International Journal of Application or Innovation in Engineering & Management (IJAIEM)
Web Site: www.ijaiem.org Email: editor@ijaiem.org
Volume 4, Issue 12, December 2015 **ISSN 2319 - 4847**

Privacy and Secure Revocable Data Access Control in Multi-Authority Cloud Storage

Rashmi Jadhav[1], Prof. Deepti Varshney[2]

[1] SRCOE Pune Dept. of Computer Engineering Savitribai Phule Pune University

[2] SRCOE Pune Dept. of Computer Engineering Savitribai Phule Pune University

ABSTRACT

Cloud users uses "Cloud storage" service to host their data in the cloud. Access control service provided by cloud is used for giving protection against unauthorized access to data.Ciphertext-Policy Attribute-Based Encryption (CP-ABE) is mostly considered for data access control in cloud storage. The existing CP-ABE is difficult to apply in multi-authority cloud storage due to the attribute revocation problem. The proposed revocable multi-authority CP-ABE scheme provides solution to the attribute revocation problem. The proposed scheme updates the components of the revoked attribute only and generates latest secret keys for the revoked attribute and forwards it to the non revoked users who have the attributes as revoked attributes. The Backward security and Forward security is maintained. If the revoked user enters into the system again by doing the registration process means, the particular user is identified via the identity card detail in the revocation list and they are not allow in the system, so that these users are stopped at the registration phase itself.

Keywords: Multi Authority, Cloud Storage, Cloud, Privacy, Security, Encryption

1. INTRODUCTION

Distributed processing, parallel processing and grid computing together emerged as cloud computing. Cloud computing is a model for enabling ubiquitous, suitable, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. In the cloud computing user data is not stored locally but is stored in the data center of internet. The cloud computing uses technology visualization for all provided services. It is used for generalization of the computing resources. The varies companies which provide cloud computing service are responsible for managing could and maintain the operation of these data centers. The users can access the stored data at any time by using Application Programming Interface (API) provided by cloud providers through any terminal equipment connected to the internet. Not only storage services provided but also hardware and software services are available to the general public and business markets.

1.1 MULTIAUTHORITY STORAGE

In Multi-Authority storage systems, there will be many authorities[5].Users may store attributes issued by multiple jurisdictions and data owners may also share the data using access policy defined over attributes from different authorities. Users attributes are changed dynamically in multi-authority cloud storage systems. A user can permit some new attributes or revoked some current assign attributes.

2. LITERATURE REVIEW

Cloud Computing servers provides promising platform for storage of data. Sharing of personal medical records is an become apparent patient centric model of health information exchange, which is often outsourced to store at third party, such as cloud providers Attribute based encryption (ABE) techniques to encrypt each patient's medical record file. The technique describes a new mechanism which enables secure storage and controlled sharing of patient's health data. Technique explore Key Policy Attribute Based Encryption (KPABE) and Multi Authority Attribute Based Encryption to enforce patient access control policy such that all the users of system can download the data ,but only authorize user can view the medical records. framework of secure sharing of individual medical records in cloud computing, utilize various forms of ABE to encrypt the medical record files, so that patients can allow access not only by individual users, but also various users from public domains with different professional roles, qualifications and affiliations[8].Advantages of technique are:1.Multiple security domains.2.Reduce the key management complexity for owners and users.3.A high degree of patient privacy is guaranteed by exploiting multi-authority ABE framework. Limitations of technique are: 1.The framework addresses the unique challenges brought by multiple owners and users.2. Storing personal medical records on the cloud server leads to need of Encryption Mechanism.

The new methodology for realizing Cipher text-Policy Attribute Encryption (CP-ABE)[3] under concrete and non interactive cryptographic assumptions in the standard model. Solutions allow any encrypt to specify access control in terms of any access procedure for the attributes present in the system. In most client system, cipher Text size, encryption, and decryption time scales linearly with the complexity of the access procedure. The only previous work to achieve these parameters was limited to a proof in the generic group model. Three constructions within our framework [7]. First system is proven selectively secure under a supposition that we call the decisional Parallel Bilinear Die-Hellman Exponent (PBDHE) supposition which can be viewed as a generalization of the BDHE assumption. Next two constructions provide performance trade off to achieve provable security respectively under the (weaker) decisional Bilinear-Diffe-Hellman Exponent and decisional Bilinear Die-Hellman assumptions. Technique presented the cipher text-policy attribute-based encryption systems that are e client, expressive, and provably secure under concrete assumptions. All of constructions fall under a common technique of embedding an LSSS challenge matrix directly into the public parameters. Constructions provide a trade in terms of the complexity of assumptions [2]. Advantages of this methodology are 1.Provide a trade off in terms of efficiency and the complication of assumptions.2.It achieved corresponding expressiveness and efficiency to the Goyal construction, but in the Cipher text Policy Attribute Based Encryption setting. Limitations are 1.Framework was limited to a proof in the generic group model. 2. Problem of finding an expressive CP-ABE system under a more solid model.

Attribute-based encryption (ABE) is an effective cryptographic primitive for achieving fine-grained access control of cipher texts. A well-known concern in the multi-authority ABE[6] setting is that malicious users leak their private keys to construct private decryption devices and distribute them to illegal users. To deal with this key abuse problem, technique introduces the concept of multi-authority attribute-based traitor tracing (MABTT), and proposes a concrete MABTT scheme. Based on the subgroup conclusion problem for three primes, the MABTT scheme is proved to be fully secure by using dual system encryption technique. The MABTT system sanction adaptive pirates to be trace [4].Advantages of this methodology are 1.Permits adaptive pirates to be traced 2.To construct a scheme which allows a greater number of key extraction queries by the pirate than ours allows. Disadvantages are 1.Alleviate the key leakage problem in the settings of multi-authority ABE.

In several distributed systems a user should only to access data if a user posses a certain set of credentials or attributes. Currently, the only method forcing such policies is to employ a trusted server to store the data and mediate access control. However, server storing the data is compromised, then the confidentiality of the data will be compromised. Technique presents a system for realizing complex access control on encrypted data that we call Cipher text-Policy Attribute-Based Encryption. By using technique encrypted data can be kept confidential even if the storage server is untrusted moreover, technique are secure against collusion attacks. Previous Attribute-Based Encryption systems used attributes to report the encrypted data and built policies into user's keys while in our system attributes are used to report a user's credentials, and a party encrypting data determines a policy for who can decrypt. Thus, methods are conceptually closer to long-established access control methods such as Role-Based Access Control (RBAC).In addition[1], Methods provide an implementation of system and give performance measurements .Advantages of this technique are 1.System allows plans to be expressed as any monotonic tree access structure 2.Resistant to collusion attacks in which an attacker might obtain multiple secret keys.3.It included several optimization techniques. Disadvantages are 1.It is increasingly difficult to guarantee the security of data using long-established methods. 2.Sensitive data is stored in an encrypted form. 3.Unable to efficiently handle more expressive types of encrypted access control.[10] The relationship between users and resources is dynamic in the cloud, and service providers and users are typically not in the same security domain. Identity-based security cannot be used in an open cloud computing environment, where each resource node may not be familiar, or even do not know each other. Technique will focus on the following three broad categories of access control models for cloud computing: (1) Role-based models; (2) Attribute-based encryption models and (3) Multitenancy models. Cloud scale to tens of thousands of physical machines, with a lot more virtual machines added and removed, enterprise level access control mechanisms will not be scalable enough to handle attacks. Advantages of this technique are 1.A tenant in turn manages the access control list of the objects owned by them and the capability list of the subjects belonging to them.2.Cloud access control is more scalable and robust than the typical network-based techniques. Disadvantages are 1.Due to the multi-tenancy model of cloud computing, users (tenants) of a cloud computing environment prefer their traffic to be isolated from all other tenants.2.To employ a centralized repository for policies and group members.

In an identity based encryption scheme, each user is identified by a unique identity string. An attribute based encryption scheme (ABE), in contrast, is a method in which each user is identified by a set of attributes, and some function of those attributes is used to regulate decryption ability for each cipher text. This scheme allows any polynomial number of independent authorities to observe attributes and distribute secret keys. An encrypt can choose, for each authority, a number dk and a group of attributes; he can then encrypt a message such that a user can only decrypt if he has at least dk of the stated attributes from each authority k. This scheme can tolerate an arbitrary number of corrupt the authorities [11]. Advantages are 1.Allows any polynomial number of independent authorities to monitor attributes and distribute secret keys. 2. The set of attributes allowed in each clause must be disjoint . Disadvantages are 1.In the multi authority

scheme as stated; each user must go to every authority before he can decrypt any message. 2. Multi Authority Scheme for Large Universe and Complex Access Structures.

A promising approach to mitigate the privacy risks in Online Social Networks (OSNs) is to shift access control implementation from the OSN provider to the user by means of encryption. EASIER, an architecture that supports fine-grained access control strategy and dynamic group membership by using attribute-based encryption. A key and novel feature of architecture, however, is that it is possible to remove access from a user without issuing new keys to other users or re-encrypting existing cipher texts. Technique achieves this by creating a proxy that participates in the decryption process and enforces revocation limitations. The proxy is minimally trusted and cannot decrypt cipher texts or provide access to previously revoke dusters. Technique describes EASIER architecture and construction provides performance evaluation, and prototype application. Although technique showed our approach in an OSN setting, it can be applied to any context where ABE is implemented. Technique implemented the scheme and compared it with Bethen court CPABE. Results show that EASIER is scalable in terms of estimation and communication for OSN's [9]. Advantages are 1. Attribute based encryption systems with different types of express. 2. Key-Policy ABE and Cipher text-Policy ABE capture two interesting and complimentary. 3. The primary challenge in this line of work is to find a new system with elegant forms of expression that produce more than an arbitrary combination of techniques. Disadvantages are 1.Attribute Based Encryption systems used attributes to describe the encrypted data and built policies into user's keys. 2. While in system attributes are used to describe a user's credentials, and a party encrypting data determines a policy for who can decrypt.

3. EXISTING SYSTEM

Multi-authority Cipertext Policy Attribute Base Encryption (CPABE) is mostly considered technology for data access control in cloud storage systems. Users may hold various attributes issued by multiple authorities. The data access policy over the attribute is defined by the authorities and not by the data owners. The existing system is not applicable for multi-authority cloud storage due to its attribute revocation problem. If any attribute is revoked means all the Cipher text associated with the authority whose attribute is revoked should be replaced or updated. The existing system relies on a trusted server.

DRAWBACKS

(1) Multi-authority CP-ABE allows the central authority to decrypt all the Cipher texts.
(2) It does not support attribute revocation.
(3) All the Cipher texts associated with the authority whose attribute is revoked should be replaced or updated.

4. PROPOSED SYSTEM

It is based on the single-authority CP-ABE and it is extended to multi-authority. This technique is applied in multi-authority CPABE protocol to combine the secret keys generated by different authorities for a user and prevents the collusion. The global authority is separated into Certificate Authority (CA) and Attribute Authorities (AA). The CA sets up the system and registration of each user and AA is done by CA. The CA provides unique identity to each user and unique identity to each AA.Attribute Authority only generates the secret keys for the attribute and forwards it to the user. Each AA generates global public key. It combines the global public key and public key generated by CA for generating the secret key. The data owners first split the data into multiple components according to logical granularities and design an access policy for each attributes. The data owner encrypts the data with content keys using symmetric encryption algorithm. Then the content keys are encrypted based on access policies of each attribute and send the encrypted data together with Cipher texts to the cloud. When an attribute of the user is revoked, only those components associated with the revoked attribute in secret keys and Cipher texts need to be updated. The AA generates a new version number for the revoked attribute and generates an update key. By using the update key, the components associated with the revoked attribute in the Cipher text can also be updated to the current version.

The corresponding updated Cipher texts in cloud also updated. In addition to this the revoked user can access the system after doing the registration process again and get the access according to access control policy. After registration the revoked user may try to access the system using his/her old authentication details. Therefore the authentication details of each and every user involved in the system are stored separately. The unique identity of the user such as Social Security Number (SSN) General Identity card number is added in the revocation list. If the revoked user enters into the system again by doing the registration process means, the particular user is identified via the identity card detail in the revocation list and will not be added to the system, so that they are stopped at the registration phase itself. There is the possibility for the revoked user or external attacker to hack the token of the existing user from the database of the cloud and access the stored data using the hacked token. To prevent from such vulnerability, hash value of the token corresponding to each user is stored in the database instead of direct token itself. Whenever user enters into the system with token, authentication is done as follows: Hash value of the token is calculated and it is matched with the stored hash value in the database. If it is matched, they are authenticated user else their access is denied.

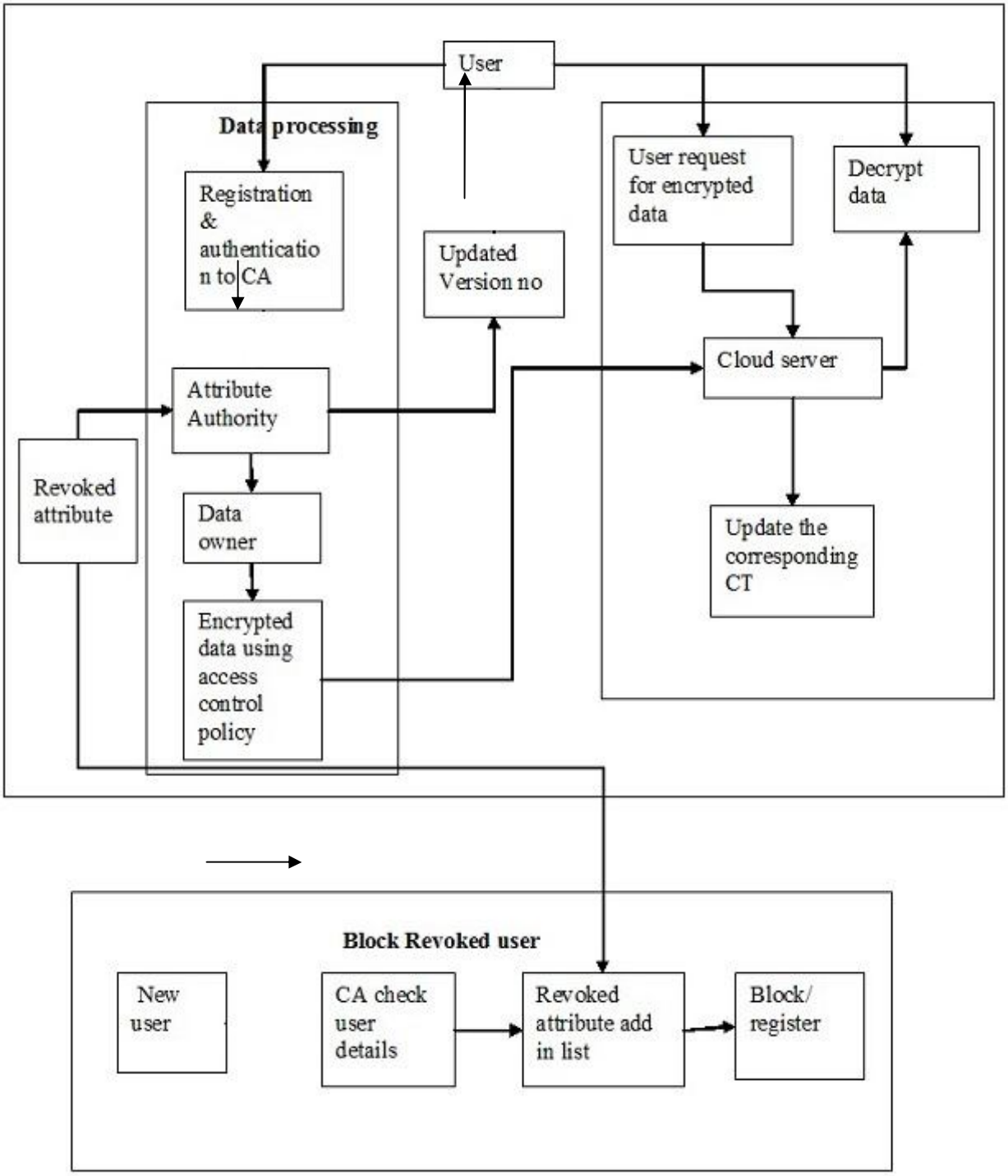

Fig.1 Architecture

ADVANTAGES

(1) The global authority is separated into Certificate Authority (CA) and Attribute Authorities (AA).
(2) AA combines the global public key and public key generated by CA for generating the secret key. So that the central authority was not able to decrypt the Cipher texts.
(3) Only the components associated with the revoked attribute is updated and no need to update all the attribute components generated by the authority which generated the revoked attribute.
(4) The Cipher text updating in cloud enables the Forward Security.
(5) All the users are need to hold only the latest secret key, no need to keep records on the previous secret keys.

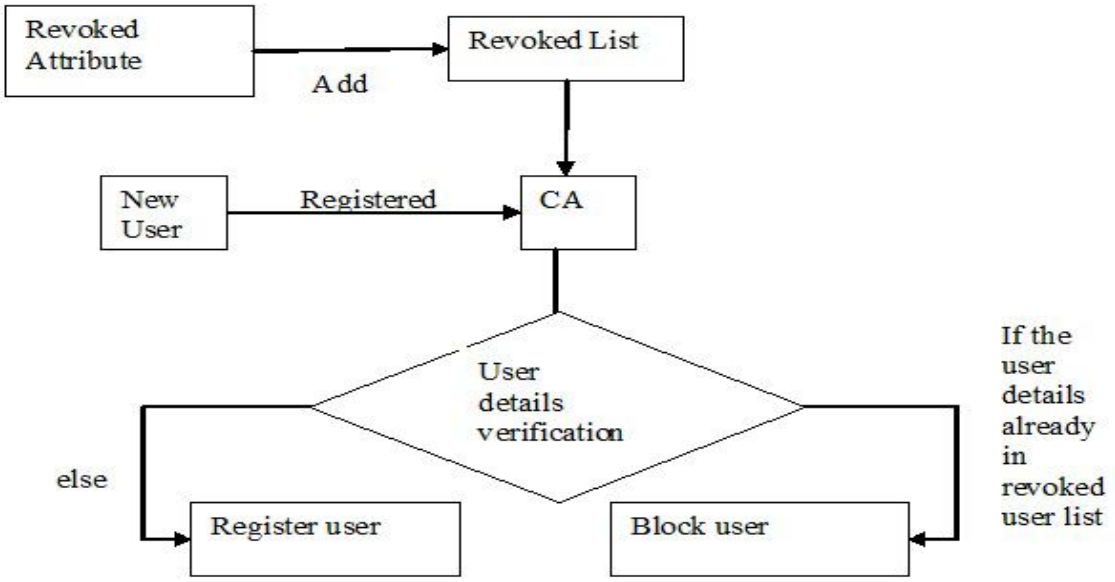

Fig.2 Block Diagram

5. CONCLUSION

A revocable multi-authority cipher text policy attribute based encryption (CP-ABE) scheme can support efficient attribute revocation. Then, technique constructed an effective data access control strategy for multi-authority cloud storage systems. The revocable multi-authority cipher text policy attribute based encryption (CP-ABE) is a promising technique, which can be register in any remote storage systems and online social networks (OSN) etc.

6. FUTURE WORK

During the transmission of data to the cloud, there is the chance for modification over the data by the attacker. In order to check the integrity of data, hash code is generated for symmetric key while encrypting the data. Generated hash is sent along with encrypted data. Cloud generates hash value for the received encrypted data. Generated and received hash values are compared by the Cloud. If both are same it means that data has not been modified. If the data is modified, Cloud reports the information to the data owner and asks to re-encrypt the data.

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.