100 = 90\%$$

- **Existing SABSC**: With '20' cloud user data considered for evaluation, '16' cloud users data sent to other cloud users without modification, the cloud data security is measured as given below.

$$CDS = \frac{16}{20} * 100 = 80\%$$

- **Existing CLS-PRE**: With '20' cloud user data considered for evaluation, '15' cloud users data sent to other cloud users without modification, the cloud data security is measured as given below.

$$CDS = \frac{15}{20} * 100 = 75\%$$

Figure 5 given below shows the convergence graph of data security. It is measured in terms of percentage (%). Here, the cloud users send data of different sizes and also at different time intervals. From the figure, it is illustrative that the cloud data security is non-linear. For example, with 20 cloud users sending their data to other end via cloud, the cloud data security using BQ-MES method is found to be 90%, 80% using [1] and 75 using [2]. On the other hand, with 140 cloud users sending their data to other, the cloud data security using BQ-MES method is found to be 87.25%, 78.25% using [1] and 71.45% using [2]. With different sizes and data being sent at different time, the cloud data security is not linear.

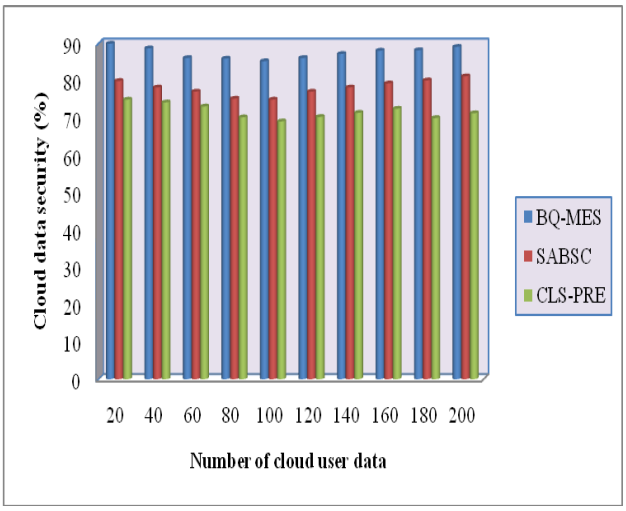

Fig. 5 Convergence graph of cloud data security

However, comparative analysis shows betterment found using BQ-MES when compared to [1] and [2] respectively. This is because of the application of Bilinear Quantum Mutual Signcryption and Unsigncryption. By incorporating Bilinear Quantum Mutual Signcryption and Unsigncryption, key generation is performed via quantum principle. The quantum principle possesses the advantage that it cannot be easily formulated and hence, breaking the quantum value is also found to be highly complicated. The second reason is the application of mutual exclusion probability. By applying this probability measure, only highly probable constraint satisfaction is allowed to extract the data and hence, even modification of the data is not possible. Hence, the data is said to be highly secured as it is in the form of polarized values.

Here, cloud data security is said to be ensured by applying both quantum principle and mutual exclusion probability. As a result, the cloud data security is said to be improved using BQ-MES method by 12 % compared to [1] and 22% compared to [2].

VI. CONCLUSION

In this paper, we first developed a novel Bilinear Setup Mapping model that is computationally efficient ensuring data security in cloud environment. Then, we presented a novel Quantum Public and Private Key Generation model. In the proposed method, cloud data owners interact with the cloud service provided to obtain a signed authorization template via quantum principle, which is then used by the cloud user for retrieval of data. This is done by computing quantum properties like polarization between a cloud data owner and third party private key generation for each session. Finally, the method verifies the authorization via mutual exclusion probability model with respect to both the cloud data owner and cloud user via cloud service provider for granting access. Besides, as data is stored in quantum canonical equilibrium system, the data is said to be secured in cloud environment. The experiment is carried out under the simulation platform, and the simulation results are compared with state-of-the-art methods. The results show that the algorithm used in Bilinear Quantum Mutual Exclusive Signcryption (BQ-MES) method were proved to be computationally efficient and secured than the state-of-the-art methods.

REFERENCES

1. Zhenhua Liu, Yaohui Liu, Yaying Fan, “Searchable attribute-based signcryption scheme for electronic personal health record”, IEEE Access, Oct 2018 (Searchable Attribute Based Sign Cryption – SABSC)
2. Emmanuel Ahene, Junfeng Dai, Hao Feng, Fagen Li, “A certificateless signcryption with proxy re-encryption for practical access control in cloud-based reliable smart grid”, Telecommunication Systems, Springer, Nov 2018 (Certificate Less Signcryption with Proxy Re Encryption – CLS-PRE)
3. Fagen Li, Bo Liu, Jiaojiao Hong, “An efficient signcryption for data access control in cloud computing”, Computing, Springer, Feb 2017
4. Ruhui Ma, Jin Cao, Dengguo Feng, Hui Li, Yinghui Zhang, Xixiang Lv, “PPSHA: Privacy preserving secure handover authentication scheme for all application scenarios in LTE-A networks”, Ad Hoc Networks, Elsevier, Nov 2018
5. Tarunpreet Bhatia, A. K. Verma, “Cryptanalysis and improvement of certificateless proxy signcryption scheme for e-prescription system in mobile cloud computing”, Annals of Telecommunications, Springer, Sep 2017
6. Caixue Zhou, “An improved lightweight certificateless generalized signcryption scheme for mobile-health system”, International Journal of Distributed Sensor Networks 2019, Vol. 15(1), Dec 2018
7. Y. Sreenivasa Rao, “A secure and efficient Ciphertext-Policy Attribute-Based Signcryption for Personal Health Records sharing in cloud computing”, Future Generation Computer Systems, Elsevier, Dec 2016
8. Santosh Chandrasekhar, Ahmed Ibrahim, Mukesh Singhal, “A novel access control protocol using proxy signatures for cloud-based health information exchange “,Computers & Security, Elsevier, Feb 2017
9. Qian Xu, Chengxiang Tan, Zhijie Fan, Wenye Zhu, Ya Xiao, Fujia Cheng, “Secure Multi-Authority Data Access Control Scheme in Cloud Storage System based on Attribute-Based Signcryption “, IEEE Translations and Content Mining, May 2018
10. Fuhu Deng, Yali Wang, Li Peng, Hu Xiong, Ji Geng, Zhiguang Qin, “Ciphertext-Policy Attribute-Based Signcryption With Verifiable Outsourced Designcryption for Sharing Personal Health Records”, IEEE Translations and Content Mining, May 2018
11. Xi-Jun Lin, Lin Sun, Haipeng Qu, “Generic construction of public key encryption, identity-based encryption and signcryption with equality test”, Information Sciences, Elsevier, Apr 2018
12. Fagen Li, Yanan Han, Chunhua Jin, “Certificateless online/offline signcryption for the Internet of Things”, Wireless Network, Springer, Dec 2015
13. Durbadal Chattaraj, Monalisa Sarma, Ashok Kumar Das, “A new two-server authentication and key agreement protocol for accessing secure cloud services”, Computer Networks, Elsevier, Dec 2017
14. Pairat Thorncharoensri, “Policy controlled system with anonymity”, Theoretical Computer Science, Elsevier, May 2017
15. Jing Zhang, Lixiang Li, Yongli Tang, Shoushan Luo, Yixian Yang, Yang Xin, “Secure two-party computation of solid triangle area and tetrahedral volume based on cloud platform”, PLOS ONE | https://doi.org/10.1371/journal.pone.0217067 June 13, 2019
16. Yunchuan Sun, Junsheng Zhang, Yongping Xiong, Guangyu Zhu, “Data Security and Privacy in Cloud Computing”, Hindawi Publishing Corporation International Journal of Distributed Sensor Networks, July 2014
17. Amany AlShawi, “Applying Data Mining Techniques to Improve Information Security in the Cloud: A Single Cache System Approach”, Hindawi Publishing Corporation Scientific Programming, Jun 2016
18. JiaqingMo, Zhongwang Hu, Hang Chen, Wei Shen, “An Efficient and Provably Secure Anonymous User Authentication and Key Agreement for Mobile loud Computing”, Wireless Communications and Mobile Computing, Wiley, Feb 2019
19. Run Xie, Chanlian He, Dongqing Xie, Chongzhi Gao, Xiaojun Zhang, “A Secure Ciphertext Retrieval Scheme against Insider KGAs for Mobile Devices in Cloud Storage”, Security and Communication Networks, Wiley, Jun 2018
20. Shangping Wang, Tingting Gao, Yaling Zhang, “Searchable and revocable multi-data owner attribute-based encryption scheme with hidden policy in cloud storage”, PLOS ONE | https://doi.org/10.1371/journal.pone.0206126 November 1, 2018

AUTHORS PROFILE

Mrs.Kavitha.K pursed Bachelor of Computer Applications from Bharathidasan University, Trichy in 2001 , Master of Computer Applications from Bharathiar University, Coimbatore in 2004 and also pursued Master of Philosophy in Periyar University, Salem in 2005.She is currently pursuing Ph.D in Bharathiar University. She is also currently working as Assistant Professor in Department of Computer Applications, Dr.NGP Arts and Science College, affiliated to Bharathiar University. Her main research work focuses on Cloud Security and Privacy. She has 6 years of teaching experience and 3years of research experience. Internal Communication No. for this paper from my institution : DrNGPASC 2019-20 CS017.

.

Dr. Saravanan V, pursed Bachelor of Science from Madurai Kamarajar University, Madurai in 1994 and Master of Computer Applications from Bharathidasan University, Trichy in 1999 and Mater of Philosopy in Computer Science from Manonmanium Sundaranar University , Tirunelveli in 2002 and Doctorate in Computer Science from Manonmanium Sundaranar University , Tirunelveli in 2016 and currently working as Professor and Head of the Department of Information Technology, Hindusthan College of Arts and Science, Coimbatore, Since 2004. He has published more than 45 research papers in reputed journals International journals and Conferences. His main research work focuses on Networking, DataMining, Image Processing, Cloud Computing and Big Data Analytics, . He has 20 years of teaching experience and 16 yrs of Research experience.

.