IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Revue d'Intelligence Artificielle
Vol. 33, No. 1, February, 2019, pp. 33-37
Journal homepage: http://iieta.org/journals/ria

IBLIND Quantum Computing and HASBE for Secure Cloud Data Storage and Accessing

Kranthi Kumar Singamaneni*, Pasala Sanyasi Naidu

Department of CSE, GITAM Institute of Technology, GITAM Deemed to be University, Vishakhapatnam, India

Corresponding Author Email: kkranthicse@gmail.com

https://doi.org/10.18280/ria.330106

Received: 2 October 2018
Accepted: 13 January 2019

Keywords:
cloud storage, Blind quantum computing, cloud service provider, cloud users

ABSTRACT

Cloud computing is a universal conventional system. With the exponential development of cloud data and storage room, cloud security has turned out to be one of the intriguing exploration regions of cloud registering servers. Property based encryption is an open key encryption calculation that permits cloud users to anchor their delicate data in the general population cloud servers. Credited based Quantum cryptography will anchor the user data transmission and correspondence through cloud frame programmers. Be that as it may, daze quantum registering will anchor the moment spying or getting to of data handling in cloud from any awful cloud provider or outsider. In this paper we proposed an algorithm based on blind quantum computing for to secure the communication between data owner and CSP. And enhanced the hierarchal attribute-based encryption algorithm using BCQ key sharing which provides user data providing and group accessing of cloud data. The experimental results show that the proposed mechanism is efficient than the existing CP-ABE enhancements.

1. INTRODUCTION

For almost as long as programmable computers have existed, there has been a solid inspiration for clients to run figurings on equipment that they don't by and by control. At first, this was because of the surprising expense of such gadgets combined with the requirement for specific offices to house them. Colleges, government offices and substantial enterprises housed PCs in focal areas where they ran employments for their clients in clumps.

After some time, PCs have turned out to be universal, however interest for unified assets has not subsided. Indeed, even today, the utilization of appointed calculation is far reaching, as cloud figuring [1]. While we don't yet know how the field of quantum processing will create, it appears to be sensible to theorize that it will take after a comparative way. Undoubtedly this theory is to some degree borne out by

ongoing endeavors to give access to simple quantum processors over the Internet [2].

Today we are in an obviously better position to empower remote access to quantum PCs than was conceivable with early customary PCs, because of the presence of fast worldwide interchanges systems, and the omnipresence of traditional processors. Besides, the disclosure of quantum key circulation conventions has given the impulse to create quantum correspondence over existing optical fiber systems [3]. These components just serve to expand the degree for early reception of appointed quantum calculation.

While the choice of assigning figurings to remote frameworks may have solid down to earth and financial inspiration, it opens a heap of security concerns [4]. Specifically, if the calculation is performed on untrusted equipment, at that point this opens the likelihood that either the protection or the trustworthiness of the calculation might be endangered. Encryption can be utilized to conceal correspondence between the customer and the server from busybodies, while confirmation codes can be utilized to recognize any endeavor to change these messages [5]. In any case, such methods do nothing to balance the danger postured by a bargained or vindictive server.

In a perfect world, to defeat these worries, one would need an approach to appoint undertakings to a remote server while guaranteeing security, even from the server executing them, and to guarantee the accuracy of the outcome [6].

The cloud figuring storage room is completed by the customers' demand. The customers can get to their out sourced data from cloud server at whatever point. From most recent couple of years, monstrous measure of information is re circulated in cloud figuring information stockpiling free of their beginning stage and nature [7]. The security and assurance of those data has transformed into our prime concern.

To decide this issue of assurance and security, various cryptographic computations are delivered. Cloud security can be described as the route toward scrambling a message to an encoded outline and unscrambling it by the endorsed clients. By completing an ensured and advanced cryptographic count, extended security can be added to the fragile data appear in cloud servers [8].

Tragically, the outsourced information is not inside the controlling extent of data proprietors. These data can be simply controlled by cloud specialist co-ops. In any case, daze quantum figuring will anchor the moment listening in or getting to of information preparing in cloud from any horrible cloud supplier or outsider.

Figure 1 shows the basic cloud architecture and the storage space and how the data owner, CSP and cloud users communicate among them self's. As of late, various conventions have risen which try to handle the protection issues raised by assigned quantum calculation.

Going under the wide heading of visually impaired quantum calculation (BQC), these give a route to a customer to execute a quantum calculation utilizing at least one remote quantum

servers while keeping the structure of the calculation covered up. While the objective of BQC conventions is to guarantee just the protection of the calculation, numerous likewise take into account check of the calculation being performed, by inserting shrouded tests inside the calculation [9].

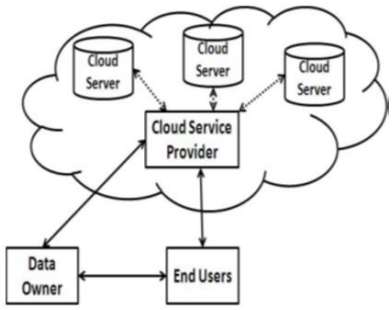

Figure 1. Cloud architecture

To date, BQC has been considered in an extensive variety of settings, with changing necessities on the capacity of the customer and the server or servers. At last, the most attractive setting would be an unquestionable BQC convention which could be performed between a customer with no quantum capacities and a solitary quantum server [10].

Shockingly, advance on such a convention has demonstrated moderate. Some portion of the trouble is that the server could hold an entire transcript of the correspondence amid the convention, enabling them to rerun their side of the procedure ordinarily [11].

In this, paper we introduced a convention which depends on BCQ, it can accomplish the better method for anchoring from listening in and furthermore gives the honesty of the information, this convention is significantly usefull in the middle of the correspondence of cloud client and CSP [12].

We are proposing another technique to improve the HASBE which is to be between the clients and the information proprietors that is it can accomplish secure gathering correspondence and furthermore give protection of client. Whatever is left of the paper is sorted out as takes after. Area 2 shows the far reaching view about the current writing, segment 3 talk about the proposed components, segment 4 displays the trial assessment lastly segment 5 finishes up the paper.

2. RELATED WORK

Kan Yang et al [6] have composed a privacy preserving evaluating convention for cloud frameworks. The convention underpins dynamic tasks on information and clump evaluating for multi-cloud condition. It utilizes bilinear blending to create a scrambled verification. The check of the confirmation accuracy is then executed by the information inspector. In this convention, the computational overhead of the reviewer is moved to the cloud server.

Anyway it neglects to give information privacy and client approval. Qian Wang et al. [7] have a given a confirmation plan to capacity security by coordinating information uprightness and dynamic information tasks. In this plan, an evaluator confirms the uprightness of capacity information. The dynamic information activities incorporate square inclusion and erasure utilizing Merkle Hash Tree (MHT) system.

They have connected the strategy of bilinear total mark for keeping up numerous inspecting undertakings. Be that as it may, it doesn't give privacy and approval. Yan Zhu et al. [8] have outlined a Provable Data Possession (PDP) conspire for guaranteeing the uprightness of cloud information stockpiling. In PDP, different cloud specialist co-ops (CSPs) agreeably keep up the customer's information.

A portion of the current study chips away at security issues of cloud registering is examined beneath. Naresh vurukondaets et al. [10] have made an investigation which recognized the issues of cloud information stockpiling, character administration and access control. Conceivable arrangements were recommended for a portion of the issues. Ayesha Malik et al. [11] have characterized a strategy for cloud suppliers that ensure clients' information and vital data. In their investigation, they have clarified distinctive attributes of the cloud processing, diverse administration models and so on.

Yunchuan Sun et al. [12] have looked into changed security answers for information stockpiling security and security assurance in cloud figuring. They have introduced a relative research examination of the current strategies with respect to information security Mazhar Ali et al. [13] have talked about different security issues of cloud registering.

Their study comprises of most recent security arrangements alongside total discourse on security issues. They additionally gave a concise exchange on security issues and arrangements identified with versatile cloud figuring. Sultan Aldossary et al. [14] have talked about the issues of cloud information stockpiling and arrangements.

The overview included issues of virtualization, information uprightness, information accessibility, information privacy. Aside from these information security issues, they have drilled down different dangers on cloud figuring.

The two fundamental segments of PDP are progressive system utilizing hash list and homomorphic evident reaction. It gives resistance against spillage of information and phony of label assaults. However, it doesn't give secrecy and approval.

3. PROPOSED METHOD

The fundamental thought is that the correspondence between cloud user and cloud service provider Cloud user imparts to CSP the entryways that he needs to apply utilizing a quantum private inquiry (QPQ)- roused convention: Cloud user encodes this data into a quantum enlist, and he haphazardly mixes his correspondence with "draws". CSP must apply the doors indiscriminately and send back her enroll without removing data from it. In the event that he tries to remove the data, cloud user can distinguish this from a solitary qubit estimation of the bait states he got back and he can intrude on their calculation.

Along these lines, CSP can decide at most a steady number of ventures of the calculation before cloud user has a high likelihood of recognizing that he is deceiving. Asymptotically in J, he, subsequently, gets no data on her calculation. Additionally, it is simple for cloud user to cover up both her info information (since the encoding of the info state is a piece of the calculation) and her yield information (since she can teach CSP to influence irregular flips of the yield to state bits before the last estimation). At last, by adjusting the approach proposed, our plan can enable the computationally constrained

cloud user to test whether CSP is playing out the calculation asked.

Algorithm-1: Blind Quantum Computation protocol for communication of CSP and data owner

1. Data owner preparation

For each column x=1,….,n

For each row y=1,….,m

1.1 Data owner prepares|φx,y_ε R{_+θx,y_=√1 2(|0_+eiθx,y|1_)|θx,y=0,∏/4,….,7∏/4} ad send the qubits to CSP.

2. CSP's Preparation

2.1 CSP creates an enlarged state from all received qubits, according to their indices,by applying CTRL-Z gates between the qubits in order to create a brickwork state $G_n^x m$ (see Definition 1).

3. Interaction and Measurement

For each column x=1,….,n

For each row y=1,….,m

3.1 Data owner computes φ_x,y where sX0

Y=sZ0

Y=0

3.2 data owner chooses x,y ε R {0,1} and computes Φx,y=φ_x,y+θx,y+x φx,y

3.3 data owner transmits φx,y to CSP.CSP measures in the basis {_+ φx,y_, _+ φx,y_}.

3.4 CSP Transmits the result sx,y ε {0,1} to Data owner.

3.5 if rx,y=1 abive, Data owner flips sx,y, otherwise

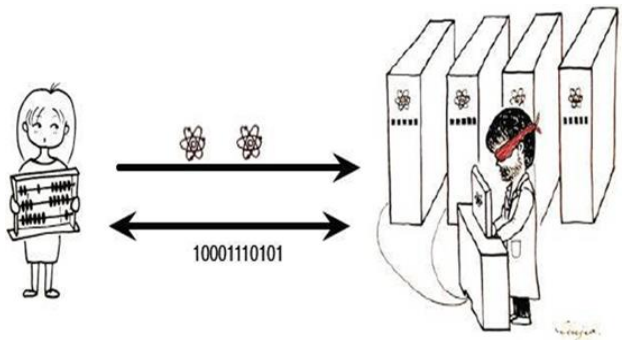

Figure 2. Quantum authentication and secure transmitting between cloud user and CSP

Algorithm 2. User Authentication and Quantum Bases distribution

1-Data proprietor solicitations to have an association with CSP

Information proprietor QKD: EPR-Data owner (IDData proprietor || IDCSP) QKD will enroll the association ask for status in log record and check the ID of Data proprietor for client Authentication. Additionally, QKD checks CSP's ID status (Busy, Free). On the off chance that CSP is free, QKD moves to stage 2.

2. QKD sends to CSP an association ask for containing Data proprietor's demand QKD CSP: EPU-CSP (IDData proprietor || IDCSP)

3. When CSP answer by tolerating the association with Data proprietor, CSP will send to QKD an affirmation message CSP QKD: EPR-CSP (IDData proprietor || IDCSP) QKD unscrambles the message and includes association's status between Data proprietor and CSP and the two are validated to send and get information.

4. QKD begins appropriating quantum bases (+,X) in some succession to encode the message to Data proprietor and CSP in a scrambled message utilizing their open keys.

4.1 QKD Data proprietor: EPU-Data owner (IDData proprietor || IDCSP || QB).

1. 2 QKD CSP: EPU-CSP (IDData proprietor || IDCSP || QB).

The cloud service provider deals with a cloud to give data stockpiling service. Data owners scramble their data documents and store them in the cloud for offering to data customers. To get to the mutual data records, data customers download encoded data documents of their enthusiasm from the cloud and after that decode them. Every datum owner/buyer is administrated by a space expert.

A space expert is overseen by its parent area specialist or the confided in expert. Data owners, data purchasers, space experts, and the confided in specialist are composed in a various leveled way. Here we use QKD with HASBE for authentication and key distribution between users QDK is used. And for group communication we use HASBE. Quantum communication mechanism is used for the authentication of data owner and CSP. And also between the users and data owner and CSP. The mechanism is as follows.

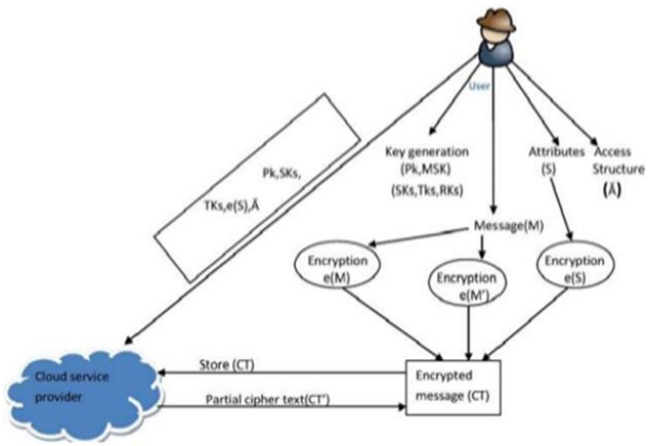

Figure 3. Key generation in HASBE using quantum key generation channel

Algorithm 3. HASBE using QKD for cloud data security

1. Setup: Given a security parameter K that is sufficiently gigantic, AUC will produce a framework parameter params and a root ace key MK0.

2. CreateMK: Using framework parameter params and their own particular ace keys, AUC or Sub-AuCs can make ace keys for bring down level Sub-AuCs.

3. CreateSK: With its own lord key MK_ and framework parameter params, Sub-AuC1 makes mystery key SKu for every customer on the off chance that it is certain that the general population key of the client is PKu, or there would be no mystery key for the client.

4. CreateUser: Sub-AuCs will make clients' mystery personality keys SKi;u and mystery quality keys SKi;u;a for them if the Aub-AuC ensures that the property an is responsible for it and the client u fulfills a. What's more, if not there would be no mystery personality keys or mystery property keys.

5. Encrypt: With R indicating an arrangement of clients' IDs, A speaking to the quality based access structure, the pubic keys of the considerable number of clients that are in R, and people in general keys of the considerable number of properties that are in A, the information supplier, which is likewise an information client of the distributed computing for this situation, can encode the detecting information D into ciphertext C.

6. RDcrypt: Given the ciphertext C, an information client having the exact ID that is in R can decode the ciphertext C into plaintext D with params and the client's mystery key SKu. ADcrypt: Given the ciphertext C, an information client having a characteristic set fag that fulfills A, which implies that the purchaser claims no less than a property key SKi;u;a, can likewise decode the ciphertext C into plaintext D with framework parameter params, the client's mystery personality key SKi;u, and the mystery trait key SKi;u;a.

Key Name	Meaning
MK0 Root key	Owned by AuC
MK_ Master key	owned by Sub-AuC
PK_ Public key	owned by Sub-AuC1
PKi Public key	owned by Sub-AuCs
MKi Master key	owned by Sub-AuCs
PKu Public key	owned by users
SKu Secret key	owned by users
, SKi;u Secret identity key	owned by users
SKi;u;a Secret attribute key	owned by users
PKu Public key	owned by attributes

4. EXPERIMENTAL RESULTS

The analyses were performed on a machine running UBUNTU part form 14.04 LTS with an Intel Corei3 CPU 2.50 GHz and 4 GB memory. Just a single CPU was utilized for calculation. Our model framework is executed in JAVA.

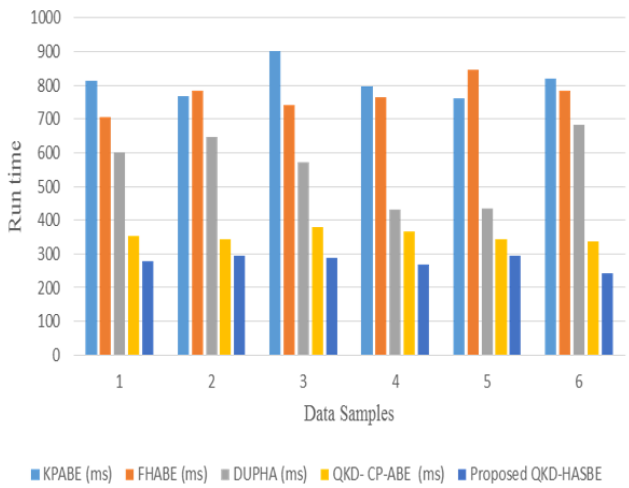

Figure 4. Performance analysis of average encryption and decryption time

Figure 4 outlines the execution of the proposed model to the customary hash calculations on cloud registering. From the table, it is watched that proposed demonstrate has less time calculation contrasted with the customary models.

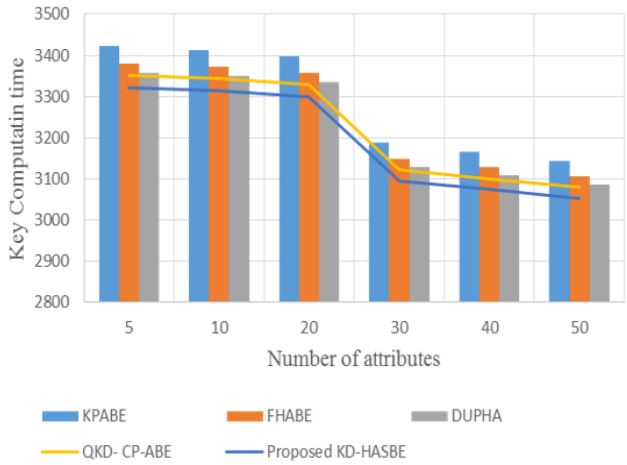

Figure 5. Key computation time of various methods

Figure 5 enlightens the execution key calculation time of the proposed model to the conventional hash calculations on cloud figuring. From the chart, it is watched that proposed demonstrate has less time calculation contrasted with the customary models.

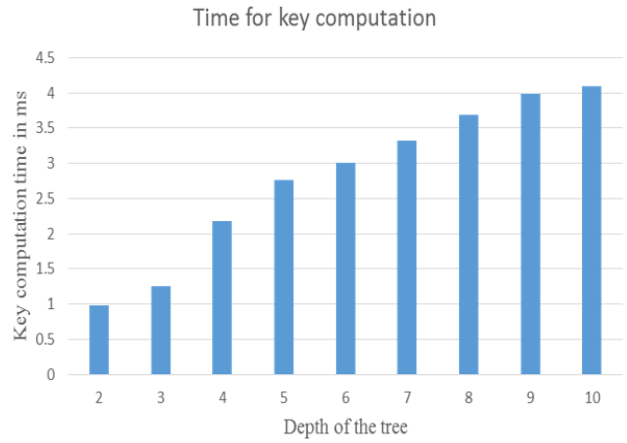

Figure 6. Key computation time with respect to depth of the tree in QKD-HASBE

Figure 6, delineates the key calculation time as for the profundity of the tree in HASBE the structure resembles a hierarchal model or tree structure, in view of the profundity of the tree the key calculation time fluctuates.

5. CONCLUSION

In this paper, blind quantum cryptography is considered as one of the best ways to secure communication data and restricts the unauthorized access of users. The security issues are resolved in order to achieve better security. Major issues such as key generation, encryption and decryption with network computation are enhanced HASBE based quantum model. To conquer these issues, a novel visually impaired quantum key dispersion based figure content arrangement ABE demonstrate was actualized in cloud condition. Exploratory outcomes demonstrated that the proposed show has high calculation speed, stockpiling overhead and anchored key dissemination contrasted with conventional CPABE, KPABE and QKD-CPABE models.

REFERENCES

[1] Scott, A. (2007). The limits of quantum computers. In Proceedings of the Second International Conference on Computer Science: Theory and Applications, CSR'07, pages, Berlin, Heidelberg. Springer-Verlag, 4-4. http://doi.org/10.1186/s13635-016-0051-2

[2] Barz, S., Kashefi, E., Broadbent, A., Fitzsimons, J.F., Zeilinger, A., Walther, P. (2012). Demonstration of blind quantum computing. Science, 335(6066): 303-308. http://doi.org/10.1186/s13677-015-0037-5

[3] Bennett, C.H., Hayden, P., Leung, D.W., Shor, P.W., Winter, A. (2005). Remote preparation of quantum states. Information Theory, IEEE Transactions on, 51(1): 56–74. http://doi.org/10.1109/tit.2004.839476

[4] Broadbent, A., Fitzsimons, J., Kashefi, E. (2009). Universal blind quantum computation. In Foundations of Computer Science. FOCS '09. 50th Annual IEEE Symposium on, pp. 517-526. http://doi.org/10.1504/IJAHUC.2017.085129

[5] Cao, Z.J., Liu, L.H. (2009). On the complexity of shor's algorithm for factorization. In Information Science and Engineering (ISISE), 2009 Second International Symposium on, pp. 164-168. http://doi.org/10.1109/ISISE.2009.86

[6] Divincenzo, D.P., Leung, D.W., Terhal, B.M. (2002). Quantum data hiding. Information Theory, IEEE Transactions on, 48(3): 580-598. http://doi.org/10.1109/18.985948

[7] Bensch, S. (2015). Cloud networks for sustainable ubiquitous services. International Journal of Computational Science and Engineering, 10(4): 336–346.

[8] Gorantla, M.C., Boyd, C., Nieto, J.M.G. (2010). Attribute-based authenticated key exchange. Information Security and Privacy, Springer, Berlin, Heidelberg.

[9] Dikaiakos, M.D., Katsaros, D., Mehra, P., Pallis, G., Vakali, A. (2009) Cloud computing: distributed internet computing for it and scientific research. IEEE Internet Comput., 13(5): 10-13.

[10] Liu, X., Zhang, Y., Wang, B., Yan, Mona, J. (2013). Secure multi-owner data sharing for dynamic groups in the cloud. IEEE Trans. Parallel Distributed Syst., 24(6): 1182-1191.

[11] Moritoh, Y., Imai, Y., Inomo, H., Shiraki, W. (2011). A cloud service on distributed multiple servers for cooperative learning and emergency communication. Commun. Comput. Inf. Sci., 188: 377-390.

[12] Shen, J., Zhou, T., He, D., Zhang, Y., Sun, X., Xiang, Y. (2017). Block design-based key agreement for group data sharing in cloud computing. IEEE Trans. Dependable Secure Comput., 1: 1.

[13] Shi, J., Li, H., Zhou, L. (2013). The technical security issues in cloud computing. Int. J. Inf. Commun. Technol., 5(3–4): 109–116.

[14] Wang, C., Shen, J., Lai, C.F., Huang, R., Wei, F. (2018). Neighborhood trustworthiness based vehicle-to-vehicle authentication scheme for vehicular ad hoc networks. In: Practice and Experience, Concurrency and Computation.

[15] Wang, C., Ren, K., Yu, S. Urs, K.M.R. (2012). Achieving usable and privacy-assured similarity search over outsourced cloud data. In: Proceedings of International Conference on Computer Communication, pp. 451-459

[16] Yu, S., Wang, C., Ren, K., Lou, W. (2010). Achieving secure, scalable, and fine-grained data access control in cloud computing. In: Proceedings of International Conference on Computer Communication, pp. 1-9.