JCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Special Issue, 6, March 2019 E-ISSN: 2347-2693

A Study on Secure Sharing of Application Data in Cloud Computing

P. Kiran Kumar Naik[1*], GV. Ramesh Babu[2]

[1]Dept. of Computer Science, SVU College of CM&CS, Tirupathi, India
[2]Dept. of Computer Science, SV University, Tirupathi, Andhra Pradesh,

Corresponding Author: palthya.kirankumar@gmail.com

DOI: https://doi.org/10.26438/ijcse/v7si6.162166 | Available online at: www.ijcseonline.org

Abstract: Cloud clients utilizes "Cloud storage" administration to have their information in the cloud. Get to control benefit gave by cloud is accustomed to giving assurance against unapproved access to information. Cipher text-Policy Attribute-Based Encryption (CP-ABE) is generally considered for information get to control in distributed storage. The current CP-ABE is hard to apply in multi-specialist distributed storage because of the characteristic repudiation issue. The proposed revocable multi-specialist CP-ABE plot gives answer for the characteristic denial issue. The proposed plot refreshes the segments of the disavowed quality just and produces most recent mystery keys for the repudiated credit and advances it to the non renounced clients who have the properties as denied traits. The Backward security and Forward security is kept up. On the off chance that the repudiated client goes into the framework again by doing the enlistment procedure implies, the specific client is recognized by means of the character card detail in the renouncement rundown and they are not permit in the framework, so that these clients are halted at the enrolment stage itself.

Keywords: Cloud Storage, Security, Cloud, Privacy

I. Introduction

Appropriated handling, parallel preparing and framework figuring together developed as distributed computing. In the distributed computing client information is not put away locally but rather is put away in the server farm of web. The distributed computing utilizes innovation perception for all gave administrations. It is utilized for speculation of the registering assets. The fluctuates organizations which give distributed computing administration are in charge of overseeing could and keep up the operation of these server farms. The clients can get to the put away information whenever by utilizing Application Programming Interface (API) gave by cloud suppliers through any terminal hardware associated with the web. Storage administrations gave as well as equipment and programming administrations are accessible to the overall population and business markets.

A. Multiauthority Storage

In Multi-Authority stockpiling frameworks, there will be numerous authorities[5].Users may store qualities issued by various locales and information proprietors may likewise share the information utilizing access approach characterized over characteristics from various specialists. Clients qualities are changed powerfully in multi-expert distributed storage frameworks. A client can allow some new traits or renounced some current dole out properties.

II. Related Work

Cloud computing servers gives promising stage to capacity of information. Sharing of individual medicinal records is a turned out to be obvious patient driven model of wellbeing data trade, which is frequently outsourced to store at outsider, for example, cloud suppliers Attribute based encryption (ABE) methods to scramble every patient's restorative record document. The system depicts another component which empowers secure capacity and controlled sharing of patient's wellbeing information. Strategy investigate Key Policy Attribute Based Encryption (KPABE) and Multi Authority Attribute Based Encryption to implement quiet get to control arrangement with the end goal that every one of the clients of framework can download the information ,yet just approve client can see the therapeutic records. system of secure sharing of individual medicinal records in distributed computing, use different types of ABE to scramble the therapeutic record documents, so patients can permit get to by individual clients, as well as different clients from open areas with various expert parts, capabilities and affiliations[8].Advantages of procedure are:1.Multiple security domains.2.Reduce the key administration many-sided quality for proprietors and users.3.A high level of patient protection is ensured by abusing multi-specialist ABE structure. Constraints of strategy are: 1.The structure addresses the one of a kind difficulties brought by different proprietors and users.2. Putting away individual medicinal records on the cloud server prompts to need of Encryption Mechanism.

The new system for acknowledging Cipher content Policy Attribute Encryption (CP-ABE)[3] under cement and non intuitive cryptographic presumptions in the standard model. Arrangements permit any encode to indicate get to control regarding any get to method for the characteristics show in the framework. In most customer framework, figure Text size, encryption, and unscrambling time scales straightly with the many-sided quality of the get to system. The main past work to accomplish these parameters was constrained to a proof in the bland gathering model. Three developments inside our structure [7]. In the first place framework is demonstrated specifically secure under a supposition that we call the decisional Parallel Bilinear Diffie-Hellman Exponent (PBDHE) supposition which can be seen as a speculation of the BDHE suspicion. Next two developments give execution exchange off to accomplish provable security individually under the (weaker) decisional Bilinear-Diffe-Hellman Exponent and decisional Bilinear Die-Hellman presumptions. Procedure introduced the figure content strategy trait based encryption frameworks that are e customer, expressive, and provably secure under solid suspicions. All of developments fall under a typical method of installing a LSSS challenge grid specifically into people in general parameters. Developments give an exchange terms of the multifaceted nature of suspicions [2]. Favourable circumstances of this system are 1.Provide an exchange off as far as productivity and the confusion of assumptions.2.It accomplished comparing expressiveness and effectiveness to the Goyal development, yet in the Cipher content Policy Attribute Based Encryption setting. Restrictions are 1.Framework was constrained to a proof in the non specific gathering model. 2. Issue of finding an expressive CP-ABE framework under a more strong model.

Quality based encryption (ABE) is a compelling cryptographic primitive for accomplishing fine-grained get to control of figure writings. A notable worry in the multi-expert ABE[6] setting is that malevolent clients release their private keys to develop private unscrambling gadgets and appropriate them to illicit clients. To manage this key manhandle issue, method presents the idea of multi-expert property based double crosser following (MABTT), and proposes a solid MABTT conspire. In view of the subgroup conclusion issue for three primes, the MABTT plan is ended up being completely secure by utilizing double framework encryption system. The MABTT framework endorse versatile privateers to be follow [4].Advantages of this system are 1.Permits versatile privateers to be followed 2.To develop a plan which permits a more noteworthy number of key extraction questions by the privateer than our own permits. Burdens are 1.Alleviate the key spillage issue in the settings of multi-specialist ABE.

In a few dispersed frameworks a client ought to just to get to information if a client groups a specific arrangement of qualifications or properties. As of now, the main technique compelling such strategies is to utilize a trusted server to store the information and intercede get to control. In any case, server putting away the information is traded off, then the secrecy of the information will be bargained. Method displays a framework for acknowledging complex get to control on scrambled information that we call Cipher content Policy Attribute-Based Encryption. By utilizing strategy encoded information can be kept private regardless of the possibility that the capacity server is untrusted also, procedure are secure against agreement assaults. Past Attribute-Based Encryption frameworks utilized ascribes to report the scrambled information and incorporated arrangements with client's keys while in our framework credits are utilized to report a client's accreditations, and a gathering encoding information decides an approach for who can unscramble. In this way, strategies are reasonably nearer to since a long time ago settled get to control techniques, for example, Role-Based Access Control (RBAC).In addition[1], Methods give an execution of framework and give execution estimations. Advantages of this system are 1.System permits arrangements to be communicated as any monotonic tree get to structure 2.Resistant to plot assaults in which an assailant may acquire different mystery keys.3.It incorporated a few enhancement procedures. Hindrances are 1.It is progressively hard to ensure the security of information utilizing since quite a while ago settled techniques. 2.Sensitive information is put away in a scrambled shape. 3.Unable to effectively deal with more expressive sorts of encoded get to control.[10] The connection amongst clients and assets is powerful in the cloud, and specialist organizations and clients are ordinarily not in a similar security area. Character based security can't be utilized as a part of an open distributed computing condition, where every asset hub may not be natural, or even don't have any acquaintance with each other. Procedure will concentrate on the accompanying three general classifications of get to control models for distributed computing: (1) Role-based models; (2) Attribute-based encryption models and (3) Multi-tenancy models. Cloud scale to a huge number of physical machines, with significantly more virtual machines included and evacuated, venture level get to control instruments won't be sufficiently adaptable to deal with assaults. Focal points of this method are 1.A inhabitant thus deals with the get to control rundown of the articles claimed by them and the capacity rundown of the subjects having a place with them.2.Cloud get to control is more versatile and vigorous than the ordinary system based procedures. Weaknesses are 1.Due to the multi-tenure model of distributed computing, clients (occupants) of a distributed computing condition incline toward their movement to be disconnected from all other tenants.2.To utilize an incorporated archive for strategies and gathering individuals.

In a character based encryption plot, every client is distinguished by an exceptional personality string. A property based encryption plot (ABE), conversely, is a technique in which every client is recognized by an arrangement of properties, and some capacity of those ascribes is utilized to manage decoding capacity for each figure content. This plan permits any polynomial number of free experts to watch traits and disperse mystery keys. An encode can pick, for every specialist, a number dk and a gathering of qualities; he can then scramble a message with the end goal that a client can just unscramble on the off chance that he has in any event dk of the expressed properties from every expert k. This plan can endure a subjective number of degenerate the specialists [11]. Focal points are 1.Allows any polynomial number of free experts to screen qualities and disperse mystery keys. 2. The arrangement of qualities permitted in every statement must be disjoint . Impediments are 1.In the multi specialist conspire as expressed; every client must go to each expert before he can decode any message. 2. Multi Authority Scheme for Large Universe and Complex Access Structures.

A promising way to deal with alleviate the security chances in Online Social Networks (OSNs) is to move get to control usage from the OSN supplier to the client by methods for encryption. Less demanding, an engineering that backings fine grained get to control system and element amass participation by utilizing trait based encryption. A key and novel component of engineering, notwithstanding, is that it is conceivable to expel access from a client without issuing new keys to different clients or re-encoding existing figure writings. Strategy accomplishes this by making an intermediary that partakes in the unscrambling procedure and authorizes renouncement constraints. The intermediary is insignificantly trusted and can't decode figure messages or give access to beforehand renounce dusters. Method depicts EASIER engineering and development gives execution assessment, and model application. Despite the fact that system demonstrated our approach in an OSN setting, it can be connected to any setting where ABE is actualized. Procedure executed the plan and contrasted it and Bethen court CPABE. Comes about demonstrate that EASIER is versatile as far as estimation and correspondence for OSN's [9]. Points of interest are 1. Trait based encryption frameworks with various sorts of express. 2. Key-Policy ABE and Cipher content Policy ABE catch two fascinating and complimentary. 3. The essential test in this profession is to locate another framework with rich types of expression that deliver more than a self-assertive blend of methods. Detriments are 1.Attribute Based Encryption frameworks utilized ascribes to depict the scrambled information and incorporated approaches with client's keys. 2. While in framework ascribes are utilized to portray a client's qualifications, and a gathering scrambling information decides a strategy for who can decode.

III. Methodology

Multi-expert Ciphertext Policy Attribute Base Encryption (CPABE) is for the most part considered innovation for information get to control in distributed storage frameworks. Clients may hold different qualities issued by numerous specialists. The information get to strategy over the characteristic is characterized by the experts and not by the information proprietors. The current framework is not appropriate for multi-expert distributed storage because of its property renouncement issue. On the off chance that any property is denied implies all the Cipher content related with the expert whose characteristic is renounced ought to be supplanted or refreshed. The current framework depends on a confided in server.

A. Drawbacks

(1) Multi-specialist CP-ABE permits the focal expert to unscramble all the Cipher writings.

(2) It doesn't bolster trait denial.

(3) All the Cipher writings related with the expert whose property is repudiated ought to be supplanted or refreshed.

IV. Results and Discussion

It depends on the single-specialist CP-ABE and it is reached out to multi-expert. This method is connected in multi-authority CPABE convention to join the mystery keys created by various specialists for a client and keeps the intrigue. The worldwide expert is isolated into Certificate Authority (CA) and Attribute Authorities (AA). The CA sets up the framework and enrolment of every client and AA is finished by CA. The CA gives one of a kind character to every client and one of a kind personality to every AA. Property Authority just creates the mystery keys advances it to the client. Every AA creates worldwide open key. It joins the worldwide open key and open key produced by CA for creating the mystery key. The information proprietors first split the information into different segments as indicated by intelligent granularities and outline a get to arrangement for each qualities. The information proprietor encodes the information with substance keys utilizing symmetric encryption calculation. At that point the substance keys are encoded in view of get to strategies of each property and send the scrambled information together with Cipher writings to the cloud. At the point when a property of the client is disavowed, just those segments related with the denied quality in mystery keys and Cipher writings should be refreshed. The AA creates another rendition number for the repudiated trait and produces a refresh key. By utilizing the refresh key, the parts related with the denied property in the Cipher content can likewise be refreshed to the present variant.

The comparing refreshed Cipher messages in cloud additionally refreshed. Notwithstanding this the disavowed client can get to the framework in the wake of doing the enrollment procedure again and get the entrance as per get to control approach. After enrollment the disavowed client may attempt to get to the framework utilizing his/her old validation subtle elements. Along these lines the confirmation points of interest of every last client required in the framework are put away independently. The remarkable personality of the client, for example, Social Security Number (SSN) General Identity card number is included the repudiation list. In the event that the disavowed client goes into the framework again by doing the enrollment procedure implies, the specific client is distinguished through the personality card detail in the repudiation list and won't be added to the framework, so they are halted at the enlistment stage itself. There is the likelihood for the renounced client or outer assailant to hack the token of the current client from the database of the cloud and get to the put away information utilizing the hacked token. To keep from such defencelessness, hash estimation of the token comparing to every client is put away in the database rather than direct token itself. At whatever point client goes into the framework with token, validation is done as takes after: Hash estimation of the token is computed and it is coordinated with the put away hash an incentive in the database. In the event that it is coordinated, they are verified client else their get to is denied.

A. Advantages

(1) The worldwide expert is isolated into Certificate Authority (CA) and Attribute Authorities (AA).

(2) AA joins the worldwide open key and open key created by CA for producing the mystery key. So that the focal specialist was not ready to unscramble the Cipher writings.

(3) Only the segments related with the repudiated property is refreshed and no compelling reason to refresh all the trait parts produced by the specialist which created the disavowed characteristic.

(4) The Cipher content refreshing in cloud empowers the Forward Security.

(5) All the clients are have to hold just the most recent mystery key, no compelling reason to keep records on the past mystery keys.

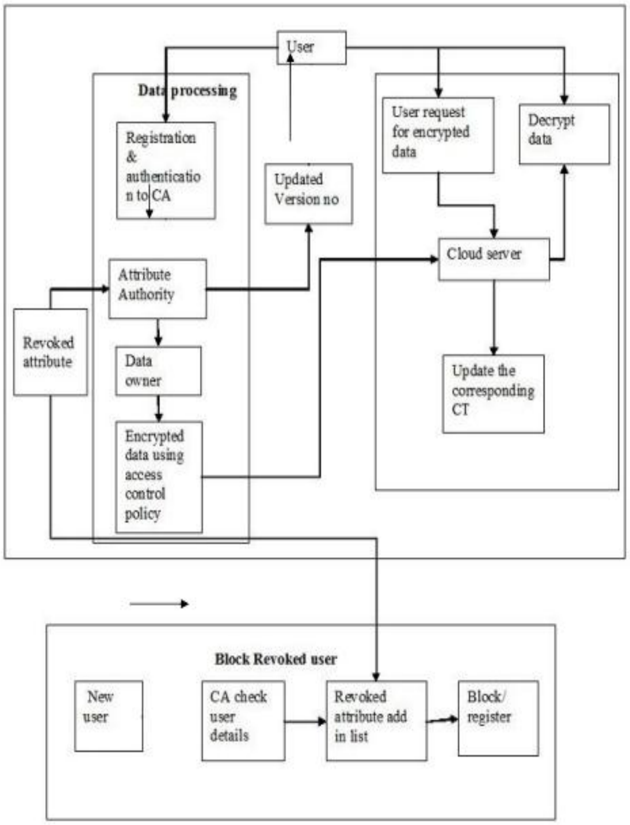

Figure.1. Architecture

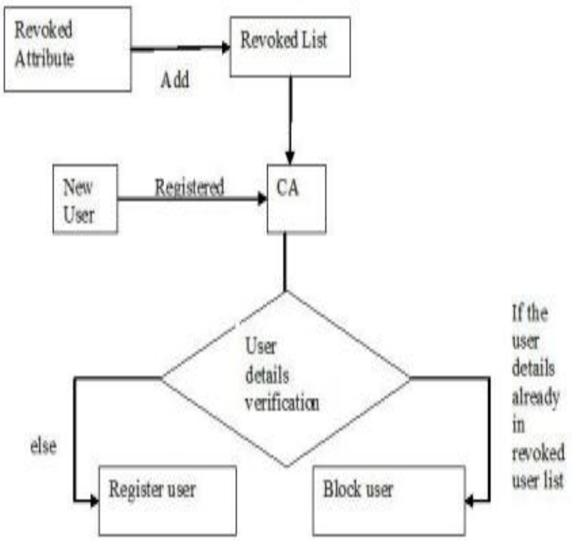

Figure.2. Block Diagram

V. CONCLUSION AND FUTURE SCOPE

A revocable multi-expert figure content approach quality based encryption (CP-ABE) plan can bolster proficient property denial. At that point, method built a powerful information get to control procedure for multi-expert distributed storage frameworks. The revocable multi-specialist figure content approach quality based encryption (CP-ABE) is a promising method, which can be enlist in any remote stockpiling frameworks and online interpersonal organizations (OSN) and so forth.

Amid the transmission of information to the cloud, there is the shot for alteration over the information by the assailant. With a specific end goal to check the trustworthiness of information, hash code is created for symmetric key while encoding the information. Produced hash is sent alongside encoded information. Cloud produces hash an incentive for the got scrambled information. Produced and got hash qualities are analyzed by the Cloud. In the event that both are same it implies that information has not been changed. In the event that the information is adjusted, Cloud reports the data to the information proprietor and asks to re-encode the information.

REFERENCES

[1]. J. Bethen court, A. Sahai, and B. Waters, “Cipher text Policy Attribute Based Encryption,” in Proc. IEEE Symp. Security and privacy (S&P07), 2007, pp. 321-334.

[2]. B. Waters, “Cipher text-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization,” in Proc. 4th Int l Conf. Practice and Theory in Public Key Cryptography (PKC 11), 2011, pp. 53-70.

[3]. V. Goyal, A. Jain,O. Pandey, and A. Sahai, ”Bounded Cipher text Policy Attribute Based Encryption,” in Proc. 35th Int l Colloquium on Automata, Languages, and Programming (ICALP08), 2008, pp. 579-591.

[4]. A.B. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters, “Fully Secure Functional Encryption: Attribute Based Encryption and (Hierarchical) Inner Product Encryption,” in Proc. Advances in Cryptology EUROCRYPT 10, 2010, pp. 62-91.

[5]. M. Chase, “Multi-Authority Attribute Based Encryption,” in Proc. 4th Theory of Cryptography Conf. Theory of Cryptography (TCC 07), 2007, pp. 515-534.

[6]. M. Chase and S.S.M. Chow, “Improving Privacy and Security in Multi-Authority Attribute-Based Encryption,” in Proc. 16th ACM Conf. Computer and Comm. Security (CCS 09), 2009,pp. 121-130.

[7]. A.B. Lewko and B. Waters, “Decentralizing Attribute-Based Encryption,” in Proc. Advances in Cryptology EUROCRYPT 11, 2011, pp. 568-588.

[8]. M. Li, S. Yu, Y. Zheng, K. Ren, andW. Lou, ”Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption,” IEEE Trans. Parallel Distributed Systems, vol. 24, no. 1, pp. 131- 143, Jan. 2013.

[9]. S. Jahid, P. Mittal, and N. Borisov, “Easier: Encryption-Based Access Control in Social Networks with Efficient Revocation,” in Proc. 6th ACM Symp. Information, Computer and Comm. Security (ASIACCS 11), 2011, pp. 411- 415.

[10].S. Ruj, A. Nayak, and I. Stojmenovic, “DACC: Distributed Access Control in Clouds,” in Proc. 10th IEEE Int?l Conf. Trust- Com, 2011, pp. 91-98.

[11].D. Boneh and M.K. Franklin, “Identity-Based Encryption from the Weil Pairing,” in Proc. 21st Ann. Int l Cryptology Conf.: Advances in Cryptology CRYPTO 01, 2001, pp. 213-229.

Author Profile

Palthya Kiran Kumar Naik, received Bachelor of Science (Bsc Electronics) degree from S K University, Anantapur in the year of 2012-2015. Pursuing Master of Computer Applications from Sri Venkateswara University, Tirupati in the year of 2016-2019. Research interest in the field of Computer Science in the area of Cloud Computing Application Security and Software Engineering.

Dr.GV Ramesh Babu,MCA,M.Tech,Ph.D and also working as an Assistant Professor in Dept. of. Computer Science, Sri Venkateswara University College of Commerce Management and Computer Science, Tirupati (AP)-India.