International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 5, Issue 5
May 2018

Integration of Multi User Key Management with Policy Previlege using ABE in Cloud

Mr. T. Vijaykanth Reddy
B.Tech,M.E, (Ph.D)
Department of Computer Science Engineering,
St.Peter's Engineering College, Kompally,
Hyderabad, Telangana

B. Kalyani,
Student, Department of Computer Science Engineering,
St Peter's Engineering College, Kompally,
Hyderabad, Telangana

M. Nikitha,
Student, Department of Computer Science Engineering,
St Peter's Engineering College, Kompally,
Hyderabad, Telangana

M. Rukesh,
Student, Department of Computer Science Engineering,
St Peter's Engineering College, Kompally,
Hyderabad, Telangana

Abstract—Most current security solutions are based on perimeter security. However, Cloud computing breaks the organization perimeters. When data resides in the Cloud, they reside outside the organizational bounds. This leads users to a loss of control over their data and raises reasonable security concerns that slow down the adoption of Cloud computing. Is the Cloud service provider accessing the data? Is it legitimately applying the access control policy defined by the user? This paper presents data-centric access control solution with enriched role-based expressiveness in which security is focused on protecting user data regardless the Cloud service provider that holds it. Novel identity-based and proxy re-encryption techniques are used to protect the authorization model. Data is encrypted and authorization rules are cryptographically protected to preserve user data against the service provider access or misbehaviour. The authorization model provides high expressiveness with role hierarchy and resource hierarchy support. The solution takes advantage of the logic formalism provided by Semantic Web technologies, which enables advanced rule management like semantic conflict detection. A proof of concept implementation has been developed and a working prototypical deployment of the proposal has been integrated within Google services.

Keywords: Attribute based encryption, Revocation, Cloud Parameters, CP-ABE, KP-ABE, Cloud Security, Multi authority.

1.Introduction

In a parallel filing system, file information is distributed across multiple storage devices or nodes to permit synchronous access by multiple tasks of a parallel application. Some samples of superior parallel file systems that area unit in production use area unit the IBM General Parallel Filing Station(GPFS), Google Filing System(Googles), Lustre, Parallel Virtual filing system(PVFS), and panamas, Multi-user tendency can price lesser thanexpected price within the single user surroundings.Whereas coping with cloud computing, confidential information will be secured from the unauthorized access and internal threats cloud servers use sensible techniques for achieving this demand like encoding and secret writing of knowledge. The information is hold on within the encrypted format on the server & a fancy question will be discharged thereon. Cloud server can maintain the access management policies to reveal the information from the information that area unit within the encrypted format. Within the access management policies, we have a tendency to use KMA (Key Management Authority) that provides the keyset for encoding & secret writing of information. The attributes entered by the user can produce one public key that is cipher text primarily based. Thus, this method is termed as cipher text

International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 5, Issue 5
May 2018

primarily based technique. This secret is used for encoding. Whereas registering, user can select the policy and choose the attributes on the security policy is predicated. Due to this it's referred to as cipher text policy attribute primarily based encoding(CP_ABE). The most results of this project area new incontrovertibly secure attested key exchange protocols. Our protocols, more and more designed to attain every of the properties, demonstrate the trade-offs between potency and security.

2. Literature survey

A secure user-enforced data access control mechanism must be provided before cloud users have the liberty to outsourcesensitive data to the cloud. Many authors focused their attention on various attribute based encryption techniques.

2.1 Techniques

Crescenzo, Ostrovsky and Rajgopalan [2] came up with an economical and secure time-release cryptography theme employing a "time server" that inputs this time into the system. Cramer and Shoup [3] presented a new public key cryptosystem. They analysed that it is provably secure against adaptive chosen ciphertext attack.

Boneh and Franklin [4] came up with a fully functional identity-based encryption scheme. The scheme has chosen ciphertext security in the random oracle model assuming a variant of the computational Diffie-Hellman problem. Sahai and Waters [5] introduced the concept of Fuzzy Identity Based Encryption. This concept allows error-tolerance between the identity of a private key and the public key used to encrypt a cipher text.

Boneh, Creseenzo, Ostrovsky and Persiano [6] studied the problem of searching on data which is encrypted using a public key system. They proposed a mechanism called Public Key Encryption with keyword search which enables user to provide a key learning more about email. Nali, Adams, Miri [7] described a provably-secure efficient collusion-resistant threshold attribute-based encryption(thABE) scheme.

Pirretti, Traynor, McDaniel and Waters [8] presented a novel secure information management architecture and implementation. They illustrated the infrastructure through the creation and performance evaluation of distributed file system and a social network. Bethencourt, Sahai and Waters [9] came up with a system for ciphertext-Policy Attribute Based Encryption for a new type of encrypted access control where user's private keys are specified by a set of attributes and a party encrypting data can specify a policy over the attributes specifying which users are able to decrypt.

Ostrovsky, Sahai and Waters [10] presented the first Attribute Based Encryption system that supports the expression of formulas in key policies. They achieved this through a novel application of revocation methods into existing ABE schemes. Sun and Liu [11] came up with a multi group key with a management scheme that achieves hierarchical access control in secure group communication in which multiple data schemes are distributed to group members having various access privileges.

The proposed scheme has less overhead associated with key management. Cheung, Cooliy, Khazan and Newport [12] proposed a new scheme called group key management scheme which is based on ciphertext-policy attribute-based encryption. Cheung and Newport [13] presented several related CP-ABE schemes. Boldyreva, Goial and Kumar [14] proposed an identity-based encryption scheme with efficient revocation, whose complexity of key updates is significantly reduced compared to the previous solution.

3. Policy Privilege

This policy privilege that defines privileges having the varied users within the organizations. Organization area unit allowed to own specifically processed the quantity of teams users have privileges to access information within the organization. This policy defines the users agency have access to and management of sensitive or regulated information. This policy defines the access to information type users, this policy is meant to attenuate risk to structure resources and information by establishing the privileges. This classes embrace Restricted user, common user, Administrator these categories include Restricted user, Standard user, Administrator.

International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 5, Issue 5
May 2018

4.Key Management

Key management is that the management of keys in an exceedingly cryptosystem. This includes handling the generation, exchange, storage, use, and replacement of keys. It includes science protocol style, key servers, user procedures, and alternative relevant protocols. Key management issues keys at the user level, either between users or systems.

4.1.1Key-policy attribute based encryption (KP-ABE)

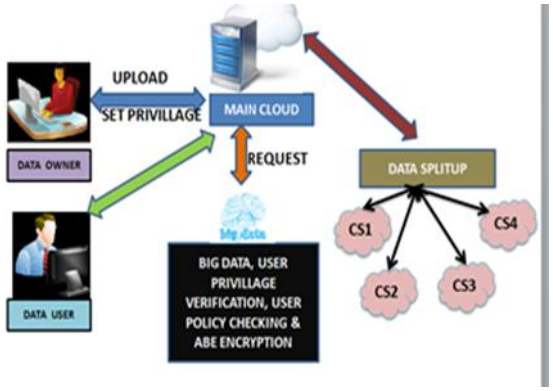

Fig .1 Architecture of Proposed system

In KP-APE, the owner of the informationcreates a master. Mistreatment the master, the owner encrypts the information such a cipher text is labelled with a group of attributes. The tree-based access structure contains leaves that area unit related to attributes. A user is in a position to decode a cipher text if the attributes related to the cipher text satisfies the user's key access structure.

4.1.2 Cipher text-policy attribute based encryption (CP-ABE)

In CP-ABE system, a user's personal key's related to a collection of attributes. Once a celebration encrypts a message during this system, they specify associate associated access structure.

5. Proposed Approach

This section describes architecture, functional diagram and algorithm used to implement the proposed system.

5.1. Proposed System

In the Proposed System, every user has to feed User Name, Password for Data access. Server generates the set of Keys to the Users for Data Access. Data owner uploads their data with index in server. Server split and stores the owner data in different sub servers. ABE access policies are expressed based on the attributes of users or data. We adopt attribute-based encryption (ABE) as the main encryption primitive. However, to integrate ABE into a large-scale data system, important issues such as key management scalability, dynamic policy updates, and efficient on-demand revocation are non-trivial to solve.

5.2. Modification Process

In the Modification Integration of cloud is achieved. Main cloud chunks the User data and stores in different sub Cloud servers. Admin generates Policy Key (View / Modify) based on the User's Profile. If any user tries to misbehave an immediate Alert is communicated to the Data Owner. Data Owner can change the Policy Key and Access Policy in runtime. Our System should able to update its policy automatically. We are implementing ABE Algorithm for Profile based Data Access.

Advantages:-Avoid Congestion, High security, Data sharing can be achieved for three type of user according to their privileges. Group Key generation is achieved if any user logout from the group then the group key is changed and it intimated to other user through the e-mail. Data integrity is maintained by using the token key to view the file context.

5.3. Proposed scheme

A. System Model

The system model consists of 3 completely different entities: the cloud, a bunch manager (i.e., the corporate manager), and an organised range of cluster members(i.e., the staffs) as Illustrated in Fig. cloud provides high priced storage services.

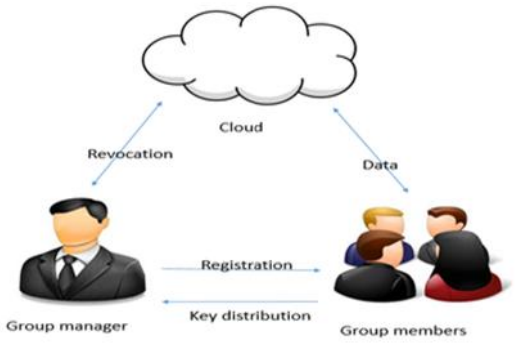

Fig.2.Process Flow

International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 5, Issue 5
May 2018

However, the cloud isn't totally sure by users since the CSPs area unit terribly possible to be outside of the cloud user's sure domain. Like we have a tendency to assume that the cloud server is honest however curious. That is, the cloud server won't mechanically delete or modify user knowledge attributable to the protection of information auditing schemes, however can try and learn the content of the hold on knowledge and therefore identities of the cloud users.

B. Design goals

In this section, we have a tendency to describe the most style goals of the planned theme together with access management, knowledge confidentiality, similarity and traceability, and potency as follows:

Access control:-The need of access management in cluster control, First, cluster member's area unit use cloud resource for knowledge operations. Second, while not authorization users cannot access cloud resource at any time an revoked users won't capable of victimization the cloud once more once they're revoked.

Data Confidentiality:-Confidentiality and data integrity and handiness moreover – area unit protections against malicious software package (malware) spyware, span and phishing attacks. A crucial and difficult issue for knowledge confidentiality is to take care of its handiness for dynamic teams. New users ought to rewrite info hold on within the cloud before their participation, and revoked, users is unable to rewrite the info touched into the cloud once the revocation.

Anonymity and Traceability:-Anonymity guarantees that cluster member will success the cloud while not revealing the important identity it permits effective protection for user identity, it poses a possible within attack risk to the system. To tackle the within attack, the cluster management ought to have the power to reveal the important identities of information.

Efficiency:-The potency is outlined as follows. Any cluster member will store, modify and share knowledge files with others within the cluster by the cloud. User revocation may be achieved while not busy bodies the remaining users and signed receipts are collected once secure content sharing the remaining users don't have to be compelled.

Datasharing:-To attain privacy preserved knowledge sharing for dynamic themes within the cloud, the theme combines the cluster signature, signed receipt and dynamic broadcast cryptography techniques. Specially, the cluster signature and signed receipt theme permits users to anonymously use the cloud.

C. System Architecture

Cloud CSPs (Cloud service providers) and provides volume in a storage services. However, the cloud isn't absolutely sure by users since the CSPs area unit terribly possible to be outside of the cloud users' sure domain. Similar to, we have a tendency to assume that the cloud server is honest however curious. That is, the cloud server won't maliciously delete or modify user knowledge attributable to the protection of information auditing schemes, however can try and learn the content of the hold on knowledge and therefore the identities of cloud users.

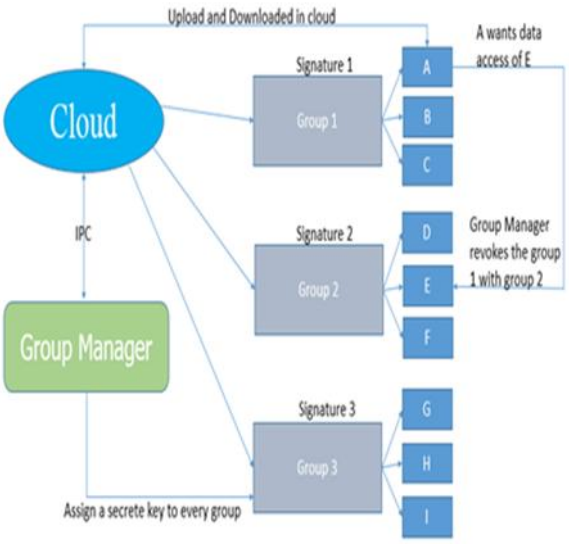

Fig 3. System Architecture

Cluster manager takes charge of system parameters generation, user registration, user revocation, and

revealing the important identity of a dispute knowledge owner. Within the given example, the cluster manager is acted by the administrator of the corporate. Therefore, we have a example, the cluster manager is acted by the administrator of the corporate. Therefore, we have a tendency to assume that the cluster manager is absolutely sure by the opposite parties. Group members area unit cluster a collection of registered that may store their personal knowledge into the cloud server and share them with others within the group. In our example, the staffs play the role cluster members. Note that, the cluster membership is dynamically modified, owing to the workers resignation and a new worker participation within the company.

6. Implementation

The basic operations performed by cloud admin making login for brand new users, activate group login, deactivate space group login. Company admin have authority to register branch of company, register designations offered specially branch, register worker for that branch. Each worker has their own document list and received document list. Staff will set attributes for his or her documents on the premise of designation, designationwise expertise, and branch in order that solely staff satisfying those attributes will access that document. Staff will get their received documents by specifying their secret key. Whenever any worker logged in they will transfer the document on server by specifying attributes for it. Then document is encrypted by generating the key. Whereas downloading the document staff satisfying attributes do authentication of coding keys and might decipher the document.

7.Conclusion and future scope

7.1 Conclusion

We have enforced a secure knowledge sharing model exploitation attribute based mostly secret writing technique that overcomes a number of the problems studied in existing literature. It provides user revocation mechanism in order that file owner will revoke permission of file form different users. It additionally removes key written agreement drawback. It provides secured knowledge sharing with Associate in permission attribute based mostly secret writing. Associate in permission enforced model is for sharing of files in group only.

7.2 Future scope

In future implemented model are often deployed on cloud and might be utilised by numerous companies. For implementation purpose we have a tendency to area unit thought of the kind of file as document, computer file which might be enhanced to sound file, video file, image file etc. Also secret attributes are often magnified so as to produce high security to the model on cloud.

REFERENCES

[1] Junbeom Hur, “Improving Security and Efficiency in Attribute-Based Data Sharing”, IEEE Transactions on Knowledgeand Data Engineering, vol. 25, no. 10, 2013.

[2] G. Di Crescenzo, R. Ostrovsky, and S. Rajagopalan, “Conditional Oblivious Transfer and Timed-Release Encryption”,in Advances in Cryptology- Eurocrypt '99, Lecture Notes in Computer Science, Vol. 1592, pp. 74, 1999.

[3] R. Cramer and V. Shoup, “A practical public key cryptosystem provably secure against adaptive chosen ciphertextattack”, in Advances in Cryptology - Crypto, Lecture Notes in Computer Science, Vol. 1462, Springer-Verlag, pp. 13,1998.

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

[5] Sahai and B. Waters, “Fuzzy Identity-Based Encryption”, Proc. Int’l Conf. Theory and Applications of CryptographicTechniques - Eurocrypt ’05, pp. 457-473, 2005.

[6] D. Boneh, G.D. Crescenzo, R. Ostrovsky, and G. Persiano, “Public-Key Encryption with Keyword Search”, inAdvances in Cryptology - Eurocrypt, Springer, volume 3027 of LNCS, pages 506, 2004.

[7] D. Nali, C. Adams, and A. Miri, “Using threshold attribute-based encryption for practical biometric-based accesscontrol”, pp.173-182, November 2005.

[8] M. Pirretti, P. Traynor, P. McDaniel, and B. Waters, “Secure Attribute-Based Systems”, Proc. ACM Conf. Computerand Comm. Security, 2006.

[9] J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-Policy Attribute-Based Encryption”, Proc. IEEE Symp. Securityand Privacy, pp. 321-334, 2007.

[10] R. Ostrovsky, A. Sahai, and B. Waters, “Attribute-Based Encryption with Non-Monotonic Access Structures”, Proc.ACM Conf. Computer and Comm. Security, pp. 195-203, 2007.

[11] Y. Sun and K. Liu, "Scalable hierarchical access control in secure group communications", In Proc. of the IEEEInfocom, Hong Kong, China, March 2004.
[12] L. Cheung, J. Cooley, R. Khazan, and C. Newport, "Collusion-resistant group key management using attribute-basedencryption", Cryptology ePrint Archive Report 2007/161, 2007.
[13] L. Cheung and C. Newport, "Provably Secure Ciphertext Policy ABE", Proc. ACM Conf. Computer and Comm.Security, pp. 456-465, 2007.
[14] A. Boldyreva, V. Goyal, and V. Kumar, "Identity-Based Encryption with Efficient Revocation", Proc. ACM Conf.Computer and Comm. Security, pp. 417-426, 2010.