ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 1, January 2017

A Survey on Advanced Multi-Authority Access Control System for Public Cloud Storage

Gangeshkumar Rahangdale[1], Prof. Archana Raut[2]

M.Tech Student, Dept. of Computer Science & Engineering, G.H.R.C.E, Nagpur, India[1]

Professor, Dept. of Computer Science & Engineering, G.H.R.C.E, Nagpur, India[2]

ABSTRACT: Attribute Base Encryption (ABE) is a tool to assurance data owner's control above their data in public cloud storage. The proposed Attribute Base Encryption system include one and only power to keep up the entire trait set, which can carry a single point bottleneck problem on both safety and execution. In this way, some multi-power plans are proposed, in which various powers independently keep up disjoint trait subsets. In any case, the single-point bottleneck issue stays unsolved. In the proposed work, we have developed a system which will provide the data security in trusted as well un-trusted cloud environments. The system will focus long communication scenario between data owner, CA, user and authorities as well TTP using different security techniques, it will provide highest security than all existing approaches.

KEYWORDS: Cloud Computing, CP-ABE, CA, KP-ABE, Cipher text, TTP.

I. INTRODUCTION

To fulfil basic prerequisites of information data storage and elite estimation, cloud computing has drawn tremendous considerations from both industry and academic. cloud storage is an imperative utility of distributed computing [1], which gives administrations to information proprietors to convey information to store in cloud through Internet. In existing CP-ABE plans [3], [5], [6], [7], there is just a single power in charge of key appropriation and characteristic administration.

This one and only power plan can take a solitary point bottleneck issue on both execution and security. Once the power is concurred, an assailant can without much of a stretch get the one and only master key, then he/she can create keys of attributes to unscramble/decrypt the encoded information. Additionally, once the authority is smashed, the framework can't function admirably. Regardless of the possibility that some multi-authority cryptographic plans [2], [4], [10] has proposed, despite everything they can't deal with the bottleneck issue on both security and execution cited previously. In these multi-authority encryption scheme, the whole quality set is partitioned into different separate subsets and every characteristic subset is still overseen by single power. However, the aggressor can't increase private keys of all characteristics in the event that he/she hasn't concurred all authorities. In addition, the foe can acquire private keys of specific traits by altering specific at least one powers. What's more, the single-point congestion on execution is not yet tackled in these multi-power CP-ABE plans.

In this research work, from another viewpoint, we organize a limit multi-authority ABE get to control conspire for open distributed storage, in which numerous powers together deal with a uniform attribute set. In this research work, preferred standpoint of (t; n) edge secret sharing, the private key can be imparted to numerous powers, and an approved client can create his/her secret key by communicating with any t authority. performance and security execution examination comes about demonstrate that Threshold Multi-Authority System [1] is not just testable secure when not as much as t powers are concurred, additionally vigorous when no not as much as t powers are alive in the framework. Besides, by easily consolidating the great multi-power plot with Threshold Multi-Authority System, we build up a half and half one, which fulfils the diagram of characteristics originating from individual powers and in addition accomplishing framework level heartiness. Every Attribute (AA) and Trusted Third Party (TTP) will free quality effect that is responsible for entitling and revoking customer's credits as demonstrated by their part or identity in its range. In

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 1, January 2017

our arrangement, every trademark is associated with a singular AA, yet every AA can manage a self-decisive number of characteristics. Every AA has full control over the structure and semantics of its qualities. Each AA is accountable for delivering an open trademark key for each property it supervises and a riddle key. For each customer reflecting his/her properties. Fundamental commitments of this work can be given as takes after:

- In ABE scheme information stockpiling that prompts to single-point bottleneck issue on execution and security against the just a single power for any attribute authority. To the best of our insight, we are the first to propose an architecture with joint effort of AA and TTP to manage the issue and secret key sharing.
- By presenting the threshold secret sharing (t;n) and ABE scheme with trusted third party, we propose and perceive a verifiable and vigorous multi-power get to control framework out in the open cloud, in which various authorities and TTP together deal with a secret key sharing.

Furthermore, by efficiently coordinating the established multi-authority conspire with our own, we develop a half breed one, which fulfils the situation of properties originating from various powers and in addition accomplishing security and framework level strength.

II. RELATED WORK

Wei Li, et al. [1] proposed a multi-authority system get to control framework to manage the bottleneck issue. By presenting the combination of (t, n) edge secret sharing and CP-ABE technique. In which different powers together deal with a homogeneous property set. Assist by easily connecting the old scheme with this plan, develop a cross breed one, which can catch the situation of properties landed from various powers and additionally accomplishing framework level vigor.

Hong, et al. [2] proposed a Data Access Control Systems for cloud. Client can change the just scrambled/encrypt cipher text to a before variant, which can be further unscrambled/decrypt with his/her review old-adaptation secret keys. Creator additionally proposed a multi-power ciphertext-arrangement attribute based encryption, information get to control for distributed storage, in which the creators suggested that the instrument in taking care of with characteristic renouncement could accomplish in reverse security and forward security.

Jung, et al. [3] proposed a semi-mysterious and a completely unknown characteristic based benefit control conspire to indicate the client protection issue in an open cloud. The proposed framework could ensure client's security against every power. Partial data is reveal in AnonyControl. This method was vigorous against power alteration, and trading off of up to (N −2) powers did not convey the entire framework down.

Yang, et al. [4] proposed a fluctuating scheme, where dynamic and secures fluctuating strategy acquainted with take care of the trait change issue in the framework. Property variance strategy is alterable as in it procure less calculation and correspondence cost, and is secure as in it can finish both in reverse and forward security. This plan doesn't require the server to be dependable, in light of the fact that the key redesign is forced by every quality power not the server.

Wei Teng et al. [5] recommend a progressive cipher text policy quality based encryption (CP-ABE) get to control plot for steady size cipher text. It is an orderly plan in light of the fact that the length of ciphertext and the quantity of bilinear matching estimation to a steady are settled, which update the adequacy of the framework and keep away from the additional overhead of capacity. The plan is versatile, adaptable, and issue fine-grained get to control of drew in information in distributed computing.

Baojiang Cui et al. [6] propose a key total searchable encryption (KASE) plot. The proposed KASE conspire enroll to any distributed storage that backings the assessed bunch information sharing usefulness, which implies client may especially impart a gathering of chose records to specific clients, while permitting the last to perform catchphrase look over the previous. Here an information proprietor just needs to issue a solitary key to a client for dispersing an expansive number of information and the client just needs to present a solitary trapdoor to the cloud for enquiring the common information.

Hua Deng et al. [7] proposed a cipher text-approach various leveled ABE (CP-HABE) plot with short cipher text. In this examination work, the characteristics are requested in a grid and the clients have more elevated amount traits can exchange their get to controls to the clients having lower level properties. This property empowers a CP-HABE plan to give countless from various associations by approved keys.

Jin Li et al. [8] built up a Secure Outsourced ABE plot, which help both key-issuing and decoding. It empties all get to approach and property related capacities in the key-issuing procedure or decoding to a Key Generation Service Provider (KGSP) and a Decryption Service Provider (DSP) separately, disregard just a consistent number of

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 1, January 2017

straightforward operations for AA and qualified clients to perform locally. It likewise gives adequate states of the outsourced brings about a successful way.

Ge et al. [9] the past CP-ABE plan was just secure against picked plaintext assaults (CPA), which was excruciating to acquire security versus picked cipher text assaults (CCA). Thus A. Ge et al. built up a Threshold CP-ABE conspire with consistent size cipher text, which gives security fortress both CPA and CCA plot.

Kan Yang and Xiaohua Jia [10] proposed a get to control structure for multi-power frameworks with effective and secure multi-power get to control conspire for distributed storage. An effective multi-power CP-ABE conspire don't require a worldwide power. It just backings any LSSS get to structure. They likewise composed another procedure to take care of the quality renouncement issue in multi-authority CP-ABE frameworks.

S. Ruj et al. [11] proposed a DACC (Distributed Access Control in Clouds) get ready for information stockpiling and access in mists. This plan dispose of different encoded duplicates of same information. Cloud stores encoded information for secure information stockpiling. The fundamental preferred standpoint of this plan is aggregate of key circulation focuses (KDCs). In DACC at least one KDCs appropriate keys to information proprietors and clients. KDC may offer access to specific fields in all records. In this way, a solitary key replaces random keys from information proprietors. Proprietors and clients are designate sure arrangement of traits. Encoded information with the traits stores in the cloud. DACC likewise bolsters disavowal of clients, without resending keys to every one of the clients of cloud administrations.

H. Lin et al. [12] proposed a MA-FIBE encryption plot without a focal power. In this exploration work an encrypted can encode a message with the end goal that a client could unscramble just on the off chance that he has no less than one key of the given properties about the message for in any event t+1 powers; t <= n/2 legitimate powers of all the n property powers are available in the proposed plot.

Allison Lewko et al. [13] proposed two completely secure useful cryptographic methods, a completely secure characteristic based encryption (ABE) plan and trait concealing predicate encryption (PE) plot for inward item predicates. Both of these plans contract the double framework philosophy to exhibit full security.

M. Pursue et al. [14] proposed a multi-power ABE with client security and without the trusted power. It supplants the trusted focal power and ensures the client's protection by stopping the powers from pooling their data on specific clients, accordingly making ABE more utilizable by and by.

Keita Emura et al. [15] proposed another plan, Cipher text Policy Attribute-Based Encryption (CP-ABE) steady length of the quantity of blending calculation and cipher text. Get to structure utilized as a part of this plan is worked by AND entryways on numerous property estimations. Moreover, the quantity of extra bits required from picked plaintext assault secure CP-ABE to picked cipher text assault CP-ABE is lessened by 90% as for that of the early procedure.

Vipul Goyal et al. [16] proposed the primary making of a CP-ABE plot having a security evidence in light of an extraordinary number theoretic supposition and supporting propelled get to controls. It bolsters developments which can be displayed by a limited size get to tree with edge rationale doors. The bound on the span of the get to trees is taken at the season of the framework setup and is spoken to by a tuple (d, num) where d speaks to the greatest profundity of the get to tree and num speaks to the most extreme number of tyke each non-leaf hub of the tree.

John Bethencourt et al. [17] proposed CP-ABE conspire. In this examination work, trait arrangements are coordinated with information and qualities are incorporated with keys. Just those keys whose coordinated characteristics fulfill the arrangement incorporated with the information can unscramble it. By utilizing this strategy scrambled information can be kept private regardless of the possibility that the capacity server is suspicious.

III. PROPOSED METHODOLOGY

The proposed research work has been distributed into 5 different stages these are below.

1) Authorities Aa first registers to CA to get (aid,aid.cert)
2) User register to CA to get (uid, uid. cert)
3) User gets his/her SK from any t out of n Aas as well as TTP
4) Owners get PK from CA
5) Owners upload (CT) to the cloud server.
6) Users download (CT) from the cloud server.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 1, January 2017

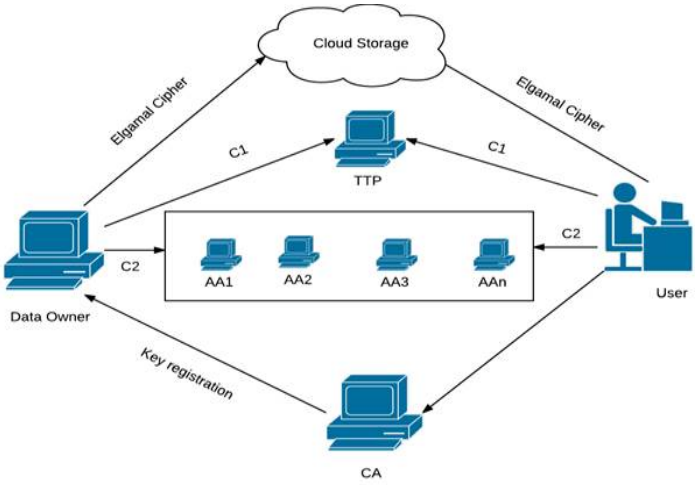

Fig. 1: System Architecture

There are six sorts of substances in the framework as in Fig 1: an endorsement power (CA), trademark powers (AAs), information proprietor (proprietors), the cloud (server) and information purchasers (clients). The CA is a worldwide trusted testament power in the plan. It sets up the framework and acknowledges the enlistment of the considerable number of clients and AAs in the framework. For each legitimate client in the framework, the CA appoint a worldwide one of a kind client character to it furthermore produces a worldwide open key for this client. Be that as it may, the CA is not included in any property association and the development of mystery keys that are associated with quality. For occurrence, the Certificate Authority can be the Social Security Administration, an autonomous office of the US government. Every client will be issued a Social Security Number (SSN) as its worldwide personality. Each AA and TTP will free trait impact that is in charge of entitling and repudiating client's credits as indicated by their part or personality in its area. In our plan, each characteristic is connected with a solitary AA, yet every AA can deal with a self-assertive number of qualities. Each AA has full control over the structure and semantics of its qualities. Every AA is in charge of producing an open characteristic key for every property it oversees and a mystery key. For every client mirroring his/her properties. Table captions appear centred above the table in upper and lower case letters. When referring to a table in the text, no abbreviation is used and "Table" is capitalized.

IV. Conclusion and Future Work

To the best of our knowledge we proposed a revocable decentralized information system get to control framework can bolster effective characteristic denial for multi-authority cloud storage systems. It kills decoding overhead of clients as indicated by properties. This safe characteristic based encryption system for powerful information security that is being part taken in the cloud. This revocable multi-authority data access scheme with obvious outsourced decoding and it is secure and undeniable. This scheme will be a promising procedure, which can be applied in any remote storage framework. In future, we introduce the efficient user revocation system on top of proposed anonymous ABE. Supporting client revocation is an essential issue in the genuine application, and this is one of the greatest challenges in the application of CP-ABE technique.

References

1. Wei Li, KaipingXue, YingjieXue, and Jianan Hong, "TMACS: A Robust and Verifiable Threshold Multi-Authority Access Control System in Public Cloud Storage", IEEE Transactions on Parallel and Distributed Systems, DOI 10.1109/TPDS.2015.2448095.
2. Jianan Hong, KaipingXue and Wei Li, "Comments on "DAC-MACS: Effective Data Access Control for Multi-Authority Cloud Storage Systems"/Security Analysis of Attribute Revocation in Multi-Authority Data Access Control for Cloud Storage Systems", IEEE transactions oninformation forensics and security, VOL. 10, NO. 06, June 2015.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 1, January 2017

3. Taeho Jung, Xiang-Yang Li, Zhiguo Wan, and Meng Wan, "Control Cloud Data Access Privilege and Anonymity with Fully Anonymous Attribute-Based Encryption", IEEE transactions on information forensics and security, VOL. 10, NO. 01, January 2015.
4. Kan Yang and Xiaohua Jia, "Expressive, Efficient, and Revocable Data Access Control for Multi-Authority Cloud Storage", IEEE Transactions on parallel and distributed systems, VOL. 25, NO. 07, July 2014.
5. Wei Teng, Geng Yang, Yang Xiang, Ting Zhang and Dongyang Wang, "Attribute-based Access Control with Constant-size Ciphertext in Cloud Computing", IEEE Transactions on Cloud Computing, DOI 10.1109/TCC.2015.2440247.
6. Baojiang Cui, Zheli Liu and Lingyu Wang, "Key-Aggregate Searchable Encryption (KASE) for Group Data Sharing via Cloud Storage", IEEE Transactions on computers, vol. 6, no. 1, January 2014.
7. H. Deng, Q. Wu, B. Qin, J. Domingo-Ferrerd and L. Zhang, "Ciphertextpolicy hierarchical attribute-based encryption with short ciphertexts", Information Sciences, vol.275, pp:370-384,2014.
8. Li, X. Huang, J. Li, X. Chen, and Y. Xiang, "Securely outsourcing attribute-based encryption with checkability", IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 8, pp. 2201–2210, 2014.
9. A. Ge, R. Zhang and C. Chen, "Threshold Ciphertext Policy AttributeBased Encryption with Constant Size Ciphertexts", Public Key Cryptography: 13th International Conference on Practice and Theory in Public Key Cryptography (PKC2010), LNCS7372, pp: 336-349, 2012.
10. Kan Yang, Xiaohua Jia, "Attributed-based access control for multiauthority systems in cloud storage", in Proceedings of IEEE 32nd International Conference on Distributed Computing Systems. IEEE, 2012, pp. 536–545.
11. S. Ruj, A. Nayak, and I. Stojmenovic, "Dacc: Distributed access control in clouds", in Proceedings of the 10th IEEE International Conference on Trust, Security and Privacy in Computing and Communications. IEEE, 2011, pp. 91–98.
12. H. Lin, Z. Cao, X. Liang, and J. Shao, "Secure threshold multiauthority attribute based encryption without a central authority", Information Sciences, vol. 180, no. 13, pp. 2618–2632, 2010.
13. A. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters, "Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption", in Proceedings of the 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques. Springer, 2010, pp. 62–91.
14. M. Chase and S. Chow, "Improving privacy and security in multiauthority attribute-based encryption", in Proceedings of the 16th ACM conference on Computer and communications security. ACM, 2009, pp. 121–130.
15. K. Emura, A. Miyaji, A. Nomura, K. Omote and M. Soshi, "A ciphertext-policy attribute-based encryption scheme with constant ciphertext length", Information Security Practice and Experience: 5th International Conf. (ISPEC 2009), LNCS5451, pp:13-23, 2009.
16. V. Goyal, A. Jain, O. Pandey, and A. Sahai, "Bounded ciphertext policy attribute based encryption", in Proceedings of the 35th International Colloquium on Automata, Languages and Programming. Springer, 2008, pp. 579–591.
17. J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attributebased encryption", Proceedings of IEEE Symposium on Security and Privacy. IEEE, 2007, pp. 321–334.

BIOGRAPHY

Gangeshkumar Rahangdale is a M. Tech student from G.H Raisoni College of Engineering, Nagpur(An Autonomous Institute Affiliated to RTM Nagpur) he has completed his Bachelor of Engineering in Information Technology from G. H Raisoni College of Engineering, Amravati in the year 2014. He is interested in cloud computing, Networking, and has greater interest in programing languages

Archana Raut is anAssistant Professor at the G.H Raisoni College of Engineering, Nagpur (An Autonomous Institute Affiliated to RTM Nagpur) she has completed a Post graduate degree in Computer Science Engineering (WCC) at the RTMNU, NagpurShe took up his first post as an Assistant Professor at the G.H Raisoni College of Engineering, Nagpur (An Autonomous Institute Affiliated to RTM Nagpur). Her area of interest includesCommunication, Database management system, Operating systems, Mobile operating system, Data mining and Data warehouse.