International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-8, Issue-1, Jan 2020 E-ISSN: 2347-2693

An Enhanced Anonymity Control Scheme based on Quantum Cryptography in Cloud Environment

V. Sreenija Reddy[1*], Revathi A.[2], Phani kumar N.[3]

[1,2,3]Dept. of Computer Science & Engineering, S. V College of Engineering, Tirupati, India

[*]*Corresponding Author: sreenija.srj123@gmail.com, Tel.: 08332039887*

DOI: https://doi.org/10.26438/ijcse/v8i1.5356 | Available online at: www.ijcseonline.org

Accepted: 14/Jan/2020, Published: 31/Jan/2020

Abstract— Cryptography is widely used technique to provide security in large networks like cloud environments. Classical cryptography and quantum cryptography are two widely used techniques. Classical cryptography uses simple mathematical methods to provide security. So it is more vulnerable to several attacks such as eaves dropping, man-in-the-middle attack etc. But in classical cryptography digital signatures are used to provide best authentication. Quantum cryptography uses quantum mechanical properties to provide security. It uses photons and polarization but it requires more communication rounds. So by combing classical and quantum cryptography to show a new combination. Here we can use implicit user authentication, explicit mutual authentication and we can digital signatures to provide best authentication. The main objectives of this article are design and develop an enhanced anonymity control scheme based on quantum cryptographic techniques. EANCTRL- an enhanced anonymity control scheme based on Quantum key distribution is presented in this article.

Keywords: Quantum Computing, Cryptography, cloud computing, Anonymity in cloud

I. INTRODUCTION

Distributed and cloud computing is a progressive figuring strategy, by which registering assets are given powerfully by means of Internet and the information stockpiling and calculation are redistributed to somebody or some gathering in a cloud It enormously stands out and eagerness from both industry as well as the scholarly world since of the productivity, however it furthermore has at any rate three difficulties that must be taken into consideration before its going to be novel to the paramount of our information. Above all else, information privacy ought to be ensured. The info security isn't just about the given information substance. Because the most appealing piece of the distributed computing is the calculation redistributing, it is a lengthy ways past adequate to simply lead an entrance control. Almost certain, clients want to control the advantages of information control of different clients or cloud servers. This will be in the grounds that after touchy data or calculation is re-appropriated towards the cloud servers or another client, that will be out of users‟ control as a rule, security dangers would rise significantly in light to the fact that the servers may wrongfully assess users‟ information and access delicate data, or different clients might have the choice to derive touchy data from the calculation that is re-appropriated. In this way, the entrance along with the activity should be controlled. Furthermore, individual data (described as each users qualities set) is in danger in light of the fact that ones personality is verified dependent on his data because of the end goal of access control (or benefit control in this paper). As individuals are getting progressively concerned about their character security nowadays, the personality protection additionally must be ensured before the cloud enters our life. Ideally, any power or server alone ought not know any clients individual data. To wrap things up, the distributed computing framework should really be flexible on account of security break in which some bit of the framework is undermined by assailants. They are partners one to the other such as the decision of encryption arrangement (who are able to or can not decode the message) is created by various gatherings.

In the KP-ABE, a figure content is related with lots of traits, and a private key is related with a monotonic access structure like a tree, which depicts this users personality . A client can unscramble the figure content if and just if the entrance tree inside the private key is fulfilled by the characteristics in the figure content. Notwithstanding, the encryption strategy is portrayed within the keys, and so the encoded does not have authority that is whole the encryption arrangement. He has to think that the generators that are key keys with right structures to deal with clients. Besides, when are-encryption happens, the entirety for the clients in a similar framework must have their private keys re-gave to access there-scrambled records, and this procedure causes significant issues in execution. On the other hand, those issues and

overhead are altogether illuminated into the CP-ABE . When you look at the CP-ABE, figure writings are designed with an entrance structure, which determines the encryption arrangement, and keys that are private generated by users‟ properties. A customer can unscramble the figure content if and merely if his traits into the key that is private the entrance tree indicated into the figure content. Thusly, the encoded holds a authority that is definitive the encryption arrangement. Additionally, the as of this moment gave private keys will not be altered except if the entire framework reboots.

II. RELATED WORK

In [1], creators suggested that in enormous systems, security is given dependent on quantum key dispersion conventions by relating old style cryptography and quantum cryptography. They proposed unequivocal and understood shared confirmation intends to examine their recommended works. Their works incorporate verifying replay, and listening in assaults. Productivity can be improved in their proposed conventions by giving number that is least of rounds among Quantum Key Distribution (QKD). Utilizing Unbiased Chosen Basis (UCB) idea, another system for giving security is initiated. Into the perspective on UCB, QKD utilizes procedure that is no-cloning quantum estimation to provide a protected key contrary to the assaults involving the members. Quantum estimation quantifies the qubits determined by predisposition i.e., Rectangle or Diagonal premise. Obscure quantum state can't be copied and cannot duplicate the qubits if aggressor is unconscious for the polarization based on the announcement of no-cloning proposition. These proposed works goes about as another path for assessing QKDPs.

In [4,11], in quantum cryptography to understand confirmation firmly all hash that is inclusive are examined. Vulnerabilities identified with man-in-the-center assaults are considered. Verification lifetime is employed to gauge the scrambled labels. This recommends crude estimates like utilizing additional key for additional verification, diminishing data spillage, and changing mystery hash work habitually. Further research thoughts are given to utilize less validation that is key-expending solid security.

In [5], like in [1, 2] creators spotlight on building up a protected model for enormous systems. Here, they join mechanics of both style that is old and quantum cryptography. QKD structure with arrange plan and administrations that provides security is talked about here. For security confirmation of QKDP, UCB is utilized. It expresses that, QKD gives greater security with the use of polarization. A session key is utilized to share the mystery keys over and again for a long time. This model can oppose replay assaults and assaults that are latent.

The techniques utilized as of now are hazardous and obligated to inactive assaults, and these assaults can be tackled by quantum cryptography in[2], as in old style cryptography. The mix of certain QKDP and unequivocal QKDP are proposed by consolidating both old style cryptography and quantum cryptography to offer verified transmission between the members. Dynamic multicast frameworks are utilized in this proposed strategy that depend on bilinear maps, which can additionally fathom versatility issues. Verification is accomplished by utilizing Identity-tree. Both forward and in reverse mystery can be accomplished in this plan.

In [7,6], the idea of multi-server is proposed, in which a customer in parallel can talk to numerous servers using the end goal of validation. This introduces a two server framework that straightforwardly cooperates aided by the client and it is unmistakable to guide server. In this, Classical Key Exchange (CKE) and QKD models can be used. It proposes the utilization of incorporating both the models.

III.RESULTS AND DISCUSSION

First we could join through the use of the versatile. At that true point synchronize the report and transfer that record. Into the wake of transferring we could offer validation and safety with the use of the half reproduce traditional and quantum cryptography away from sight. This documents are exposed distinctly with the use of safety key when this occurs.

In this plan different methods determined by the property founded encryption were proposed to validate the storage that was distributed. Various procedures are proposed to protected the provided ideas substance protection by means of access control. we propose EANCTRL determined by quantum dissemination that is key allow cloud servers to regulate users‟ arrive at advantages without once you understand their character information.

The user and TC concur their polarization with the use of the pre-shared mystery type in this coordinated conventional cryptography and quantum cryptography. These mystery key with arbitrary sequence may be used to create another encryption key to session that is encode during the hour of key appropriation No matter if comparable session secrets are transmitted a similar polarization of qubits could not be gotten by the beneficiary They will follow our proposed convention whenever all was said in done, yet try to discover nevertheless much data as could reasonably be expected independently .The proposed methods can secure user‟s security against each energy that are solitary. Incomplete data is revealed in AnonyControl and no data is revealed in AnonyControl-F. We right from the start actualize the toolbox that are genuine of mult-iauthority based encryption

conspire AnonyControl and AnonyControl-F.

It presents verifiable client verification and client confirmation that is express. The comprehended client confirmation guarantees that secrecy is possilble to acknowledged customers. After secure communication session that is using, unequivocal client validation is conceivable. Also incorporate advanced markings at unequivocal verification.

a) Key dissemination stage
b) Adding computerized marks utilizing session key

Beneath calculation tells the best way to give security by utilizing half and half traditional and quantum cryptography.

Arrangement Phase
•Consider two clients who shared the session key safely.
•KTU is mystery key between confided in focus and client for estimating predisposition
•IF (KTU)i=0 then D premise
•Otherwise R premise can be considered.

Key Distribution Phase
1.First IMA should be possible, for example, members can validate through believed focus dependent on their login accreditations.
2.Trusted focus shares the sender and recipient keys. This is alluded as pre-shared mystery key.

3. Random number and session key are produced by confided in focuses. At that point it registers.
$R_{TA}=h(K_{TA},r_{TA}) \oplus (sk||U_A||U_B)$ for sender and computes $R_{TB}=h(K_{TB}, r_{TB}) \oplus (sk||U_A||U_B)$ for receiver.
4. The qubits generated by using trusted center for sender as
   - If $(r_{TA} \,||\, R_{TA})$ i= 0, $(K_{TA})I = 0$,
     Then $(QTA)i$ is $1/\sqrt{2}$ $(|0> +|1>)$
   - If $(r_{TA} \,||\, R_{TA})i=1$, $(K_{TA})i=0$,
     Then $(Q_{TA})I$ is $1/\sqrt{2}$ $(|0>-|1>)$.
   - If $(r_{TA} \,||\, R_{TA})i=0$, (K_{TA}) I=0,
     $(K_{TA})i=1$, then (Q_{TA}) i is $(|0>)$.
   - If$(r_{TA} \,||\, RTA)$ i=1, (K_{TA}) I=1,
     Then (Q_{TA}) i is | 1)

5. Trusted center generates qubits for receiver is same as above
   Participants receive qubits depending on secret key and measured based on bias D or R
   Once qubit is measured then computes
   $sk'||U_A||U_B=h(K_{TA},r'_{TA}) \oplus R'_{TA}$ for sender
   $sk'||U_B||U_B=h(K_{TB},r'_{TB}) \oplus R'_{TB}$ for receiver
6. Checksum can be computed is
   $CS_A=h'(sk', r_A) \oplus (U_A||U_B)$ for sender
   $CS_B=h'(sk'',r_B) \oplus U_B||U_A)$ for receiver
7. Checks the checksum for two participants as
   Check $U_A||U_B=h'(sk'',r'_A) \oplus CS'_A$ at receiver side
   Check $U_B||U_A= h'(sk', r'_B) \oplus CS'_B$ at sender side
8. Then build the session key SK and SK'
   $SK=h(sk',0)$
   $SK'=h(sk'',0)$

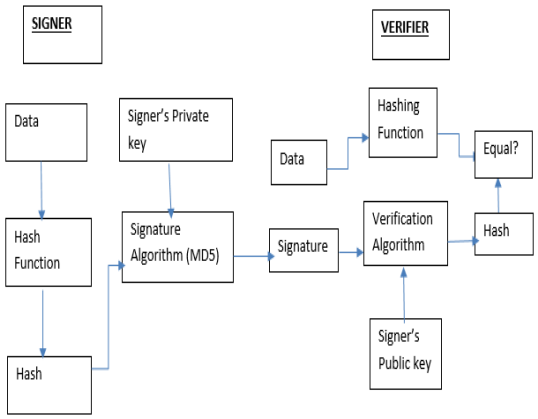

Figure 2: Proposed Framework

Advanced Signatures Phase

1. By utilizing the session key sender processes the computerized marks

Advanced marks are produced by utilizing MD5 calculation as follows
- Append the length and cushioning bits
- can be instated
- Message is prepared in 16-word squares
- Finally, computerized marks is made

2. The encoded message can be send to recipient
Collector confirms advanced marks by utilizing the sk" created by recipient.
The message is decoded at the recipient if the signature and key is confirmed.
Security Proof
UCB suspicion in quantum cryptography should be possible.
Convention member
The believed focus and approved arrangement of members can be utilized in reconciliation of traditional cryptography and quantum cryptography. In simultaneous execution confided in focus thus many number of members can exist.
Long haul mystery key
It is a long irregular parallel string which is shared between confided in focus and members.

IV.PERFORMNACE EVALUATION

The table shows that pre-shared mystery key is utilized in longer term, in light of the fact that without the verification believed focus can't show the mystery key. Quantum cryptography utilizes pre-shared

EPR matches between confided in focus and members to unravel man-in-the-center assault. In proposed plot we can utilize best advanced marks verification conspire.

Table 1: Performance assessment

Comparison	Classical key Model	Quantum key Model	EANCTRL
Vulnerable to man-in –the middle attack	No	Yes	No
Digital Signatures	Yes	No	Yes
Security Proof	No	No	Yes
Quantum Channel	No	Yes	Yes
Vulnerable to Passive Attack	Yes	No	No
Clock Synchronization	No	No	No
Communication Round	3	5	2
Pre-shared Secret key	Longer Duration	EPR Pairs	Longer Duration
Vulnerable to man-in –the middle attack	No	Yes	No
Digital Signatures	Yes	No	Yes
Security Proof	No	No	Yes
Quantum Channel	No	Yes	Yes
Vulnerable to Passive Attack	Yes	No	No

V. CONCLUSION AND FUTURE WORK

By consolidating the traditional and quantum cryptography we can give security and verification and furthermore decrease the quantity of correspondence adjusts. We can utilize understood client verification and express common confirmation and including computerized marks. We can actualize this security and confirmation in Cloud based application. So proposed model is increasingly compelling contrast with other when giving both security and validation. Qubits cost can be diminished in future. Believed focus can be increasingly viable to explain replay assaults and to give secure session key utilizing mystery key, arbitrary number and qubits. In enormous systems security can be accomplished by consolidating strategies with computerized marks. Mixture old style and quantum cryptography gives best security and validation. So we can utilize this for any application in future.

REFERENCES

[1] P. Dileep Kumar Reddy, R. Praveen Sam, C. Shoba Bindu "Optimal Blowfish Algorithm based Technique for Data Security in Cloud" Int. J. Business Intelligence and Data Mining, ISSN online 1743-8195, ISSN print 1743-8187, Vol. **11**, No. **2**, Pp.171–189.DOI: 10.1504/IJBIDM.2016.10001484. (Inder Science) (UGC Approved). Journal No: 1648, **2016.**

[2] P. Dileep Kumar Reddy, R. Praveen Sam, C. Shoba Bindu "Tripartite partite key assignment scheme for security of cloud data classes" Journal of Theoretical and Applied Information Technology, Vol.**95**. No **13**, ISSN: 1992-8645, E-ISSN: 1817-3195, Pg.No:3116-3126. (Scopus& UGC), Journal No: 23566, **15th July 2017.**

[3]Tzonelih Hwang, Kuo-Chang Lee, and Chuan-Ming Li, "Provably Secure Three-Party Authenticated Quantum Key Distribution Protocols," IEEE Transactions on Dependable and Secure Computing,pp. 71-80, Vol. **4**, No. **1**, March **2007**

[4] C.H.Bennett, "Quantum Cryptography Using any Two symmetrical States, "Physical Rev. Letters, vol.**68**,no. **3121**, **1992.**

[5] N.Asokhan, V.Niemi, and K. Nyberg, ""Man-in-the-Middle in Tunneled Authentication Protocals," Proc. Int'l Workshop Security Protocols, **2003.**

[6] Aysajan Abidin, "Shortcomings of Authentication in Quantum Cryptography and Strongly Universal Hash Functions," Linköping considers in science and innovation, **2010**

[7] Tasleem et al., "Cross breed Approach: Combining Classical Cryptography and QKD for Password Authentication," International Journal of Computer Science and Communication Networks, Vol. **2**, No. **4**, pp. **512-515**

[8] Dr.G.Ananda Rao et al., "Three Party Authentication Key Distributed Protocols Using Implicit and Explicit Quantum Cryptography," Indian Journal of Computer Science and Engineering, pp.143-145, Vol. **2**, No. **2**, **May 2011**

[9] T.S.Thangavel and A. Krishnan, "Coordinated Quantum and Classical Key Scheme for Two Servers Password Authentication," Journal of Computer Science, Vol. **6**, No. **12**, pp. 1396-1405, **2010**

[10] M. Bellare and P. Rogaway, "Provably Secure Session Key Distribution: The Three Party Case," Proc. 27th ACM Symposium Theory of Computing, pp. **57-66**, **1995.**

[11] Mr. P. Dileep Kumar Reddy**, "**Handover Key Management for Re-Authentication in Cloud Technology for Accessing Data Classes", International Journal for Research in Applied Science & Engineering Technology (IJRASET**)** ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887**,** Volume **5** Issue **IX**, **(UGC Approved)**Journal No: 45842, Pg no 1951 to 1953, Doi. 10.22214/IJRASET, **September 2017.**

AUTHORS PROFILE

Ms. V Sreenija Reddy pursed Bachelor of Technolgy from Sri Venkateswara enginerring college for women, Tirupat in 2017. She is currently pursuing M.Tech in Department of Computer Science & Engineering.

Ms. A. Revathi is as an Assiatant Professor in the Department of Computer Science & Engineering at SV College of Engineering, Karakambadi Road, Tirupati. She has 13 years of experience in teaching. She completed B.Tech in Siddharth Institute of Engineering and Technology, Puttur in 2005, M.Tech in Sree Vidyanikethan Engineering College, Tirupati in 2009, She is currently pursuing Ph. D in Sri Padmavati Mahila Visvavidyalayam, (Women's University) Tirupati, Andhra Pradesh - India

Mr. N. Phani Kumar is as an Assiatant Professor in the Department of Computer Science & Engineering at SV College of Engineering, Karakambadi Road, Tirupati. He has 11 years of experience in teaching. He completed M.Tech in Annamacharya. Institute of Technology & Sciences in 2008, Rajampet Andhra Pradesh, India.

