International Journal of Science Engineering and Advance Technology (IJSEAT)
ISSN 2321-6905 , Vol. 7, Issue 8,August -2019

The Secured Data Sharing For Multiauthority Access in Cloud Storage

R.N.D.S.S. Lakshmi[1], Prof. B.V. Ram Kumar[2]
[1]M.Tech Scholar, Department of Computer Science & Engineering,
[2]Professor, Department of Computer Science & Engineering, BVC Institute of Technology & Science, Batlapalem, Amalapuram, AP, India.
Revised manuscript received on Aug 12, 2019

Abstract—

Cloud record sharing indicates to a scope of cloud services that enables individuals to store and synchronize archives, photographs, recordings and different files in the cloud—and offer them with other individuals. These services additionally enable clients to share and synchronize data among different gadgets for a solitary proprietor. These services are open through work areas, scratch pad, advanced mobile phones and media tablets, and give a basic system to synchronizing data over numerous gadgets. In cloud computing, to shield data from spilling, clients need to scramble their data before being shared. In this paper we propose a proficient encryption plan based on layered model of the entrance structure is proposed in cloud computing, which is named document progression CP-ABE plan. FH-CP-ABE broadens normal CP-ABE with a various leveled structure of access approach, in order to accomplish basic, adaptable and fine-grained access control.

Keywords - Cloud computing, Attribute Based Encryption, Access control, data security.

I. Introduction

Cloud Computing gives such a large number of services in that the most significant service which is given by it is cloud storage service. The data proprietors can store the immense measure of data into the cloud server and the data will be available adaptably from all over the place. This property of cloud gives the advantage as well as makes real test to data access control. As the cloud server can't be completely trusted by the data proprietors.

Revised Manuscript received on August 12, 2019
*Corresponding Author
R.N.D.S.S. Lakshmi,
mail id- rndslaksmi1982@gmail.com

Henceforth to do access control one of the most acknowledged schemes is Ciphertext-Policy Attribute Based Encryption (CP-ABE) [1].

In CP-ABE plot, there is an expert [2], [3] that is in charge of attribute the executives and key dispersion. The data proprietor characterizes get to strategies and gives attributes to the clients. There exists another sort of CP-ABE conspire that is multi expert CP-ABE [4], [5] with single specialist CP-ABE plot, where attributes are kept up and overseen by various confided in experts. The specialists are in charge of giving attributes to different clients. In multi expert cloud storage frameworks client attributes can be changing every now and then. Subsequently the framework must help the attribute repudiation [6], [7]. Various experts will give various attributes to the end clients. Consequently here in multi specialist framework the data will likewise be of numerous kind however every one of the clients won't have every one of the attributes. Consequently the security issue emerges. In this paper we propose another calculation called Improved Security Data Access Control. This calculation is proposed to improve the security issue exists in the current framework. The data proprietor when stores the data into the cloud server he initially scrambles the data then it will be put away in the cloud server. The key will be produced by the specialists to various clients. What's more, it will be given to the data proprietors. So when the end client gets to any data he ought to have qualified attributes as well as give the keys to get to the data. The new calculation additionally keeps up the trustworthiness of the data put away. On the off chance that the data have adjusted by any assailant the data proprietor will come to think about it when he confirms it. What's more, when any of the clients attempts to get to the data which he can't get to then this sort of assault will likewise be told by the expert

and will be educated to the data proprietor. Our framework does not require the server to be completely trusted. What's more, regardless of whether the server is semi confided in then likewise our framework gives security.

II. Related Work

In a multi-expert cloud storage framework, attributes of user‟s can be changed progressively. A client might be join some new attributes or disavowed some present attributes. [1] In 2010, S. Yu, C. Wang, K. Ren, and W. Lou, chipped away at "Attribute Based Data Sharing with Attribute Revocation,". This paper use semi-trustable on-line intermediary servers. This server empowers the expert to renounce client attributes with insignificant exertion. This plan was extraordinarily incorporating the strategy of intermediary re-encryption with CPABE, and furthermore empowers the specialist to designate a large portion of relentless assignments to intermediary servers. The benefits of this plan is More Secure against picked figure content attacks.Provide significance to attribute repudiation which is hard for CP-ABE schemes. Disadvantage: The storage overhead could be high if proxyservers keep all the intermediary re-key. [2] In 2011, S J. Hur and D.K. Noh, chipped away at Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems. This paper proposes an entrance control system based on figure content arrangement attribute-based encryption to implement access control approaches with proficient attribute and client disavowal technique. The fine-grained access control can be accomplished by double encryption conspire. This double encryption system exploits the attribute-based encryption and specific gathering key dispersion in each attribute gathering. The upside of this plan is securelymanaging the redistributed data. This plan accomplish productive and secure in the data re-appropriating frameworks. Downside: Huge issue in Enforcement of approval strategies and the help of arrangement refreshes [3] In 2011, S. Jahid, P. Mittal, and N. Borisov, took a shot at Easier : Encryption Based Access Control in Social Networks with Efficient Revocation".The proposed Easier engineering that supports two methodologies are fine-grained access control arrangements and dynamic gathering participation. Both plan accomplished by utilizing attributebased encryption, in any case, is that it is conceivable to expel access from a client without issuing new keys to different clients or re-scrambling existing figure writings. We accomplish this by making an intermediary that takes an interest in the decoding procedure and upholds denial requirements. The upside of this plan is the Easier design and development gives execution assessment, and model use of our methodology on Face book. Downside: Does not Achieve Stronger Security Guarantees. [4], In 2013, S. Jahid, P. Mittal, and N. Borisov, took a shot at Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute Based Encryption, This model proposes the utilization of double framework encryption approach. The encryption procedures from Multi-expert ABE and KeyPolicy ABE are consolidated into a solitary module. Utilization of MA-ABE procedure demonstrates useful for key administration and adaptable access and potential security risk of conniving clients is dealt with by KPABE. The proposed structure has endeavored to accomplish data security by MA-ABE and data protection by KP-ABE conspire. The general security of the framework has been improved. Downside: Existing attribute disavowal methodsrely on a confided in server or absence of proficiency likewise theyare not reasonable for managing the attribute denial issue in data access control in multi-expert cloud storage frameworks. Each Attribute specialists (AAs) is trusted however can be debased by the foe. Every client is unscrupulous and may attempt to acquire unapproved access to data.

III. ACCESS CONTROL

Access control is commonly an approach that permits denies or limits access to frameworks. It is an instrument that is particularly significant for insurance in PC security. Old style Access control models full in to three kinds [4]:

1. Macintosh: obligatory Access control

2. DAC: Discretionary Access Control

3. RBAC: Role Based Access Control

These entrance control models known as Identity put together access control wish based with respect to the way that the server is in the confided in space, So in the cloud these methodologies are exceptionally

constrained and not pertinent, as there is a need of decentralization, adaptability and adaptability for access control information situated in the cloud. Because of this issue, different examinations demonstrate that the encryption of information is the most effective strategy for access control [4]. However the standard encryption is wasteful when specifically offering information to numerous clients. Since information should be re-scrambled utilizing each open key [4]. To defeat this new issue, about the restricted of conventional encryption, sahai and al [4], present another open key crude called ABE (Attribute Based Encryption), which has noteworthy points of interest over customary PKC (Public key Cryptography) natives. In this manner it's imagined as a significant devices for tending to the issue of secure fine-grained access control.

CHARACTERISTIC BASED ACCESS CONTROL ABAC

With the advancement of huge conveyed frameworks property based access control (ABAC) has turned out to be progressively significant. As indicated by the NIST "ABAC is An entrance control strategy where subject solicitations to perform tasks on items are allowed or denied dependent on appointed traits of the subject, relegated properties of the article, condition conditions, and a lot of arrangements that are determined regarding those qualities and conditions "[14].Attribute Based Encryption (ABE) is classification of ABAC. ABE proposed to help fine-grained access control ABE can be seen as an augmentation of Identity Based Encryption framework IBE [5]. IBE has settling the issue open key partaking in which a self-assertive string can be utilized as an open key (email, IP Address, telephone number telephone…).

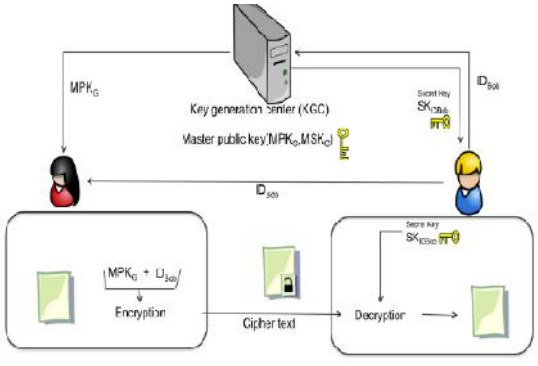

Fig.1: Identity Based Encryption system

Compared with IBE in which, encrypted data is targeted for decrypting by single known user, inABE system, the user's identity is generalized to a set of descriptive attributes instead of a single string specifying the identity of the user. Compared with the identity-based encryption, ABE has an important advantage because it makes a more flexible encryption instead of one-on-one; it is seen as a promising tool to solve the secure data-sharing problem grained and decentralized access control. ABE is used in various applications, like Electronic Health records management (HER), and PHR (Personal Health Records). In the ABE system the decryption key should bematched with the attributes of cipher text and the key will decrypt the cipher text. The private keys are constructed by the Access tree as in ABE system root node [6].

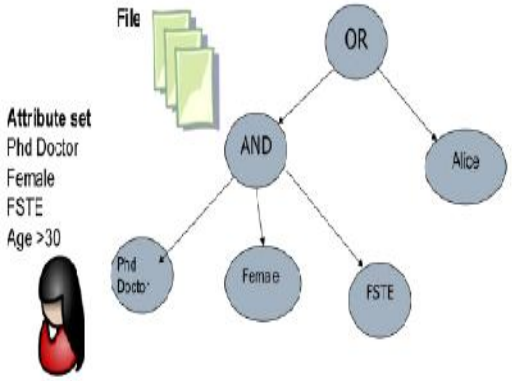

Fig.2: ABE scheme

In the cloud computing system the single authority will not able to control the multiple attributes for each user and all access rights, to address this problem for single authority ABE, the multi ABE system is introduced [9]. Due to this requirement the ABE system has been divided into two classes of multi authority ABE system: KP-ABE and CP-ABE.

IV. Security Issues Associated With the Cloud

Cloud computing is a prominent and fast growing technology has captured several professional attentions that allow many to store their data securely and the same can be accessed efficiently. Cloud service provider provides a variety of different service models such as Software-as-a Service, Platform-as-a-Service, Infrastructure-as-a-Service

and deployment models as Private, Public, Hybrid, and Community. Nowadays many professionals have started to use cloud environment as it provides the user a storage capability to store and process their data. However, the challenges like data security and access control system are the main concern of Cloud Service provider.

Security concerns associated with cloud computing environment fall into two broad categories: security issues faced by Cloud Service Providers (CSP) (organizations providing software, platform, or infrastructure-as-a-service via the cloud) and security issues encountered by their consumers (companies or organizations who host applications or store data on the cloud). However, the responsibility is shared. The Cloud Service Provider must ensure that their infrastructure is secure and that their clients' data and applications are protected with well-defined cryptographic mechanisms, while the user must acquire measures to reinforce their application and apply strong passwords and authentication course.

When an organization elects to store data or host applications on the public cloud, it loses its ability to have physical access to the servers hosting its information. As a result, potentially sensitive data is at risk from insider attacks. According to a recent Cloud Security Alliance Report, insider attacks are the sixth biggest threat to cloud computing. Therefore, Cloud Service providers must ensure that thorough background checks are conducted for employees who have physical access to the servers in the data center. Additionally, data centers must be repeatedly monitored for mistrustful movement.

In order to conserve resources, cut costs, and maintain efficiency, Cloud Service Providers may use Encryption techniques to protect data in the Cloud. The security guidance of Cloud Security Alliance (CSA) recommends data is protected at rest, in motion and in use [30]. Encrypting data avoids illegal accessing of data in Cloud, but it might entail new issues related to access control management [31]. The most three important data security features are data confidentiality, availability, and integrity which prevents data loss].

- Data Confidentiality is a property of data, usually resulting from legislative measures, which prevents it from unauthorized disclosure.
- Data integrity is the overall completeness, accuracy, and consistency of data. This can be specified by the absence of modification between two instances or between two updates of a data record, meaning data is unbroken and unaffected.
- Data availability is primarily used to create service level agreements (SLA) and similar service contracts, which define and guarantee the service provided by third-party IT service providers.

b) Reasons to Use Secure Cloud Storage and Access Control:

When it comes to storing data in the cloud, it is important to deploy cost-effective technologies and solutions that protect, preserve and manage data to ensure that it is secure, available and accessible when needed.

The cloud, of course, can be a valuable tool in helping IT achieve this objective, but it is important to understand how, where and when cloud services should be used and when they shouldn't. Cloud works best and most cost-effectively when it is part of an overall data management strategy. Because data lifecycles evolve as an organization's data mix changes, you don't want to be locked into using the cloud. Rather, you want to be able to leverage cloud services when appropriate.

Nowadays most of the organizations have started to use public clouds such as Google App Engine (GAE), Amazon Web Services (AWS), IBM Blue Cloud and Windows Azure for storing, managing, processing and accessing their valuable data. The Cloud computing environment proposes diverse services to the user; however, data access service combined with enhanced security mechanism from the cloud plays a vital role. As per the 2017 – State of Cloud Adoption and Security studies, it is observed the following important insights,

(i) In another 15 months, 80% of all IT budgets will be committed to Cloud apps and solutions.

(ii) There is a tremendous growth in Hybrid cloud adoption, increasing from 19% to 57%.

(iii) Public cloud adoption percentage has been improved.

(iv) Many organizations today completely trust public clouds to keep their data secure. Public cloud platforms started to invest more for the development and resources in security features and support. To provide better storing and accessing the data in Cloud computing requires advanced data access control techniques and security solutions.

From the survey, the access control model must provide a well strongly controlled data access facility to users and resources with enhanced security mechanism. It must also provide additional capabilities like access control manages user's files and other resources. From the point of access control, (i) cloud computing environment should provide Controlled data access to the various service of the cloud, based on the appropriate access control policies and the level of service requested (or) purchased by the user. (ii) Facilitate proper data access control policy and updated user's information. (iii) Cloud computing supports multitenant environment hence accessing data from one to another requires controlled data access policy. (iv)To ensure better and secure data access service within the cloud environment, there must be a strong relationship between trust and reputation in the data access control models. (v) Providing controlled access to both standard user files and privileged organizational functions. Major stumbling block in cloud computing data access control is a different set of users with diverse sets of enhanced security mechanisms such as storing, managing, processing and accessing of physical resources.

The issues related to data access control in Cloud computing environment can be solved with properly implemented data access control techniques with state-of the-art security solution and today's implementers can avoid such a issues made by the predecessors.

V. Proposed Methodology

In this paper, we initially propose a revocable multi-expert CP-ABE conspire, where a proficient and secure denial technique is proposed to take care of the quality renouncement issue in the framework. Our characteristic denial strategy is proficient as in it causes less correspondence cost and calculation cost, and is secure as in it can accomplish both in reverse security (The renounced client can't unscramble any new figure message that requires the disavowed credit to decode) and forward security (The recently joined client can likewise decode the recently distributed ciphertexts1, on the off chance that it has adequate properties).

Our plan does not require the server to be completely trusted, in light of the fact that the key update is implemented by each trait specialist not the server. Regardless of whether the server isn't semi confided in certain situations, our plan can at present certification the regressive security. At that point, we apply our proposed revocable multi-expert CP-ABE plot as the basic methods to build the expressive and secure information access control conspire for multi-specialist distributed storage frameworks.

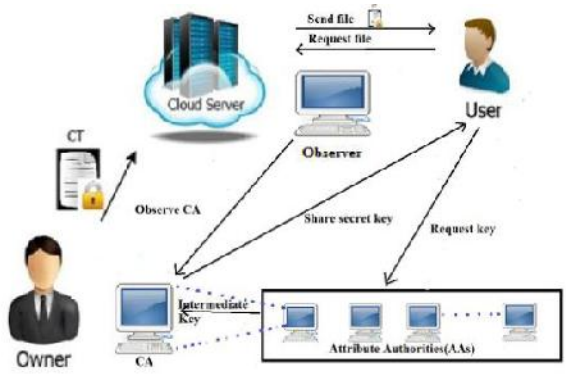

Fig 3. Proposed Architecture diagram

VI. Conclusion and Future Works

Cloud computing can be even a revolution in the computing world, by given all the types of computing resources as service (Software, platform, infrastructure), but security remains a major obstacle for the migration to the cloud computing. Migrating into the "Cloud" is not that easy but if carefully planned and deployed it will bring advantages in many areas like decreasing cost and resources. In this papers we have presented an efficient system that provide secure and fine-grained data access control in cloud Computing system based on KP-ABE and a new PRE system with CCA security, collusion resistance, and anonymity in the random oracle model . One challenge in this context is to achieve fine-grained access control, data confidentiality, data integrity, scalability and system resistant to CCAs (Chosen Cipher text Attacks), which is not provided by current work. Moreover, our proposed scheme can

enable the data owner to delegate most of computation overhead to powerful cloud servers. In future work, we would applied our proposed scheme to ensure fine-grained access control of Personal Health Records (PHR) allowing the doctors and patients to encrypt their PHRs and store them on semi-trusted cloud servers such that servers do not have access to sensitive PHR contexts.

References

[1] 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.

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

[3] S. Yu, C. Wang, K. Ren, and W. Lou, ‘‘Attribute Based Data Sharing with Attribute Revocation,’’ in Proc. 5th ACM Symp. Information, Computer and Comm. Security (ASIACCS’10), 2010, pp. 261- 270.

[4] 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.

[5] J. Hur and D.K. Noh, ‘‘Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems,’’ IEEE Trans. Parallel Distributed Systems, vol. 22, no. 7, pp. 1214-1221, July 2011.

[6] 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.

[7] S. Ruj, A. Nayak, and I. Stojmenovic, ‘‘DACC: Distributed Access Control in Clouds,’’ in Proc. 10th IEEE Int’l Conf. TrustCom, 2011, pp. 91-98.

[8] K. Yang and X. Jia, ‘‘Attribute-Based Access Control for Multi-Authority Systems in Cloud Storage,’’ in Proc. 32th IEEE Int’l Conf. Distributed Computing Systems (ICDCS’12), 2012, pp. 1-10.

[9] 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.

[10]B. Dilip Kumar Reddy, K. SaiMouni Sri, ”A Survey on Multi Authority Access Control System in Cloud Storage”, in proc. International Journal of Scientific Engineering and Technology Research, April-2017, Pages: 2635-2637

[11] Dilip Reddy. B, DrN.Kasiviswanath, DrS.ZahoorUlqHuq, “Peer to Peer Distributed Data Storage with Security in Cloud Computing”, in proc. to IJESRT International Journal of Engineering Sciences & Research Technology, vol.6 June. 2014,pp. 402-406

Authors

R.N.D.S.S. Lakshmi is pursing M.TECH (CSE) in the Department of Computer Science and Engineering from BVC Institute of Technology & Science, Batlapalem, Amalapuram, AP, India.

Prof. B.V. Ram Kumar is working as Professor and Head of the Department in Department of Computer Science & Engineering, BVC Institute of Technology & Science, Batlapalem, Amalapuram, AP, India.