Key-Aggregate Cryptosystem with Broadcast Aggregate Keys for Secure Data Sharing in Cloud Computing

Rasika R S[#1], Dr. R. V. Siva Balan., M.C.A., M.Phil., Ph.D.,[*2]
[1]*Research Scholar in Department of Computer Science, Noorul Islam Centre for Higher Education, Kumarakovil, Kanyakumari District, Tamilnadu State, India – 629 180.*
[2]*Associate Professor, Department of Computer Applications, Noorul Islam Centre for Higher Education, Kumarakovil, Kanyakumari District, Tamilnadu State, India – 629 180.*

Abstract —

Recently, cloud storage is a gaining popularity. In enterprise settings, rise in demand for data outsourcing, which assists in the strategic management of corporate data. However, users are also increasingly concerned about inadvertent data leaks in the cloud. Such data leaks, caused by a malicious adversary or a misbehaving cloud operator, can usually lead to serious breaches of personal privacy or business secrets. A key challenge to designing such encryption schemes lies in the efficient management of encryption keys. A projected a economically implementable edition KAC among small transparency cipher texts as well as collective key, use pairing. It is able to be economically shared through broadcast encryption provide towards information user as well as information owner whereas falling the reducing the protected waterway constraint. It also allow user to decrypt numerous module of information using the single input of stable range which could economically broadcast towards numerous user. Our planned scheme has proved in secure and practically efficient.

Keywords - *Data sharing, Privacy, cloud storage. Broadcast Encryption, Data Security, Key-Aggregate Cryptosystem*

I. INTRODUCTION

Currently storage on a cloud that have materialize like able to respond from appropriate along with on-demand access the enormous amount in order share above a Internet. Production user is showing consideration from cloud storage owing toward the numerous profit, counting lesser rate, improved quickness, as well as better source operation. Each day user is too allocating personal information, for example photo as well as video, through contacts during public system application base in cloud. Taking place on extra whereas benefit from convenience for allocation information during cloud storage, user is moreover slowly bothered regarding unplanned information expose through a cloud. Such information illuminating would be perform through hateful enemy otherwise ill-behaved cloud operative, be able to usually straight strict disobedience personal information otherwise private information about business. It including lower cost, greater agility, and better resource utilization. However, while enjoying the convenience of sharing data via cloud storage. Users are also increasingly concerned about inadvertent data leaks in the cloud. Such data leaks, caused by a malicious adversary or a misbehaving cloud operator. It can usually lead to serious breaches of personal privacy or business secrets. To address, data leaks in cloud storage, the data owner to encrypt all the data before uploading them to the cloud. The challenging problem is how to effectively share encrypted data. Of course users can download the encrypted data from the storage, decrypt them, then send them to others for sharing, but it loses the value of cloud storage. User must be able to delegate the access privileges of the allocation information toward others hence they will able to admittance information since server straightforwardly.

The conventional systems ensure information privacy be depend on server toward implement admittance manage mechanism [1]. The method be level toward right appreciation attack within mutual information environment such as the cloud, somewhere information equivalent toward numerous user can inhabit the similar server. Present skill on behalf of safe online information allocation come within two main flavor - trust a third party auditor [2], otherwise use the user's be the owner of input toward encrypt her information like protect privacy [3]. Within either case, a client would desire for the trustworthy as well as competent cryptographic system within position, through official guarantee safety, tall scalability as well as easiness of utilize. The most important test within scheming is such a cryptosystem deceit on efficient allocation of encrypted information. An information distribution system on the cloud be simply victorious but information owner be able to hand over the right to use their information professionally on the way to numerous user, who be able to right to use the information openly from the cloud servers. Intended this, requirements to supply each one of these user with decryption privileges to exact lessons of the information that they are certified to right to use. A

confront consequently is to plan a protected as well as competent online incomplete information distribution system that allow performing arts that task in an competent as well as protected method.

In this paper, we challenge on the way to construct exactly such a information distribution structure to facilitate provably protected moreover the same time, efficiently implementable. Here proposed a key aggregate cryptosystem (KAC) to address this problem, albeit devoid of formal proof of security. In this paper, we propose CPA and CCA secure KAC structure with the aim of professionally implementable using elliptic curve moreover appropriate for execution on cloud base information allocation environment. KAC system is able of competently shared through broadcast encryption to keep away from the use of secret channel which are expensive and not easy to understand in perform, along with it is scalable to every random number of information lessons and data user.

II. RELATED WORKS

Ahead of we initiate our extended KAC system, this segment foremost review numerous category of accessible solution as well as clarify their associations to our job. Mainly this system produces key for symmetric-key cryptosystems, still however the input derivation might need modular mathematics like use in public-key cryptosystems, which are generally more expensive than "symmetric-key operation" such as pseudorandom reason.

In [4], available a flexible makes use of of cloud storage planned for customer require as it is seam access information nearby however to in attendance at distant surface. It is significant to check the information put on the cloud. Thus it is important toward authorize an unlock verify on behalf of sincerity outsourced information all over third party auditor (TPA). TPA be moreover expensive in favor of cloud service supplier. Which check the exactness of the outsourced information, except limitation be estimate clearness.

In [5] presented a security mediator (SEM) shift that permit a customer toward guard the privacy. Customer will upload each information SEM therefore will not able toward identify the information still however it's leave-taking to manufacture confirmation taking place information. Since the user be sign by SEM must not know the uniqueness of information owner, difficulty will minimize the hope positioned on conditions of information privacy and uniqueness privacy.

In [6] presented the multi collection input administration accomplish the hierarchical right to use manage through apply a incorporated input chart too managing the group key for dissimilar user among numerous right to use establishment. Central key organization arrangement use hierarchy organization to reduce information processing, message as well as storage overhead. Which maintain thing connected toward key along with too update. It accomplishes a incorporated input chart for each customer. A further approach in favor of allocation encrypted information is Attribute-Based Encryption (ABE) [7], possible to encrypt the information among attribute. A user input as well as the attribute match that be able to decrypt the exacting cipher text. While presenting k attribute be cover between cipher texts as well as private key the decryption be approved. A communication, calculation, with storage outlay be minimize similar to central approach.

Chu et al. [8] consider how to decrease the amount of dispersed data encryption key. On the way to divide numerous papers among dissimilar encryption key among similar customer, data landlord resolve require to allocate every one such key to him/her in a conventional move toward which is typically not practical. Aim at this challenge, key aggregate Encryption (KAE) system for data allocation is projected to produce aggregate key for the user to decrypt the entire papers.

Popa [9] firstly introduces the concept of multi-key searchable encryption (MKSE) and puts forward the first feasible scheme in 2013. MKSE allows a user to provide a single keyword trapdoor to the server, but still allows the server to search for that trapdoor's keyword in documents encrypted with different keys. This might sound very similar to the aim of KASE, but these are in fact two entirely dissimilar concept. The aim of KASE is to hand over the keyword investigate accurate to some customer through distribute the collective input to him/her in a cluster information distribution scheme, while the aim of MKSE is to guarantee the cloud server be able to execute keyword investigate through single trapdoor more than dissimilar papers owing to a customer.

Gout et al. [10], [11] try to construct Identity-based encryption (IBE) with key aggregation. One of their scheme [10] assume chance oracle except a different [11] do not. Within their scheme, key aggregation be forced in the intelligence to facilitate every key to live aggregated should appear since dissimilar "identity divisions". Whereas present an exponential number of identity as well as therefore a secret keys, simply a polynomial number of them can be aggregated. Mainly prominently, their key-aggregation [10], [11] come at the expenditure of O(n) size for equally cipher texts moreover the public parameter, where n is the number of secret key which be able to be aggregate keen on a stable range single. This significantly increase the cost of store with

transmit cipher texts, which be not practical within numerous situation such as mutual cloud storage.

In [12], presented a proxy re-encryption (PRE) is fine recognized in the direction of various application counting cryptographic folder scheme. However, Alice have to faith proxy with the purpose it simply convert cipher texts according toward her teaching, which is what we desire to keep away from at the initial position. Still bad, if the proxy collude through Bob, several structure of Alice's private key be able to improve which be able to decrypt Alice's (convertible) cipher texts devoid of Bob's extra assist. That moreover means that the alteration input of proxy must survive fine sheltered. Use PRE presently moves the protected input storeroom necessity since the hand over to the substitute. It is therefore disagreeable to allow the proxy exist in the storeroom server. Which would as fine exist not suitable although each decryption require break up communication through the proxy.

III. SYSTEM ARCHITECTURE

As shown in Fig. 1, the trusted authority be able to create the particular stable range decryption input KS which combines a extracts privileges to every information module on S, as well as they utilize the unrestricted input structure that broadcast the input to the aim place for user $\hat{S}$ structure for small overhead broadcast collective input K(S, $\hat{S}$) .

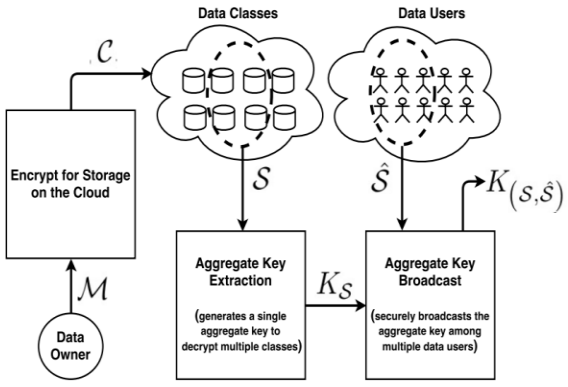

Fig.1. System Architecture

The proposition is to permit trusted authority to join the decryption authority of numerous information modules with in a particular input stable size. Whereas every category of information will be encrypt by the dissimilar unrestricted input, particular decryption input for stable range enough towards decrypt some split the module. Structure will be commonly called key-aggregate cryptosystem (KAC), moreover derive heredity beginning influential occupation happening broadcast encryption through Boneh et.al. [21]. KAC might basically live consider like double idea of broadcast encryption [21]. In broadcast encryption, particular cipher text is broadcast between numerous user, every might decrypt a similar use individual personal input. In KAC, the particular collective input is scattered among numerous user as well as might use to decrypt cipher texts encrypted among value towards dissimilar module. On behalf of broadcast encryption, a centre will have small cipher texts along with little transparency individual decryption key, whereas in KAC, a centre will have small cipher texts as well as small overhead collective key.

KAC will be company with 5 randomized polynomial-time algorithms. A organization manager in charge on behalf of set a unrestricted parameter through a Setup process. The information holder enthusiastic towards divide up the information use the organization register towards receiving the individual unrestricted as well as personal input pair generate use a KeyGen process. A information holder in charge on behalf organize each one of her information records/letters into a particular category i. Each communication be therefore encrypted through an Encrypt function moreover store on a server. While delegate the extraction privileges the exact split of communication module, information landlord use a remove process making the stable range collective extraction input single a split. At last, the certified information customer be able to utilize the collective input a extract some communication belong some category.

IV. PROPOSED WORK

The KAC construction might live powerfully extensive moreover shared among broadcast encryption scheme for distribute a collective input between a random amount information user through protected channel. Nevertheless, in a genuine earth information contribution company through information user moreover information owner, such answer require survival of safe channel, which is enormously expensive. In addition, the animatedly rising environments of the system imply that the necessity for safe channel increase in a multiplicative style by each fresh information landlord/customer combination the system. Which make the fundamental KAC system not convenient for huge size employment in spite of its cryptographically safe aggregate key creation property.

In this section, we build up a narrative instrument for public-key based aggregate key sharing which reduce the safe way necessity. They utilize broadcast encryption, that will be fine recognized method within public key cryptography, to powerfully share out a collective key between various user in a safe style.

Our extensive KAC creations use centre structure block which support B information module as well as B information user. A plan will jog (A×$\hat{A}$) instance the block within equivalent, for example generally scheme could grip n = A × B information module as well as m = $\hat{A}$ × B data user. Structure block divide up the similar place for unrestricted parameter, however utilize the individual place for personal as well as unrestricted input mechanism. Construct unrestricted constraint amount among a unrestricted input range along with a collective input range, whereas unmoving maintain stable cipher text transparency.

A structure in favor of comprehensive KAC among collective input broadcast be accessible below:

A) Setup (1λ , n, m):

Take the key as amount of information module n, a amount of user m along with a safety constraint λ. Output a unrestricted constraint pram.

B) OwnerKeyGen ():

Output the public key PK, the master-secret key msk and the broadcast secret key bsk for a data owner registering in the system.

C) Owner Encrypt(pram, PK, i, M):

Take the key as information category i ∈ {1, · · · , n} along with plaintext information M. output moderately encrypted cipher text C . Notice C be won't a last cipher text doesn't show to outside earth. Which send scheme manager through the protected channel for additional alteration like describe after that. Reminder now that some instantiation of system should make sure that incomplete cipher text C is sheltered using appropriate randomizations thus escape not anything regarding the primary plaintext data M throughout communication will be the structure manager.

$$\mathcal{C}' = (c_0, c_1', c_2, c_3) = (tQ, tPK_2^a, t(PK_2^a + Q_b), \mathcal{M} \cdot e(P_B, tQ_1))$$

D) System Encrypt(C,msk,bsk):

Take key as incomplete encrypted cipher text C, master secret key msk and the broadcast secret key bsk. Output a last cipher text C which will be accessible in a cloud. The step is carry out through scheme manager, who is a trusted third party.

E) UserKeyGen(pram, msk,i):

Take the key information customer id i ∈ {1, · · · , m} along with output a corresponding underground input dˆ

F) Extract(param, msk, S):

Take the key master secret key msk along with the split the information module $\hat{S}$ ⊆ {1, · · · , n}. Compute collective input KS in favor of every encrypted mail belong to this split module, as well as pass key to the Broadcast algorithm for generating the broadcast aggregate key.

$$K_{\mathcal{S}} = msk \sum_{j \in \mathcal{S}} P_{n+1-j} = \gamma \sum_{j \in \mathcal{S}} P_{n+1-j}$$

G) Broadcast (param, KS ,$\hat{S}$,PK, bsk):

Take the key as collective input KS as well as aim separation for user S ⊆ {1, · · · , m}. Output the particular broadcast collective input K(S, $\hat{S}$) which allow some customer $\hat{i}$ ∈ $\hat{S}$ who extract every encrypted information/letters classify them into any category i ∈ S.

$$K_{(\mathcal{S},\hat{\mathcal{S}})} = (\hat{t}Q, \mathcal{K}_1, \mathcal{K}_2)$$

***H) Decrypt*(param,C,K(S,$\hat{S}$),i,d_i,S,$\hat{S}$):**

A decryption steps currently take, further cipher text C moreover the parallel information class i ∈ S, a applicable customer id $\hat{i}$ ∈ $\hat{S}$. Which acquire the key with broadcast collective input K(S, $\hat{S}$) along with the underground input d_i. An algorithm output an extracted letter.

V. PERFORMANCE EVALUATION

This segment present an investigational legalization of the presentation moreover effectiveness of the extensive KAC manufacture through broadcast collective input on the unrestricted network base system consists the 3 VMs - information landlord customer VM to perform that Encrypt operation, information customer VM which perform a extract process, as well as the trust third party cloud VM to perform a break operation. Every two client VMs be prepared among 1GB RAM every, though server VM be prepared among 4GB RAM while performing largeness of computational operation.

Consider that: 1) Within the realistic information allocation scheme base taking place cloud storage, customer be able to regain information with some achievable tool be broadly use at the present; 2) A presentation be extremely reliant taking place the fundamental cryptographic operation particularly within union calculation, learn whether cryptographic operation base taking place union calculation be able to proficiently execute using computer plans.

A. Execution time of Encrypt:

Execution time on behalf of generate the cipher text section (suppose a landlord choose toward encrypt a cipher text use the fresh secret) equivalent toward the information module. Encrypt algorithm simply desires 206 second within computer, but

10018 second within cellular phone strategy. Which will be practicable toward upload plenty of paper moreover investigate among union calculation be able to execute speedily within computer currently.

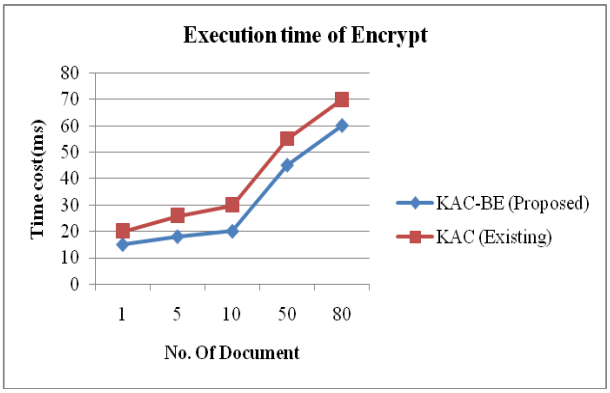

Fig. 2. Comparison of Execution time of Encrypt

B. Execution time of Decrypt:

Execution time for generating a decrypt component (if the data user chooses to decrypt the ciphertext using a new aggregate broadcast key) corresponding to a data classes. Which essentially resources a method will be broadcasting the collective input in favor of 100 papers for 100 user?

They examine a predictable moment difficulty of a mixture of algorithm within comprehensive KAC within the situation, base of the amount for ancient operation on every step. They evaluate them among a real moment necessary of every step on simulated structure of comprehensive KAC. They position a extra overhead above a predictable moment necessary of every step might recognized to system delay along with time necessary toward serialize a variety of collection fundamentals in favor of input and output.

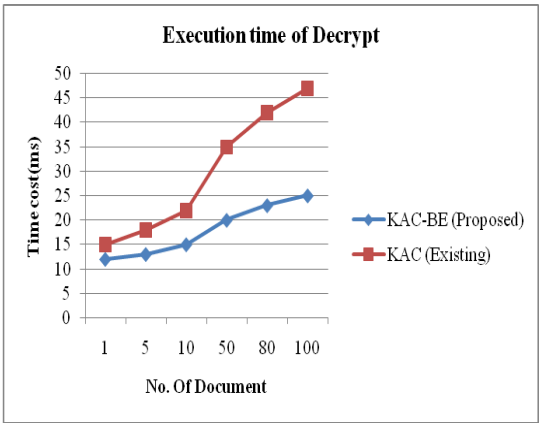

Fig. 3. Comparison of Execution time of Decrypt

VI. CONCLUSION

In this project, extended KAC creation is the completely involvement challenging along with protected alongside the non-adaptive opponent below suitable security assumption. They include established that the basic KAC framework may be capably extensive along with comprehensive on behalf of strongly broadcasting aggregate key between various information users within a real-life information allocation situation. Which provide the essential path within scheming the scalable completely public-key base online information allocation system on behalf of large-scale employment taking place on cloud. They present reproduction outcome toward confirm a gap along with time difficulty necessities in favor of scheme. A outcome launch to facilitate KAC among aggregate key broadcast outperforms extra existing protected information allocation scheme into provisions performance along with scalability.

REFERENCES

[1] Sherman SM Chow, Yi-Jun He, Lucas CK Hui, and Siu Ming Yiu. Spice–simple privacy-preserving identity-management for cloud environment. In Applied Cryptography and Network Security, pages 526–543. Springer, 2012.

[2] Cong Wang, Sherman S.-M. Chow, Qian Wang, Kui Ren, and Wenjing Lou. Privacy-preserving public auditing for secure cloud storage. Cryptology ePrint Archive, Report 2009/579, 2009. http://eprint.iacr.org/.

[3] Sherman SM Chow, Cheng-Kang Chu, Xinyi Huang, Jianying Zhou, and Robert H Deng. Dynamic secure cloud storage with provenance. In Cryptography and Security: From Theory to Applications, pages 442–464. Springer, 2012.

[4] K. Ren, and W. Lou , Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing, Apr.2010.

[5] Ming Li, and Hui Li, Storing Shared Data on the Cloud via Security-Mediator, Jul. 2013.

[6] Yan Sun and K. J. Ray Liu, Scalable Hierarchical Access Control in Secure Communications, Mar. 2004.

[7] Sushmita Ruj and Amiya Nayak, Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds, Feb.2014.

[8] C. Chu, S. Chow, W. Tzeng, et al. "Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage", IEEE Transactions on Parallel and Distributed Systems, 2014, 25(2): 468-477.

[9] R. A. Popa ,N. Zeldovich. "Multi-key searchable encryption". Cryptology ePrint Archive, Report 2013/508, 2013.

[10] F. Guo, Y. Mu, and Z. Chen, "Identity-Based Encryption: How to Decrypt Multiple Ciphertexts Using a Single Decryption Key," in Proceedings of Pairing-Based Cryptography (Pairing '07), ser. LNCS, vol. 4575. Springer, 2007, pp. 392–406.

[11] F. Guo, Y. Mu, Z. Chen, and L. Xu, "Multi-Identity Single-Key Decryption without Random Oracles," in Proceedings of Information Security and Cryptology (Inscrypt '07), ser. LNCS, vol. 4990. Springer, 2007, pp. 384–398.

[12] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage," ACM Transactions on Information and System Security (TISSEC), vol. 9, no. 1, pp. 1–30, 2006.

[13] M. Chase and S. S. M. Chow, "Improving Privacy and Security in Multi-Authority Attribute-Based Encryption," in ACM Conference on Computer and Communications Security, 2009, pp. 121–130.

[14] T. Okamoto and K. Takashima, "Achieving Short Ciphertexts or Short Secret-Keys for Adaptively Secure

General Inner-Product Encryption," in Cryptology and Network Security (CANS '11), 2011, pp. 138–159.

[15] R. Canetti and S. Hohenberger, "Chosen-Ciphertext Secure Proxy Re-Encryption," in Proceedings of the 14th ACM Conference on Computer and Communications Security (CCS '07). ACM, 2007, pp. 185–194.

[16] C.-K. Chu and W.-G. Tzeng, "Identity-Based Proxy Re-encryption Without Random Oracles," in Information Security Conference (ISC '07), ser. LNCS, vol. 4779. Springer, 2007, pp. 189–202.

[17] C.-K. Chu, J. Weng, S. S. M. Chow, J. Zhou, and R. H. Deng, "Conditional Proxy Broadcast Re-Encryption," in Australasian Conference on Information Security and Privacy (ACISP '09), ser. LNCS, vol. 5594. Springer, 2009, pp. 327–342.

[18] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, "Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records," in Proceedings of ACM Workshop on Cloud Computing Security (CCSW '09). ACM, 2009, pp. 103–114.

[19] G. Ateniese, A. D. Santis, A. L. Ferrara, and B. Masucci, "Provably-Secure Time-Bound Hierarchical Key Assignment Schemes," J. Cryptology, vol. 25, no. 2, pp. 243–270, 2012.

[20] R. S. Sandhu, "Cryptographic Implementation of a Tree Hierarchy for Access Control," Information Processing Letters, vol. 27, no. 2, pp. 95–98, 1988.

[21] Dan Boneh, Craig Gentry, and Brent Waters. Collusion resistant broadcast encryption with short ciphertexts and private keys. In Advances in Cryptology–CRYPTO 2005, pages 258–275. Springer, 2005.