Research Article

Attribute-Based Proxy Re-encryption for Health Record Maintenance in Cloud Environment

Sathis Kumar[1], and Kavitha[2]

[1]Saranathan College of Engineering, Tiruchirappalli/India, sathistrichy22@gmail.com (ORCID: 0000-0001-6510-8934)
[2]Indra Ganesan College of Engineering, Tiruchirappalli/India, nkavithamail@gmail.com (ORCID: 0000-0001-5676-3160)

Article History: Received: 11 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 23 May 2021

Abstract: In cloud secure individual information sharing is the significant issues since it makes a few protections and information privacy issue while getting to the cloud administrations. Numerous difficulties present in close to home information sharing, for example, information security assurance, adaptable information sharing, proficient position designation, calculation effectiveness enhancement, are staying toward accomplishing functional fine-grained admittance control in the Personal Health Information Sharing framework. Individual wellbeing records should be encoded to ensure security prior to moving to the cloud. Targeting addressing the above difficulties, here propose a productive information sharing instrument for Personal Data Sharing, which not just accomplishes information security, fine-grained admittance control and authority assignment all the while, yet in addition advances the calculation effectiveness and is appropriate for asset compelled workers. A large portion of the information purchasers are straightforward, while not many of them are bad and will spillage their mystery keys in the intrigue. Despite what might be expected, PKG and information proprietor are thought to be completely confidential. Moreover, public cloud 1 and public cloud 2 can't conspire with one another. The non-tricky supposition that is sensible, on the grounds that the customer can request that two cloud workers can't uncover client’s data by contract. In proposed work, PR-ABE (Attribute Based Encryption with Proxy Re-encryption) method executes to give secure encryption of clinical information. To improve the concurrency control, here halfway key sharing plan will be executed. Utilizing this, information proprietor can send halfway mystery key for the mentioned client. This methodology conquers the key speculating assault in information recovery measure.

Keywords: PR-ABE (Attribute Based Encryption with Proxy Re-encryption); KGC (Key Generation Centre); PKG (Private Key Generator); OMD (Original Medical Database); EMR (Electronic Medical Record); DMD (Duplicate Medical Database)

1. INTRODUCTION

Cloud computing is a figuring worldview, where a huge pool of frameworks is linked to in private or public organizations, to give continuously adaptable establishment to application, data and report storing. With the procedure of this progression, the expense of calculation, application empowering, content accumulating and development is reduced all around. It is a feasible method to manage experience direct cash saving favorable circumstances and it can change a worker ranch from a capital-concentrated set up to a variable assessed environment. Cloud enrolling relies upon an uncommonly vital norms of reusability of IT capacities. The qualification that circulated figuring brings stood out from ordinary thoughts of "network figuring", "scattered handling", "utility enlisting", or "autonomic preparing" is to broaden horizons across progressive cutoff points. Forrester [1] characterizes cloud computing as: “A pool of abstracted, highly scalable, and managed compute infrastructure capable of hosting end customer applications and billed by consumption”. It is an advancement that uses the web and central removed laborers to keep up data and applications and grants clients and associations to use applications without foundation and access their own archives at any PC with web access[2][7]. This development contemplates significantly more capable figuring by concentrating data storing, getting ready and information move limit. Distributed computing models are Yahoo email, Gmail, or Hotmail. Enterprises can decide to submit public, private or hybrid cloud applications [15]. Cloud Integrators can have a fundamental effect in choosing the right cloud path for each affiliation. The proposed work perform execution in re-appropriated key age, Encryption, Re-encryption key age and Decryption at the same time. The Attribute Based Encryption (ABE) is used for encryption and unscrambling of messages in which ABE is usually more efficient than RSA-based calculation.

1.1. Public Cloud

Public clouds are accessed and managed by outcasts they share favored economies of scale over clients, as the system expenses are distributed across the system among a mix of customers, giving each individual client a charming insignificant exertion, "Pay-all the more just as expenses emerge" model. All customers share a common device pool with restricted course of action, safety protections and variances in availability. These are handled by the cloud provider and maintained. One of the possible benefits of a public cloud is that it can be larger than a cloud effort, allowing interest to scale consistently.

1.2. Private Cloud

Private clouds are created exclusively for a single company. They mean addressing data protection stresses and providing greater power, which is typically sickly in a public cloud. A private cloud has two product sets:

- On-premise Private Cloud
- Remotely facilitated Private Cloud

1.3. Hybrid Cloud

In reality, hybrid clouds consolidate both public and private cloud models. Expert communities can use outcast cloud providers in a complete or inadequate manner with a hybrid cloud, extending the versatility of handling. The Hybrid cloud system is prepared for on-demand, remote scale provisioning. It is possible to use the opportunity to extend a private cloud with public cloud resources to tackle any impressive floods of exceptional weight.

The contribution of the work is that the proposed algorithm provides security efficient with non-colluding properties. The proposed conspire accomplishes better execution in re-appropriated key age, Encryption, Re-encryption key age and Decryption at the same time.

LITERATURE SURVEY

Authors: Kaitai Liang1, Liming Fang, Duncan S. Wong, and Willy Susilo

The work proposed is to assemble another CP-ABPRE with CCA protection in the subjective prophet model. Pick Waters ABE (the best improvement proposed in [13]) as a fundamental design square of the arrangement due to the going with reasons. The Waters ABE plot enhancement helps us to alter the scheme to be an ABE Key Encapsulation in the discretionary prophet model. Specifically, a material key that is overly mixed under a passage method is used in the proposed model to cover a message in a symmetrical way. Besides, Waters ABE plot utilizes LSSS to help any formula for monotonic access for figure messages. It is an appealing property for CP-ABPRE structures when being executed before long. Besides, the advancement for figure messages, whose size is straight in the size of formula, can help us with mitigating the correspondence cost achieved by re-encryption and the time of re-encryption key [2]. To make data sharing be even more capably, Proxy Re-Encryption (PRE) is proposed. PRE expands the standard Public Key Encryption (PKE) to help the arrangement of unscrambling rights. This enables a semi-accepted gathering called go-between to change a code text proposed for a get-together and another code text of the identical plaintext got ready for party B. The go-between, regardless, does not discover the deciphering keys or the plaintext covered up. PRE is a helpful, unrefined cryptographic programmed and has numerous applications, for instance, secure appropriated records systems and email sending.

Proposed work gives another approval strategy to determine who can do a plaintext uniformity test dependent on code messages. At that point, another idea of PKEwET and personality based encryption was proposed, under the name identity based encryption with equality test (IBEET). To diminish the computational time cost in the past plan, planned a plan for this reason. As of late, ABE underpins the idea of uniformity test, since it bolsters the usefulness of search and tests on the code text dependent on various access strategies. A KP-ABE with equality test (ET) conspire was proposed, which gives testing if the code messages incorporate a similar data dependent on the arrangements of various credits. Be that as it may, it just acknowledges single direction against picked figure text assaults. Proposed conspire isn't secure for a test under picked figure text assault. They proposed another plan to tackle single direction against picked figure text assault. As probably are aware, there is no unequivocal CP-ABE fine-grained admittance control conspire with correspondence test [7][9]. The information proprietor encodes his private information with relating secret entryways and stores it in the cloud. Assume there is a client expects to look in the information proprietor's code messages, he sends a solicitation utilizing explicit hidden entryway to the cloud. At the point when the cloud gets the solicitation of looking, it can choose whether two diverse code writings are encryptions of the equivalent plaintext. The point of this work is to permit the clients a simple hunt of code messages, to arrive at secure fine-grained, and access control in the cloud.

2. THEORITICAL FRAMEWORK

2.1. Exixting System

Contrasted and conventional model of ABE the current framework was embraced with two diverse public cloud workers to accomplish made sure about rethought calculation. In this framework public cloud one and public cloud two are straightforward yet inquisitive all the more unequivocally, they will follow the convention however attempt to discover whatever amount of private information as could sensibly be normal. A large portion of the customers are straightforward, while not many of them are bad and will spillage their mystery keys in plot. It is a fine grained information sharing instrument for EMR framework contributed here, which accomplishes non intuitive fine grained admittance control and authority designation all the while.

2.2. Proposed System

Design Considerations:

- To implement two cloud based secure EMR sharing scheme.
- PKG is to provide system parameters.

PRE an ABE for new access policy without revealing the plaintext.

- Develop an extensible security with the help of two cloud servers.
- Server 1 has the files that are uploaded by user itself.
- Server 2 has the fake copy of the original file.

Advantages of Proposed System:

- Communication cost is little and fixed.
- Keep public cloud workers from learning mystery data.
- Improved computation efficiency for PKG and USER.
- No collusion between two clouds.

On the off chance that a client wishes that a code text can be decoded by some particular beneficiaries, at that point picks an access rule as (“the value of attribute x is *a*” AND Here, the attribute y is *b* OR the attribute z is c.

CT = (A, B = e(P, M) e(P, B) 1 M, C_1 = sP,

C_2 = sP C_3 = t^s = e(P, B $)^{\alpha(\beta-1)s}$, C_4 = x_1H_2(e(P, M$)^{\alpha ls}$)P, C_5 = e(P, M $)^{\alpha l(s-1)}$, || M = E_k(B), C_r = H(P M),

$C_A = q_A(0)M_A, B_A = q_A(0)H_1(a)$, $C_A = q_A(0)M$, $C_A = q_A(0)B_1(a)$, $C_B = q_B(0)V_B$, $C_B = q_B(0)H_1(b)$, $C_B = q_B(0)M$, $C_B = q_B(0)H_1(b)$, $C_D = q_D(0)V_D$, $C_D = q_D(0)B_1(d)$, $C_D = q_D(0)M$, $C_D = q_D(0)B_1(d)$)

where x ∈ Xp is a random variable, J is a randomly selected session key from G1, qA(0) = qC(y), qB(0) = qC(z), qC(0) =

qR(x), qD(0) = qR(t), and qR(0) = s. It is calculated to identify the duplicate storage based on key verification.

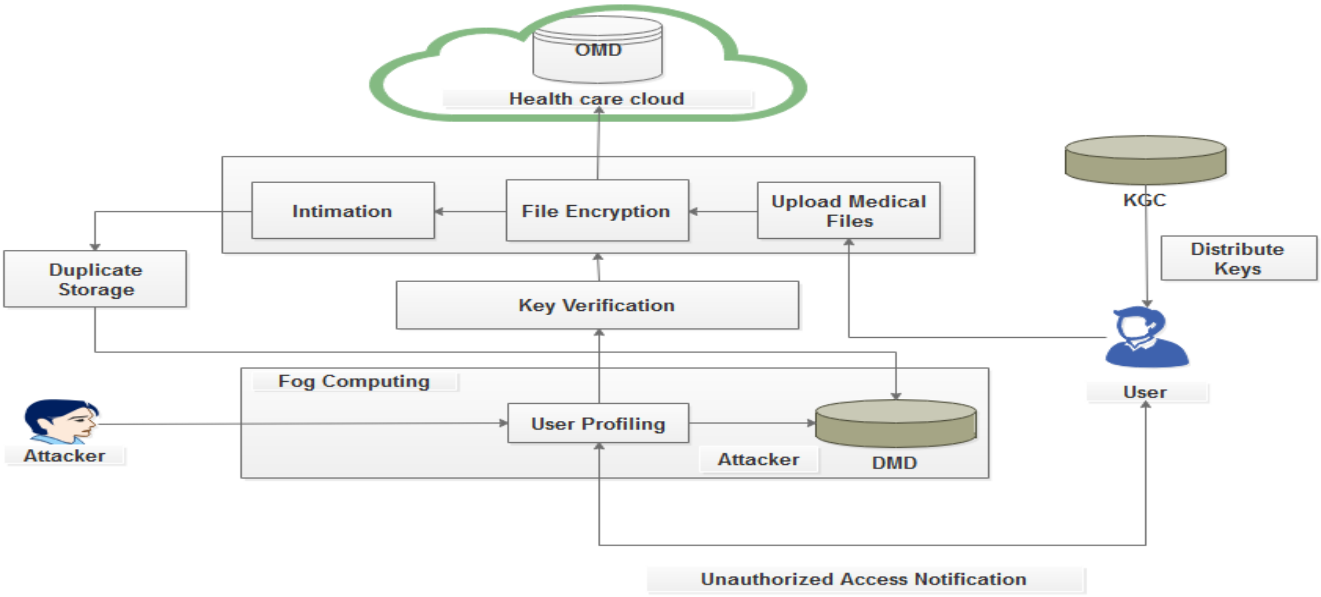

Figure 1. Architecture diagram

2.3. Algorithm Used

Attribute Based Encryption: 320 bits

- Setup (M, B) → (MK, BK):
  - The measurement of the arrangement takes a security boundary M and a universe representation B as data, which characterises the arrangement of permitted credits in the system. This results in the BK public boundaries and the MK expert mystery key.
- Encrypt (BK, M, P) → MB:
  - The encryption algorithm takes the BK public borders, a message M and a bunch of S properties as information and returns a code text MB relevant to the set of properties.
- KeyGen (MK, BK) → MB:
  - The key generation algorithm takes the professional mystery key MK and an access structure BK as information and produces a private key BK related to the attributes.

- Decrypt (PK, MB) → P:
  - The unscrambling calculation takes a private key BK related to access structure and a code text MB related to quality set S as information and yields a message M if S complies with or the blunder message ⊥ something else.

3. IMPLEMENTATION

Proposed framework will actualize utilizing PHP as front end and SQL is for back end measure. This methodology has modules like casing work creation, Medical documents transferring ,Data Encryption, Duplicate stockpiling, File access and ready framework. Information measure has document stockpiling and yield was give secure to clinical records utilizing two cloud.

ABE uses LSSS to help any monotonic access equation that is an alluring and pragmatic property for this framework. In addition, the development procedure for figure messages, which guarantees figure text size to be straight in the size of equation other than all framework attributes(cloud based), empowers us to diminish the correspondence cost caused by re-encoded figure text and re-encryption key[9][17]. In view of consumer profiling, the substantial change in CHK can be used to modify a CPA-secure PKE plan to be safe against CCA using key appropriation, it can't be inconsequentially utilized in the PRE setting. It is utilized to forestall figure text from being changed, simultaneously; PRE permits change among figure messages from DMD. On the off chance that an encryption utilizes the CHK change to ensure the legitimacy of code messages, it will handily bring about that the legitimacy of re-encryption results can't be guaranteed [18]. Along these lines, inconsequentially utilize the change in a PRE plan that frequently brings about CCA (RCCA) security [12]. The exemplary models are given in [10], [11], [13].

Using the CHK update as a black box to transform the new CPA-safe CP-ABPRE plans to be secure against non-piddling CCA, accordingly. This system is based on the flexible CP-ABE [14]. Because this versatile CP-ABE is specifically secure security, the proposed OMD development is therefore also specifically secure [15]. Here, in the randomize the key and encode theory, the flexible ABE to the Enc portion (pk, R, M) of re-encryption key rkS'M (RSA VS ECC) (see Fig. 2).URKG creates urkS as

$$\mathrm{urk}_S := (\mathrm{X}, \mathrm{Rand}(R, \mathrm{sk}_S\,), \mathrm{AdpEnc}\ (\mathrm{pk}, R, \mathrm{D}))$$

Here, AdpEnc is a flexible ABE encryption calculation and D is a spurious access structure where certain trait sets are not fulfilled under the D entry structure. RKG gets urkS and the entrance structure M as rkS is accompanied by the use of rsk=tk will be created by knowledge.

$$\begin{aligned} \mathrm{rk}_{S\to \mathrm{M}} &:= (S, \mathrm{M}, \mathrm{Rand}(R, \mathrm{sk}_S\,), \mathrm{PolicyAdp}\ (\mathrm{AdpEnc}\ (\mathrm{pk}, R, \mathrm{D}), \mathrm{M}\ , \mathrm{tk})) \\ &= (S, \mathrm{M}\ , \mathrm{Rand}(R, \mathrm{sk}_S\,), \mathrm{AdpEnc}(\mathrm{pk}, R, \mathrm{M}\ )) \end{aligned}$$

via the property of versatile ABE, Poy(PolicyAdp) (AdpEnc (pk, R, D), M, tk) yields a code text which includes an entrance structure composition M and a mystery arbitrariness R, means PolicyAdp (AdpEncD(R), M , tk) = AdpEnc(pk, R, M). Along these lines, by consolidating the randomize the key and scramble system and versatile ABE, can build a particular adaptable CP-AB-PRE plan [18]. The above property is normal by utilizing material Rand in a few plans. At that point, m: = Rand(R, m) is a plaintext randomized by the arbitrariness R. A re-scrambled code text rctM is framed as demonstrated underneath.

$$\mathrm{rct}_{\mathrm{M}} := (\mathrm{M}\ , \tilde{m} := \mathrm{Dec}(\mathrm{pk}, \mathrm{Rand}(R, \mathrm{sk}_S\,), \mathrm{oct}_{\mathrm{M}}), \mathrm{Enc}(\mathrm{pk}, R, \mathrm{M}\ ))$$

A beneficiary who's got an unscrambling key skS acquires a mystery irregularity R by decoding octM. At last, we can acquire m by registering Rem (m,˜ R). The versatile ABE broadens conventional ABE by permitting a semi-confided in outsider in order to change a code text under one structure for access M into figure text under some other structures for access M by utilizing a calculation PolicyAdp and a hidden entrance key tk. The PolicyAdp property is extremely helpful at the point when the information proprietor utilizes the cloud administration. As the cloud is semi-trusted, the appointment party that is given to the hidden entrance for scrambled information change. The information proprietor asks for the Cloud to re-scramble the en-crypted information by giving the new structure of access.

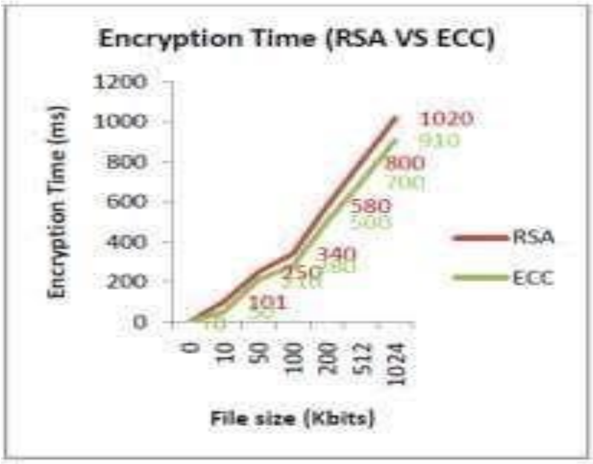

Figure 2. Encryption time of RSA and ECC

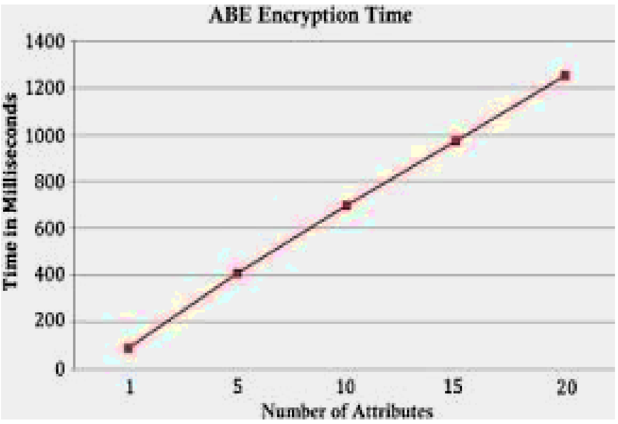

Figure 3. Encryption time of ABE

RSA calculation and Attribute Based Encryption (ABE) is used for encryption and unscrambling of messages in which ABE is usually more efficient than RSA-based calculation, as seen in figures 2 and 3 above. ABE is another one-to-numerous encryption-dependent public key that allows customers to unscramble the message depending on the arrangement of traits and access approaches.

4. Conclusion

The results shows that the implemented algorithm handles the security of the data strictly, that it provides security in sake that hackers could not reach as easy as they try to. The proposed algorithm provides security efficient clouds with non colluding properties. The proposed conspire accomplishes better execution in re-appropriated key age, Encryption, Re-encryption key age and Decryption at the same time.

References

1. Alderman, N. Farley, and J.Crampton, "*Tree-based cryptographic access control," in Computer Security - ESORICS 2017 - 22nd European Symposium on Research in Computer Security*, Oslo, Norway, September 11-15, 2017, pp. 47–64.
2. Zhang, H. Ma, and Y. Lu, "Fine-grained access control system based on fully outsourced attribute-based encryption," *Journal of Systems and Software*, vol. 125, pp. 344–353, 2017.
3. Ma, R. Zhang, Z. Wan, Y. Lu, and S. Lin, "Verifiable and exculpable outsourced attribute-based encryption for access control in cloud computing," *IEEE Transactions on Dependable and Secure Computing*, vol. 14, no. 6, pp. 679–692, 2017.
4. Castiglione, A. D. Santis, B. Masucci, F. Palmieri, A. Castiglione, J. Li, and X. Huang, "Hierarchical and shared access control," *IEEE Transactions Information Forensics and Security*, vol. 11, no. 4, pp. 850–865, 2016.

5. Sebe, J. Domingo-Ferrer, A. Martinez-balleste, Y. Deswarte, and J. Quisquater, "Efficient Remote Data Integrity checking in Critical Information Infrastructures," *IEEE Transactions on Knowledge and Data Engineering*, vol. 20, no. 8, pp. 1-6, 2008.
6. Wang, K. Ren, W. Lou, and J. Li, "Toward Publicly Auditable Secure Cloud Data Storage Services," *IEEE Network*, vol. 24, no. 4, pp. 19-24,July/Aug. 2010.
7. Zhu, H. Wang, Z. Hu, G. J. Ahn, H. Hu, and S. S. Yau, "Efficient Provable Data Possession for Hybrid Clouds," *Proc. 17th ACM Conference on Computer and Communications Security*, pp. 756-758, 2010.
8. Yang and X.Jia, "Data Storage Auditing Service in Cloud Computing: Challenges, Methods and opportunities," *World Wide Web*, vol. 15, no.4, pp. 409-428, 2012.
9. Goyal, O. Pandey, A. Sahai, and B. Waters. "Attribute-Based Encryption for Fine-grained Access Control of Encrypted Data". In *Proc. of CCS'06*, Alexandria, Virginia, USA, 2006.
10. Sahai and B. Waters. "Fuzzy Identity-Based Encryption." *In Proc. of EUROCRYPT'05,* Aarhus, Denmark, 2005.
11. Barker,W. Barker, W. Burr, W. Polk, and M. Smid, "Recommendation for key management–part 1: General (revision 3)," *NIST special publication,* vol. 800, p. 57, 2011.
12. Bos,M.E.Kaihara,T.Kleinjung,A. K. Lenstra, and P. L.Montgomery, "On the security of 1024-bit rsa and 160-bit elliptic curve cryptography.," *IACR Cryptology* ePrint Archive, p. 389, 2009.
13. Hemalatha, Dr.R.Manickachezian, "Present and Future of Cloud Computing: A Collaborated Survey Report"., *International Journal of Innovative Technology and Exploring Engineering (IJITEE)* ISSN: 2278-3075, Volume-1, Issue-2, July 2012.
14. Hemalatha, Dr.R.Manickachezian, "Implicit Security Architecture Framework in Cloud Computing Based on Data Partitioning and Security Key Distribution"., *International Journal of Emerging Technologies in Computational and Applied Sciences,* ISSN (Online): 2279-0055 , pp. 76-81, Feb.2013.
15. Hemalatha, Dr.R.Manickachezian " Dynamic Auditing Protocol using Improved RSA and CBDH for Cloud Data Storage".,*International Journal of Advanced Research in Computer Science and Software Engineering* Volume 4, Issue 1, January 2014.
16. Yutaka Kawai,"Outsourcing the Re-encryption Key Generation: Flexible Cipher text-Policy Attribute-Based Proxy Re-encryption",*Springer InternationalPublishing* Switzerland,pp. 301–315, 2015, DOI: 10.1007/978-3-319-17533-1_21.
17. Chun-I Fan, Chien-Nan Wu, Chun-Hung Chen, Yi-Fan Tseng, Cheng-Chun Feng "Attribute-Based Proxy Re-Encryption with Dynamic Membership", *IEEE 10th Asia Joint Conference on Information Security*, 2015, DOI: 10.1109/AsiaJCIS.2015.21.
18. Liang, K., Fang, L., Susilo, W. & Wong, D. S, " A cipher text-policy attribute-based proxy re-encryption with chosen-cipher text security" *5th IEEE International Conference on Intelligent Networking and Collaborative Systems*, pp. 552-559 , 2013.