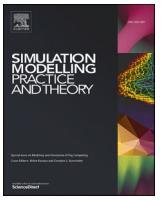
Simulation Modelling Practice and Theory 121 (2022) 102651

Contents lists available at ScienceDirect

Simulation Modelling Practice and Theory

journal homepage: www.elsevier.com/locate/simpat



Modeling and simulation of a novel secure quantum key distribution (SQKD) for ensuring data security in cloud environment

S Sasikumar [a], K Sundar [b,*], C Jayakumar [c], Mohammad S. Obaidat [d], Thompson Stephan [e], Kuei-Fang Hsiao [f]

[a] *Department of Electronics and Communication Engineering, Hindustan Institute of Technology and Science, Tamil Nadu, India*
[b] *Department of computer Science & Engineering, Velammal Engineering College, Tamil Nadu, India*
[c] *Department of computer Science, Rajiv Gandhi Institute of Youth Development (RGNIYD), Ministry of Youth Affairs & Sports, Government of India, Sriperumbudur, Tamil Nadu, India*
[d] *Chair & Professor, Computer Science Department, and Director of Cybersecurity Center, University of Texas-Permian Basin, 4901 E. University Blvd., Odessa, TX 79762, USA, with the King Abdullah II School of Information Technology, University of Jordan, Amman 11942, Jordan and with School of Computer and Communication Engineering, University of Science and Technology Beijing, Beijing 100083, China, Honorary Distinguished Professor, Amity University, Noida, UP 201301, India*
[e] *Department of computer Science & Engineering, M. S. Ramaiah University of Applied Sciences, Karnataka, India*
[f] *Senior Member of IEEE, Computer Science Department, University of Texas-Permian Basin, 4901 E. University Blvd., Odessa, TX 79762, USA*

ARTICLE INFO

Keywords:
Simulation Analysis
Quantum Key Distribution (QKD)
Cloud Data Security
Non-Abelian Encryption (NAE)
Decryption
Quantum Cryptography
Efficiency
Secure Quantum Key Distribution for Cloud Data Security (SQKD-CDS) simulation Model
Modelling

ABSTRACT

In recent days, providing data security over cloud is a complicated process. There are many research works that are developed for authentication based data security over cloud, using cryptographic methods. In contrast, physical rules are used for encrypting data. When the quantum models are appeared, it is called quantum cryptography. And, the key distribution in such models is called, Quantum Key Distribution (QKD). Using QKD in securing data is more effective against several attacks. This paper develops a novel simulation model called Secure Quantum Key Distribution for Cloud Data Security (SQKD-CDS) Model. For encrypting the user data, the simulation model uses Non-Abelian Encryption (NAE) for providing secure data security and, further, the quantum key is used for accessing the stored data from cloud. Moreover, the keys are shared between nodes in secure manner using the quantum channel. This proposed simulation model is evaluated using cloud simulator. The results show that the proposed simulation model outperforms other classical security simulation model in terms of efficiency, time complexity and computational complexity.

1. Introduction

In cloud computing paradigm, the central remote servers and the Internet are used for providing data services. The paradigm allows efficient computing paradigm by efficient storage and memory utilization, centralized processing and bandwidth consumption. Storing

* Corresponding author.
E-mail addresses: drssk75@gmail.com (S. Sasikumar), stephensundarks@gmail.com (K. Sundar), cjayakumar2007@gmail.com (C. Jayakumar), msobaidat@gmail.com (M.S. Obaidat), thompsoncse@gmail.com (T. Stephan), kfhsiao@gmail.com (K.-F. Hsiao).

https://doi.org/10.1016/j.simpat.2022.102651
Received 22 June 2022; Received in revised form 19 August 2022; Accepted 28 August 2022
Available online 29 August 2022

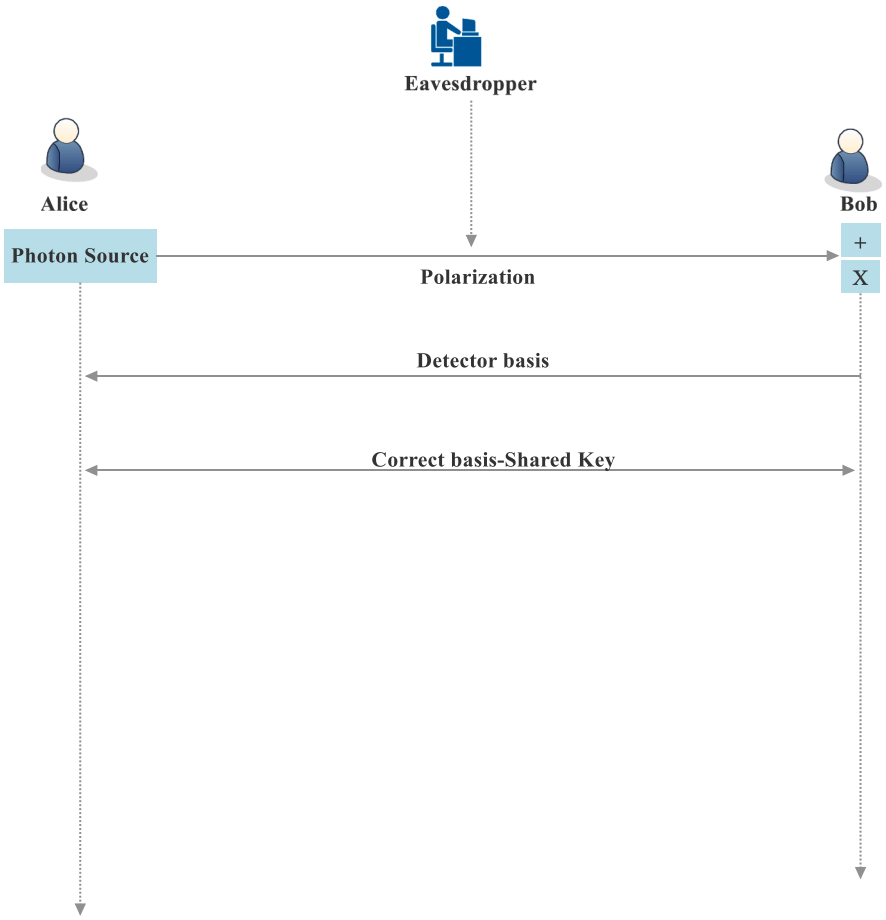


Fig. 1. Quantum Key Distribution Simulation Model.

data on to the cloud makes the processing convenient to handle the problems in hardware management [1]. Many companies are depending on cloud model and services for their daily activities. Moreover, there are Terabytes amount of data that are processed in Cloud for daily processing. Because of the constant enhancements in the operational changes in computing models, there are several significant security challenges that are evolved. The data need to be protected over cloud. In recent days, data breaches are increased and the data confidentiality is exposed in cloud environment. Hence, there is an increasing requirement for data confidentiality [2].

There are many survey works in cloud models, which are developed for balancing the resource demands of large organizations. The resource requirements of organizations include, infrastructure cost, easiness of implementation, faster services of cloud models. The security challenges include:

Data Privacy
Data Confidentiality
Reliability
Data Integrity
Authorization and Authentication

In recent scenario, Quantum Computing and Quantum Key Distribution Protocol (QKDP) is efficient in providing security over cloud data. The objective of QKDP is to perform key distribution function by producing unbreakable encryption and non-interceptable key distribution process [3] [4]. Protecting the data sharing between two entities from unauthorised access is the major concern in cloud. Using Quantum Computing, the data security is completely dependent on the efficient parameters of quantum cryptography, as the QKDP can expose any insecure activities and provide security when the data is transmitted to the encrypted cloud storage. With that concern, Secure QKD simulation model for cloud security is proposed in this work. Fig. 1presents the simulation model of quantum key distribution using the BB84 protocol.

The operations of quantum cryptography lie on the protocol of quantum mechanism for transmission of photons in secure channel. Fig. 1 shows the photon transmission between the BB84 protocol, and between Alice and Bob. The QKDP provides secure technique for key distribution. There are two methods of key distribution in QKD for encryption [5]. It involves in generating the private key from the quantum channel, as the key used is one-time encryption. The distributed keys are hypothetically considered as secure and no traditional techniques are used for the message decryption. In general, there are two types of key authentication:

1.Symmetric Key Authentication:

The two parties share short keys for authenticating the messages that are transmitted between them.

2. Public Key Authentication:

Public key authentication is more efficient than symmetric key technique since the transmitted data are broken and sent in a faster and secure manner [6].

By analysing the security advantages in QKDP in cloud model, the proposed work incorporates Quantum computing for cloud security. This paper utilizes the secret key exchange mechanism for ensuring higher rate of security. And, the contributions of the proposed model are provided below.

The security definitions are provided for clear implementation of the cloud security model

Quantum Key Distribution simulation model is proposed for generating secure keys using the qubits.

Encryption and Decryption operations are processed using the NAE mechanism.

Security Analysis are carried out for evaluating the model performance.

Comparative analysis is carried out for showing the model effectiveness.

The remaining work is organized as follows: Section 2 describes the security related issues and solutions in computing models. The proposed model and work flow are presented and explained in Section 3. The results and comparisons are done in Section 4. The work is concluded in Section 5 with highlighting the model efficiency and future works.

2. Related works

A Multi-party communication model in cloud has been developed in [7]. However, the results are erroneous in authenticating the legitimate users. For ensuring the cloud security, the authors of [8] developed a hybrid model with Quantum Cryptography and Steganography. In [9], QKDP model has been developed for managing the cloud security with minimal time complexities. A new mechanism with Advanced Encryption Standard (AES) with Quantum Computing has been developed in [10]. Furthermore, the authors of [11] developed three-party quantum key distribution and declared that the model is efficient.

In [12], the authors stated that the QKDP model works more efficient than the existing models. The key generation rate has been increased with the spatio-temporal mode of the photons. The work in [13] also developed the QKDP model. The results have shown that the communications are vulnerable to dense-coding attack. The main issue is that the eavesdroppers can obtain the session keys without proper authentication. A new Quantum Computing model has been developed in [14] with pulsed homodyne detection. The model has been proved that the work handles attacks like Trojan-horse and Intercepts-resends in an efficient manner.

A modified QKD model has been proposed in [15] which can be used for secure key distribution. Nevertheless, the model faced a problem called common key reservation. A Device Independent Quantum Key Distribution model has been proposed in [16]. The model is developed, based on the dissimilarities of two entities. The model is robust in handling the loophole attack. Multiple networks are handled effectively in [17] with the developed QKDP model in Wireless Sensor Network (WSN). Using Franson Interferometers, a QKDP model has been proposed in [18]. The results concluded that the model has not provided adequate security.

The authors in [19] presented a new model by combining KP-ABE with equality evaluation of public key encryption model. The model permits authorized users to perform security operations. The model generated security against several cipher text attacks. Fuzzy- Identity based Encryption (Fuzzy IBE) model has been proposed in [20]. Here, the identity has been defined as the collection of significant attributes. Multi-Authority based model definition has been given as the future enhancement of the work. Based on the actual and non-interactive cryptographic considerations, the CP-ABE has been provided in [21]. The model provided solution with exact definition of access control using attribute-based formula definitions. The model is also defined with four phases: setup phase, key generation operations, encryption process and decryption process.

The authors in [22] developed a CP-ABE based hidden access policy model that provides a role based access control model. The model used Inner Product Encryption (IPE) model for securing the access structure and user data from CSP.

The work presented in [23] developed two different models:

CP ABE using AND gate that utilizes a wild-card access policy, which provides standard ciphertext, without hiding the access policy

Secondly, IPE has been incorporated for hiding the access policy with effective decryptors.

The model is presented in [24] to secure both the private credentials and sensitive data. Further, the model comprised of two parts:

Data sharing has been processed with homomorphic encryption, which protects the data from offline attacks

The second section contains the scrambled circuit that analyzes the overall access policy.

Moreover, the polynomial time is needed for defining simple policies and exponential time for supporting different access rates with random complex values. Lightweight Data Sharing Model [25] developed with anonymous authentication to shorten the access control patterns, and user authenticity as well as to support the reframing process of decryption key. Here, anonymous authentication has been used to provide exact authorization data and key sharing to the appropriate data owner, whose data are matched with that.

A survey paper on cloud security is presented in (Alouffi et. A, 2021) state that there are seven significant security vulnerabilities to cloud services. Data tampering and breach were among the most frequently addressed issues in the selected literature, according to the findings. Other discovered security vulnerabilities in the cloud computing system were linked with data invasion and data storage. The findings also suggested that outsourcing consumer data remained a problem for both CSPs and cloud users. The study paper recognized blockchain as a complementary tool for addressing security issues. Data confidentiality, data integrity, and data accessibility are bolstered by the work's recommendations for future projects.

The authors (Wang et Al. 2021) provided the PDP model with the following three securities needs can be met with:

(1) The data security of the acquired firm can be ensured

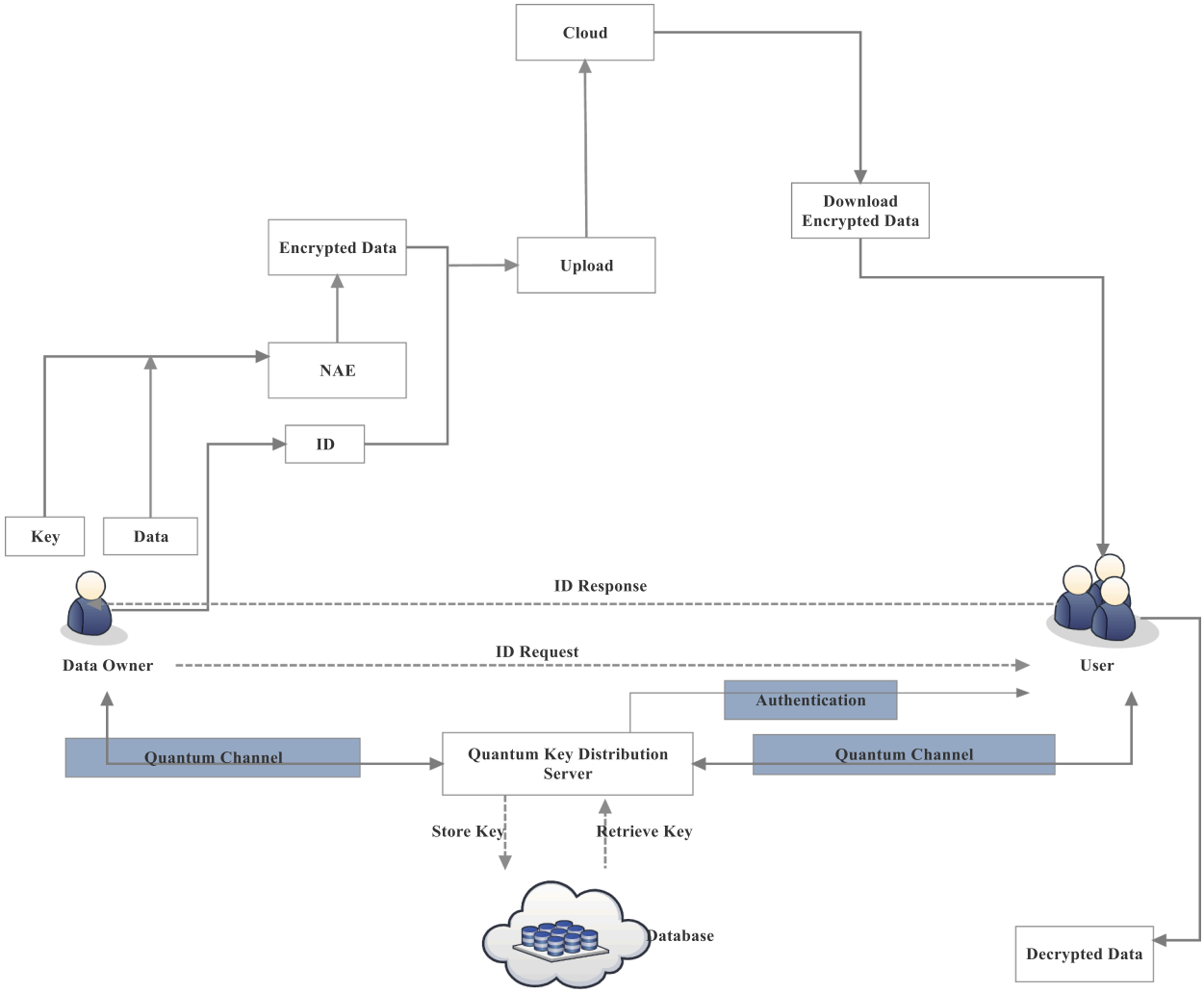


Fig. 2. Work Flow of Proposed Simulation Model.

(2) The bought data's integrity and confidentiality can be ensured,
(3) The acquired data's confidentiality can be ensured.

3. Proposed simulation model

The objective of the proposed Simulation model is to provide security to the shared data on cloud by securing the process of key sharing, using efficient encryption and decryption methods. The proposed simulation model is called as Secure Quantum Key Distribution for Cloud Data Security (SQKD-CDS). For encryption, Non- Abelian Encryption (NAE) is used here. The work flow is presented in Fig. 2, which includes, secret key generation, data encryption, data decryption and secure key sharing. Initially, the users are properly registered for providing authentication.

In this paradigm, the user records are maintained by the administrators and responsible for providing restricted access to the consumers based on their requirements. The qubits are transmitted to the users and based on that the quantum key is generated for data access. The data to be deployed in the cloud is encrypted with NAE encryption technique and stored on to the cloud server. The key used for encrypting the user records to store in cloud is transmitted through the quantum channel to the authorised consumer. The QKDP (Quantum Key distribution Protocol) is used for secure key exchange between the Data owner and the Authorised User. QKDP incorporated the basic Quantum principles of No cloning and Uncertainty. The secure key transmission through Quantum channel is secure Quantum key distribution simulation Model. This model ensures the secure key sharing . When the requests are obtained from the consumers, the signature generation is processed using the hash function. When the signature match is found, the data is provided from the service provider.

3.1. Security definitions

In order to show the security of Quantum Key Distribution, security definition is required to be given initially. A security key is defined in such a manner to satisfy the following requirements. the key bit strings are to be indistinguishable the strings are to be equally distributed

Because of some practical problems, such as the size of data and error corrections, ideal keys are not generated by the entities. In reality, some scale of failure rate is allowed in key determination process. Moreover, with some E_{cor} and E_{sec}, correct and secret error, the QKDP is considered as more secure as, *E-secure* which is determined as, $E_{cor} + E_{sec}$.

The key bit strings for Alice and Bob is given as, K_{Al} and K_{Bb} with same length 'l', respectively. The secret key is connected with the quantum state β_E, assumed by Eve. The joint state of secret key of Alice, Bob, and Eve is given as:

$$\beta_{Al,Bb,E} = \sum_{K_{Al},K_{Bb}} \Pr(K_{Al}, K_{Bb}) |K_{Al}K_{Al}| \otimes |K_{Bb}K_{Bb}| \otimes \beta_E^{(K_{Al},K_{Bb})} \tag{1}$$

Where, $K_{Al}, K_{Bb} \in \{0,1\}^l$ denotes the bit rates.

A QKDP is defined to beE_{cor}, if the probability distribution, $\Pr(K_{Al}, K_{Bb})$ and the final state $\beta_{Al,B\rho,E}$is computed as:

$$\Pr(K_{Al} \neq K_{Bb}) \leq E_{cor} \tag{2}$$

A QKDP is defined to be E_{sec}, if the state is nearer to the private state's of the single entity. And, it is given as,

$$\min_{\beta\pi} \frac{1}{2}(1 - \beta_{abort}) \parallel \beta_{Al,E} - \beta_{Al,E}^{ideal} \parallel 1 \leq E_{\text{sec}} \tag{3}$$

Where, 'β_{abort}' denotes the abort state probability. The secure quantum state created between Alice and Bob is $\beta_{Al,\,E}$ and the ideal state may cause the secret changes in the transmission is defined to be $\beta_{Al,\,E}^{ideal}$ .The security definition consists of the security property that is turned out from the trance distance.

3.2. Work flow

In the proposed model, the data from client side is encrypted using Non-Abelian Encryption (NAE) using Quantum Key Distribution. After encrypting and sharing the data on to the cloud, the data can be accessed by the authenticated users, who require the certificate from the data owner to provide the secret key from QKDP via the quantum channel. The decryption is performed after downloading the shared data from the cloud. Further, the workflow of the proposed simulation model is presented in Fig. 2.

Quantum Cryptography performs based on the quantum law of mechanics for photon transmission to the receiver through secure channel. Heisenberg's uncertainty principle is the familiar law of quantum technique, which avoids the unknown to measure the qubits in an effective manner. This states that the eavesdropper cannot acquire or duplicate the photon or manipulate. As mentioned before, between Alice and Bob, a photon is used for secret key transmission and the coding and decoding operations are performed further. In QKDP, the photons are converted into binary values, where they denote one part of data as 0 and 1. Moreover, the polarization states of the photons are given as,

Vertical Spin (|)
Right Diagonal Spin (/)
Horizontal Spin (−)
Left Diagonal Spin (\)

The first two spins are denoted with '1′ and the remaining two are represented with '0′. Alice can perform all the above operations and Bob can perform operations such as, ' + ' and ' × '.

For an instant, 10010010 is the binary code, corresponding to the key, assigned to each photon. The key is transmitted by Alice to Bob, as photon, in random selection manner through the secure quantum channel. The polarized photons are received at the other end, by Bob, and the computations are carried out using, ' + ' and ' × ' operations. As the receiver has no information about the photon polarization of the sent data, the receiver will make a guess, based on the interpretation of bit sequences. Then a secret conversation is made between the sender and receiver, where, the photon measurements are not discussed in order to avoid the third-party intrusions.

For example, Alice sends a Right Diagonal Spin (/) based photon and then it may change into Vertical Spin (|), while crossing the quantum channel. After that, the photon computations are processed using, ' + ', makes Alice to discard the photon. Nevertheless, when the photon is found to be unchanged, then " × " operation is done. It denotes that Alice says there is no change occurred and the process continues to determine the secret key. The photon polarization will be changed, only when it is found that eavesdropping has occurred. Hence, the attack can be detected during the public conversation of two entities. Further, the exact key sequence is determined and shared. When the key sequence is found to be correct, the secret key is dropped by the two entities and another key is generated.

For verifying the secret key between Alice and Bob, it can be determined with the Quantum Bit Error Rate (QBER). The equation is presented in (4).

$$QBER = \frac{NB_{wrong}}{NB_{total}} \tag{4}$$

Table 1
Pseudocode for Encryption and Decryption using Non-Abelian Group

Begin
Select Large Positive Integers l, m, n
$n = (l, m) > 1$
Declare Non-Abelian Group (G) as Public
Declare integers l, m, n as public
Derive message
$M = a^{\rho} b^{\sigma} c^{\omega} \in G$ (6)
Where, $0 \le \rho \le l$, $0 \le \sigma \le m$, $0 \le \omega \le n$
Select large odd prime 'α' such that, (s_0, t_0) is the least positive integer
Define ${t_0}^2, {s_0}^2 = 1$
Declare s_0, aas private
Declare t_0 as public
//Compute Encryption Process
$Enc_G^M = (a^{\rho} b^{\sigma} c^{\omega})^{{t_0}^2} \in G$ (7)
$a^{\rho'} b^{\sigma'} c^{\omega'} = Enc_G^M = (a^{\rho} b^{\sigma} c^{\omega})^{{t_0}^2} \in G$(8)
Where, $\rho' = \rho {t_0}^2 (\bmod l)$
$\sigma' = \sigma {t_0}^2 (\bmod m)$
$\omega' = \left(\frac{{t_0}^2({t_0}^2 - 1)}{2}\right)\rho\sigma + {t_0}^2\omega (\bmod n)$
//Compute Decryption Process
Using private keys s_0, α, compute
$(a^{\rho'} b^{\sigma'} c^{\omega'}) \otimes (a^{\rho} b^{\sigma} c^{\omega}) - a{s_0}^2 (\bmod G) = a^{\rho} b^{\sigma} c^{\omega}$ (9)
End

Where, 'NB_{wrong}' denotes the number of wrong bits and 'NB_{total}' represents the total number of bits. The results are evaluated by comparing them with maximal error level in order to detect the presence of eavesdroppers. When the bit error rate is found to be greater than the maximal error rate, the communication is concluded as not secure and it will be stopped. The communication process will be started again from the initial level. Hence, the QKDP provides a secure way of key sharing and secures the shared data over cloud.

Here, the cloud admins and the users utilize the quantum key for secure data storage, sharing and access. Moreover, the quantum key is framed based on the qubits, which can be further used for encryption and decryption operations. Moreover, in the proposed model, for authentication purposes, one-time password is generated for both the owner and user for accessing the shared data from cloud. When the user requires the data, the owner transmits the qubits, based on that; the strings are framed and forwarded to the owner.

When the authentication is done, and found that the user is a trusted one, the key is utilized for the encryption and decryption functions in both sides. The Quantum key distribution is mainly used for the enhancement of secure data transmission over cloud.

3.2.1. Generation of secret key

Once the private key is generated and distributed, the secret key is generated by the administrator using Diffie-Hellman algorithm. It is mainly used for accessing the data from cloud. It is also used for creating the access policy to control the data utilization. Here, mutual authentication is provided with the D-H algorithm. Moreover, this model does not require conditions for key sharing and storage. Further, the model allows two different entities to frame the key without knowing themselves, previously. Thus, the admin and the users are provided with the key and access policy data, maintained by the Trusted Server.

3.2.2. Data encryption and decryption using non-Abelian encryption

When the secret key is generated, the original data is divided into multiple segments and encrypted with the Non-Abelian Encryption. A non-cumulative group is framed initially and the sub segments are generated. The private key is generated based on the master key, which is the generated quantum key, based on the NAE property. Accordingly, the public key is computed and transmitted to the other entity for decryption. The property is the group of non-Abelian is, the element pair a and b,

$$ab \neq ba \forall a, b \in G \tag{5}$$

During the encryption process, the hash rate for the private key is determined. Further, the ASCII values for the divided segments are computed and $\oplus$ operation is performed. Based on that, the cipher text is generated. Further, the cipher text is transmitted to the different cloud servers. The divided segments are decrypted using the Non abelian decryption method. At the receiver side, signature verification is done. When it is verified, the decryption process is performed.

For that, the exact signature is generated for the data from different cloud servers. Using the quantum key, the private key is computed. Further, the data owner forwards the public key. With the received key, the segments are individually decrypted at the receiver end and combined to frame the shared data. The pseudocode for encryption and decryption based on Non-Abelian Group is given in Table 1.

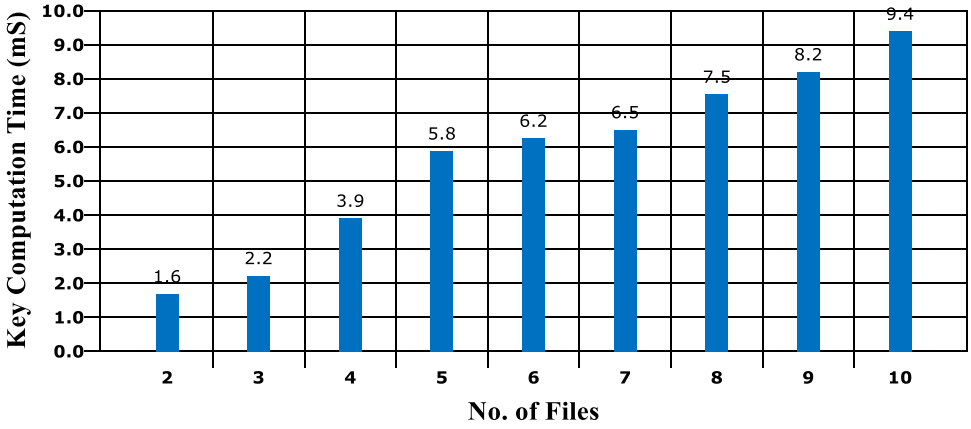


Fig. 3. Computation Time.

3.3. Security analysis

There are many attacks that can occur against the Quantum Key Distribution including:(a) man-in-the-middle attack and (b) denial-of-service attack

In the man-in-the middle attack, which occurs between the two communication entities, the eavesdropper develops a pair of QKD entities, alike the legitimate entities. It interrupts the quantum channel connecting the two elements. The eavesdropper links the devices to the quantum's vulnerable ends. Further, two independent QKD sessions are launched for both entities, where the attacker tries to act like Bob or Alice. At the end, the attacker shares a different key for the entities. Hence, Alice sends the cipher data to Bob, the attacker can acquire the message and perform decryption. After that, the content can be manipulated and sent to the other entity. By using, QKDP, the activity of the attacker can be resisted and the eavesdropper cannot process with the attack.

The denial-of-service attack in Quantum Key Distribution can be done in two process: (a) compromising the hardware of Quantum Cryptography, and (b) providing additional noise to the Quantum Model

Quantum model that uses the optical fibers for communication may become out of service, when there is a physical damage. Moreover, the denial-of-service attack for the channel is not processed in quantum channel, since, when there is more than one link between the two entities. The entities are capable of sharing the secret key with the remaining network that is not changed by the attacker.

4. Results and discussions

The proposed simulation model is evaluated using CloudSim tool and the results are compared with the previous works such as, Quantum Cryptography based Cloud Security Model (QC—CSM) and Enhanced Cloud Security Model using Quantum Key Distribution Protocol (ECSM-QKDP). CloudSim is a simulation toolkit that allows you to model and simulate cloud basic functionalities. Support for large-scale computing environments such as integrated cloud data centers, virtualized server hosts, and customized policies for distributing host resources to virtual machines, as well as energy-aware computational resources. It is a stand-alone platform for simulating cloud service brokers, availability, and policy allocation. It allows network connections between simulated system pieces to be simulated. Support for simulating a federated cloud environments in which resources from both the private and public domains are interconnected. Moreover, the results are evaluated based on the metrics such as, computation time, time taken for key generation, storage efficiency, encryption and decryption time. In addition, for evaluation, the maximum number of files are taken as, 500 and the maximum file size is considered as 400 kb. The performance of SQKD is compared with the other competing models, QC—CSM and ECSM-QKDP and evaluated.

4.1. Computation time

Here, computation time is defined as the time taken for execution of the cloud storage and access model. Moreover, it is the total amount of time taken by the cloud model for data storage of cipher text and data access from the server. The results for the computation time are depicted in Fig. 3. The computation time taken for the proposed model is effectively reduced by splitting the data into segments.

4.2. Key generation time

Key generation time is the time taken for generating the quantum key by utilizing qubits. In this process, the evaluations are carried out with the increasing number of files. The key is further used for encryption and decryption function. The obtained results are provided in Table 2 and the corresponding comparison graph is presented in Fig. 4. The key generation time of the proposed model is

Table 2
Results obtained for Key Generation Time Analysis.

Models	Key Attribute				
	10	20	30	40	50
QC—CSM	**10.6**	**14.6**	**17.5**	**23.5**	**28.8**
ECSM-QKDP	**12.5**	**21.4**	**27.8**	**28.1**	**35.8**
SQKD	**4**	**8**	**13.5**	**18.5**	**25.2**

Models	Key Attribute				
	10	20	30	40	50
QC-CSM	10.6	14.6	17.5	23.5	28.8
ECSM-QKDP	12.5	21.4	27.8	28.1	35.8
SQKD	4	8	13.5	18.5	25.2

Fig. 4. Key Generation Time Analysis.

Table 3
Results Obtained for Time based Analysis.

Number of Files	20	40	60	80	100
Encryption time of QC—CSM	**21.1**	**26.1**	**26.9**	**30.2**	**38.3**
Decryption time of QC—CSM	**14.6**	**17.3**	**19.3**	**23.0**	**36.6**
Encryption time of ECSM-QKDP	**8.8**	**9.7**	**12.7**	**15.1**	**18.3**
Decryption time of ECSM-QKDP	**5.1**	**7.0**	**9.1**	**10.0**	**12.8**
Encryption time of SQKD	**3.1**	**3.4**	**4.0**	**5.1**	**7.5**
Decryption time of SQKD	**1.6**	**2.0**	**2.3**	**2.6**	**3.9**

considerably reduced using the efficient cryptographic mechanisms; here the model attained 13.84 secs. From the graph, it can be observed that the proposed simulation model generates keys in minimal time than the compared models.

4.3. Encryption and decryption time analysis

In this, encryption time is the total time taken for the process of performing data encryption using NAE algorithm. It is shown from the results that the time of encryption is considerably increased based on the data size. Further, the decryption time is measured with the time taken for decryption. The results and values are provided in Table 3. Further, the comparative analysis is given in Fig. 5 for all three models. From the results, it can be clearly observed that the proposed model requires minimal time for encryption and decryption. Hence, time complexity is effectively reduced in the proposed model. Moreover, Table 4 and Fig. 6 display the results obtained for overall processing time-based evaluations. The results portray that the proposed simulation model utilizes minimal time than other compared previous models with the efficient implementation of QKDP with NAE.

4.4. Storage efficiency

Storage Efficiency is an important factor in cloud security. Besides, the evaluation results here are provided in Table 5 and comparisons are depicted in Fig. 7. It is explicit from the results that the proposed model utilizes minimal storage than competitive related previous works. The average memory utilization of the proposed model is calculated as, 48.303 KB, which is the lowest among all other competing models.

5. Conclusion and future work

In this paper, security of the QKDP simulation model using quantum mechanism is used for cloud security. The simulation model uses Non-Abelian group-based encryption and decryption model for enhancing the data security. Moreover, the generated keys are shared between entities through the quantum channel, which is considered to be highly secure. The original data from the owner is divided into a number of segments and stored in multiple servers using the proposed Simulation model. The service provider provides the data to the user, based on their corresponding access policies with the signature. Further, the signature is verified and the decryption operations are performed. Moreover, at the user side, the decrypted data are combined to form the original data. The results show that the overall Simulation model performance and security is effectively increased with minimal time complexities and processing time. The Quantum Key distribution protocol applies No cloning and Heisenberg Uncertainty principles which ensures the security in this simulation model. The security in the key exchange is improved through this model.

In future, the simulation work can be implemented in real-time environment and evaluated for security. The enhancement can also

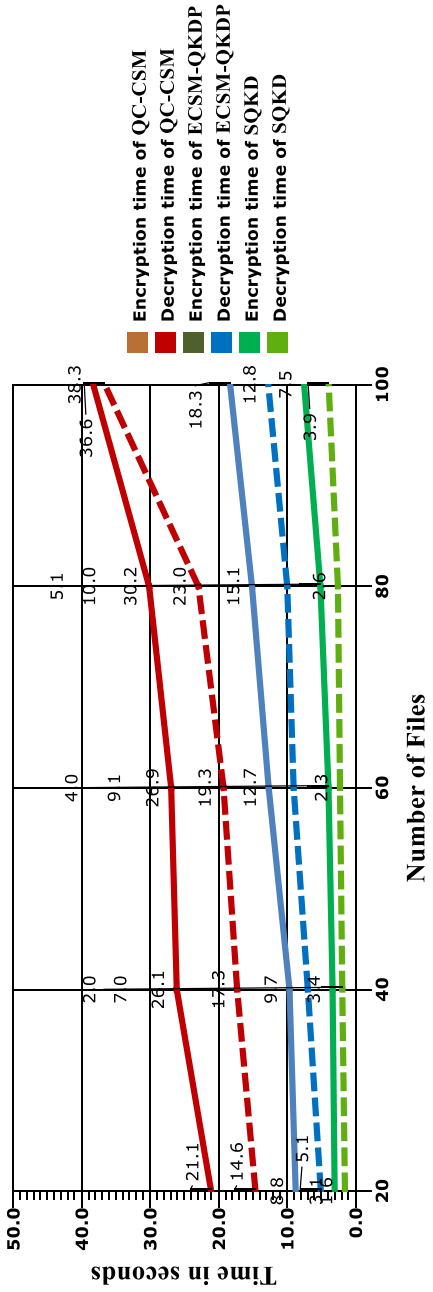


Fig. 5. Encryption and Decryption Time Comparisons.

Table 4
Values obtained for Time based Analysis.

Models	100(kb)	200(kb)	300(kb)	400(kb)
QC—CSM	**13.08**	**12.81**	**14.33**	**13.05**
ECSM-QKDP	**17.49**	**19.44**	**17.28**	**18.88**
SQKD	**4.49**	**4.44**	**6.26**	**8.01**

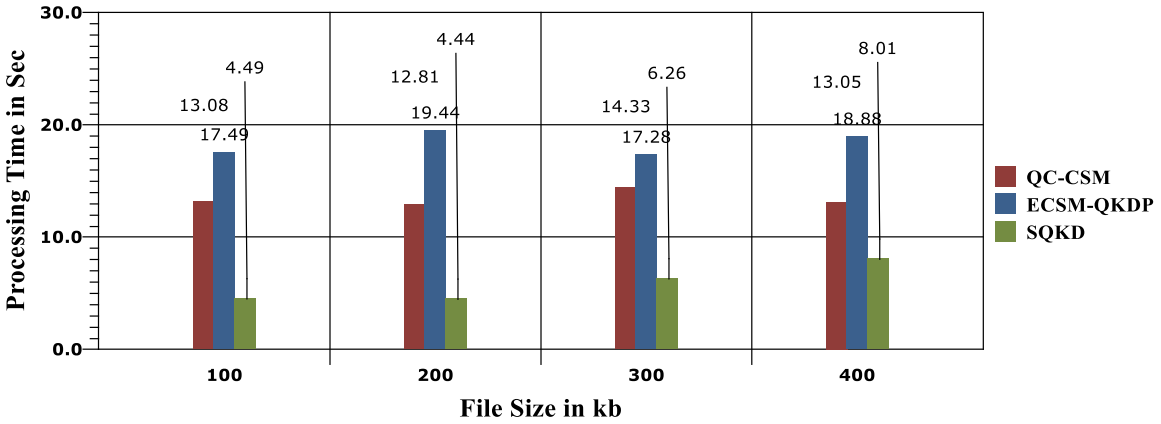


Fig. 6. Processing Time Vs File Size.

Table 5
Results Obtained for Storage Analysis.

Models	100(kb)	200(kb)	300(kb)
QC—CSM	**74.32**	**195.05**	**221.87**
ECSM-QKDP	**64.35**	**133.41**	**245.98**
SQKD	**34.98**	**96.62**	**138.31**

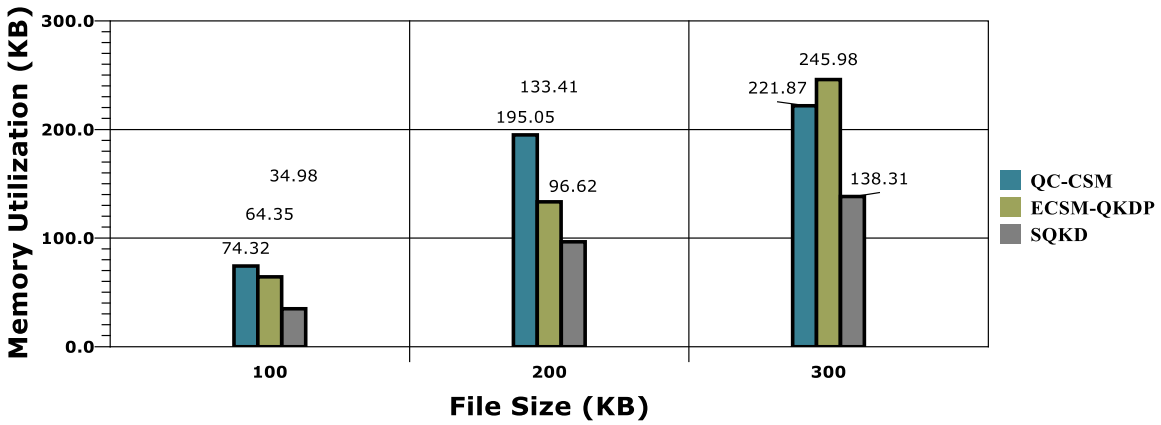


Fig. 7. Memory Utilization Vs File Size.

be done with big data processing in cloud with high security.

Data availability

The authors do not have permission to share data.

CRediT authorship contribution statement

S Sasikumar: Conceptualization. **K Sundar:** Conceptualization, Writing – original draft, Methodology, Data curation, Formal analysis. **C Jayakumar:** Investigation, Supervision. **Mohammad S. Obaidat:** Investigation, Supervision, Project administration. **Thompson Stephan:** Supervision, Writing – review & editing. **Kuei-Fang Hsiao:** Supervision, Validation, Software.

References

[1] A.J. Gabriel, B.K. Alese, A.O. Adetunmbi, O.S. Adewale, Post-quantum cryptography basedsecurity framework for cloud computing, J. Internet Technol. Secured Trans. vol.3 (no.4) (2014) 344–350.
[2] L. Sim, S. Ren, S. Keoh, K. Aung, A cloud authentication protocol using one-time pad, in: IEEE Region 10 Conference (TENCON), Singapore, 2016, pp. 2513–2516.
[3] C.C.W. Lim, C. Portmann, M. Tomamichel, R. Renner, G. Nicolas, Device-Independent Quantum Key Distribution with Local Bell Test, Am. Phys. Soc. (2013) 1–11.
[4] A. Abduvaliyev, A.-S. Pathan, J. Zhou, R. Roman, W.-C. Wong, On the vital areas of intrusion detection systems in wireless sensor networks, IEEE Commun. Surv. Tutor. 15 (3) (2013) 1223–1237.
[5] K.G. Paterson, F. Piper, R. Schack, Quantum cryptography: a practical information security perspective, Nato Secur. Through Sci. Ser. D-Inf. Commun. Secur. 11 (2007). Vol.
[6] D. Zhu, X. Li, J. Wu, A quantum key-based mobile security payment scheme, Int. J. Perform. Eng. Vol. 15 (8) (2019) 21–65.
[7] Z.A. Zukarnain, R. Khalid, Quantum key distribution approach for cloud authentication: enhance tightnite key, in: International conference on Computer Science and Information Systems (ICSIS'2014), Dubai, UAE, 2014, pp. 28–33.
[8] A.J. Gabriel, B.K. Alese, A.O. Adetunmbi, O.S. Adewale, Post-quantum cryptography based security framework for cloud computing, J. Internet Technol. Secured Trans. vol.3 (no.4) (2014) 344–350.
[9] R. Khalid, Z.A. Zukarnain, Cloud computing security threat with quantum key distribution defense model, in: Proc. of the 3rd International Conference on Green Computing, Technology and Innovation (ICGCTI2015), Malaysia, 2015, pp. 49–54.
[10] G. Sharma, S. Kalra, A novel scheme for data security in cloud computing using quantum cryptography, in: Proc. of the International Conference on Advances in Information Communication Technology & Computing, Bikaner, India, 2016.
[11] H. Shih, K. Lee, T. Hwang, New efficient three-party quantum key distribution protocols, IEEE J. Sel. Top. Quant. Electron. vol.15 (2009) 1602–1606.
[12] J.S. Cotler, P.W. Shor, A New Relativistic Orthogonal States Quantum Key Distribution Protocol, Arxiv (2016) 1–6.
[13] F. Gao, S.-J. Qin, F.-Z. Guo, Q.-Y. Wen, Dense-Coding Attack on Three-Party Quantum Key Distribution Protocols, IEEE. Vol. 10 (10) (2010) 1–6.
[14] W.A.N.G. Chuan, W.A.N.G. Wan-Ying, A.I. Qingand LONG Gui-Lu, Deterministic Quantum Key Distribution with Pulsed Homodyne Detection, Vol. 53, Chinese Physical Society and IOP Publishing Ltd, 2010, pp. 67–70.
[15] G. Zeng, X. Wang, Quantum key distribution with authentication, Natl. Key Lab. (2010) 1–15. Pp.
[16] C.C.W. Lim, C. Portmann, R.R. MarcoTomamichel, NicolasGisin, Device-Independent Quantum Key Distribution with Local Bell Test, American Physical Society., 2013, pp. 1–11.
[17] X. Huang, S. Wijesekera, D. Sharma, Agent-Oriented Novel Quantum Key Distribution Protocol for the Security in Wireless Network, Intechopen (2009) 261–277.
[18] T. Brougham, S.M. Barnett, K.T. McCusker, P.G. Kwiat, D. J.Gauthier, Security of high-dimensional quantum key distribution protocols using Fransoninterferometers, Dep. Phys. (2009) 1–14.
[19] H. Zhu, L. Wang, H. Ahmad, X. Niu, Key-Policy Attribute-Based Encryption with Equality Test in Cloud Computing, IEEE Access 5 (2017) 20428–20439.
[20] A. Sahai, B. Waters, Fuzzy Identity-Based Encryption, in: Advances in Cryptology- EUROCRYPT, Lecture Notes in Computer Science, 3494, Springer, Berlin, Heidelberg, 2005, pp. 457–473.
[21] B. Waters, Ciphertext-Policy Attribute-Based Encryption: an Expressive, Efficient, and Provably Secure Realization", Public Key Cryptography, in: Lecture Notes in Computer Science, 6571, Springer, Berlin, Heidelberg, 2011, pp. 53–70.
[22] P.A. Patil, S. Patil, S. Joshi, Hidden CP-ABE to Enhance Patient Data Privacy in Smart Healthcare Systems, Int. J. Appl. Eng. Res. 12 (13) (2017) 3950–3960.
[23] T.V.X. Phuong, G. Yang, W. Susilo, Hidden Cipher-text Policy Attribute-Based Encryption under Standard Assumptions, IEEE Trans. Inf. Forensics Secur. 11 (1) (2016) 35–45.
[24] K. Frikken, M. Atallah, J. Li, Attribute-Based Access Control with Hidden Policies and Hidden Credentials, IEEE Trans. Comput. 55 (10) (2006) 1259–1270.
[25] X. Yao, H. Liu, H. Ning, L.T. Yang, Y. Xiang, Anonymous Credential-Based Access Control Scheme for Clouds, IEEE Cloud Comput. 2 (4) (2015) 34–43.