Survey on Various Data Access Control Schemes in Cloud Computing

G.Muthulakshmi[1], S.Saranya Devi[2], A.Nandhini[3], N.Subasri[4]
Dept of CSE
ANNA UNIVERSITY REGIONAL CAMPUS COIMBATORE

Abstract- *Data storing and sharing becomes an exceptionally attractive service supplied by cloud computing platforms because of its convenience and economy. Data owner to stores and outsources their data in the cloud, which provides the data access to the user. However, there are many issues such as verifying the access authorization of a user and securely updating a cipher text in the cloud. A proper access control is the fundamental security requirement in any cloud environment, to avoid illegal access to the cloud systems. In this work gives an overview of different data access control schemes like Access control list, Role based access control, Attribute based access control, etc., that are used in the cloud, are discussed.*

Keywords- Cloud computing, cloud security, access control in cloud, data privacy.

I. INTRODUCTION

Now a days as an emerging and efficient computing model, cloud computing has attracted well-known attention and support

In many fields. Although cloud computing paradigm brings many benefits, there are unavoidable security problems. One of the important problems is how to ensure the security of user data. Security problems, such as data security and privacy protection is a major concern. In cloud computing users store their data files in cloud servers. Thus, it is crucial to prevent unauthorized access to these resources and realize secure resource sharing. Cloud computing environment, cloud service providers may be attacked by malicious attackers. These attacks may leak the private information about users for commercial interests as the data owners commonly store decrypted data in cloud servers. How to realize access control to the encrypted data and ensure the confidentiality of data files of users in an untrusted environment are the real world problems that must be solved in cloud computing, The ways to realize scalable, flexible and fine grained access control is strongly desired in the service oriented cloud computing model. Attribute-based encryption (ABE) supports the fine-grained sharing of encrypted data. In some common designs, attributes are managed by an attribute authority that is supposed to be fully trustworthy. Most of the traditional access control models are not suitable for cloud environments. They lack flexibility in managing the attributes and also have scalability issues. Conventional methods fail to support the dynamic and sophisticated nature of cloud environment, handling with large number of users in the cloud [1].

II. ACCESS CONTROL IN CLOUD

A set of rules and procedures that would help and enable user authorization to various data access is defined as access control [2].

The fundamental goal of any access control system is restricting a user to exactly what he should be able to do and protect information from unauthorized access. Thus, each access control system has its own attributes, procedures and actions, which derive from either a policy or a set of policies.

- Mandatory access control model
- Discretionary access control model
- Role based access control model
- Attribute based access control model
- Risk based access control model

In the MAC model, the administrator assigns different security levels to the subject and object. These security labels help to protect the flow of information from the higher security level to the lowest [3].

In Discretionary Access Control (DAS) model, the owner of the objects determine the permission rights on the objects or data that needs to be accessed based on the membership in a particular group or users identities. When compared to MAC model, the DAC model cannot be used in areas which need a higher level of security. The commercial operating systems like UNIX and Windows based platforms make use of DAC model, as this model is very flexible and simple to use [4]

The role based model is a normal way to control access as this model works on the basis such that the

responsibility of the subject is more vital that what the subject is [1]. Role Based Access Control (RBAC) model provides the flexibility to a subject that it can have multiple roles or membership in multiple groups. In this model the roles are predetermined to the task which is based on the access permissions.

The Attribute Based Access Control (ABAC) model mainly depends on group of attributes that are needed to make any access decisions [6]. In ABAC model the attributes can be characterized or used in multiple ways, such as role, location or start date of any project for any use which may or may not be connected to each other. This model evolved to cater to different rules, services and policies that tie up any giant organizations [9]. The Risk Based Access Control (RBAC) model works on various levels of risk in accordance with the prevailing situations. The various access decisions are taken on the basis of operational need principle [5].

III. RELATED WORK

A role based access control system called RBTBAC (Role Based Time Bound Access Control) model was proposed for electronic health record datasets [8]. Every user has some role, which could be that of a doctor, patient or nurse. Depending on the private details of the user, every role has some authority. This model was constructed using a hierarchical approach. Also, a time parameter was combined with the access control policies for every user. It specifies the time limit for accessing the records from the cloud for a user with valid role, along with selective privileges. The user can access the records within this authorized time interval. The advantages of this model are secrecy of user data was preserved, prohibition of unauthorized attacks by digital signature usage. It also maintains a cancellation list for credential by which it prevents the usage of expired identification . The main difficulty of this system is with key handling as it involves key distribution for different classes which make this model inefficient.

A flexible access control algorithm for cloud environment was recommended by Wang [1], which work on circumstantial data like security and time. This proposal was based on the role based access control model by linking the trust relationship with the customers. The trust management system reviews and modifies the trust levels after each activity. This system functions on the appropriation that each cloud holds a global certificate Authority Authorization Centre (AAC) which is in charge of access control. Although linking the access control with the calculated trust level, along with the user's behavior modification is an acceptable approach, yet this proposed system can cause certain threats such as trespassing, unaware of the techniques of granting access and the type of mechanism, probability of single point attack on AAC and the vagueness of the use of the RBAC model for granting access to users.

Recently, Liu and Xiong [12] suggested a shared authority based authentication protocol called SAPA, which is a privacy protecting access policy for the cloud. To ensure that the cloud user accesses only own data, attribute based approach is adopted and to provide data sharing among different users, a proxy re-encryption scheme is applied. This model guides various security and privacy considerations such as authentication, data anonymity, user privacy, and forward security, etc. by nameless access request matching mechanism which provides the shared right to use authority. This is only a theoretical ideal for the authentication and authorization, but not tested in the real cloud environment.

Xian et al. [11] proposed a privacy preserving access policy for cloud data with proper security. This model uses the Cipher-text Policy Attribute-Based Encryption (CP-ABE) combined with Identity-Based Encryption (IBE) scheme.

Here, each data file is described by a set of meaningful attributes and it defines a public-private key pair for each of these attributes. The user's secret key is computed as a combination public key and the attribute's secret key and thus each attribute presents a different key to each user. Decryption of a ciphertext is available only if the user has the matched attributes to satisfy the cipher text so that the privacy is ensured. This pattern is not implemented in the real cloud environment and the computational complexity is high for the encryption as well as decryption. Also for user revocation, the ciphertext needs to be re-encrypted and the user must be online to do so and this is a major obstacle to adopting this model.

Hierarchical Attribute-Based Encryption (HABE) was introduced by Wan, Liu and Deng [9] for fine-grained access control in cloud storage. It combines the Hierarchical Identity-Based Encryption (HIBE) [10] and CP-ABE algorithms. This model delegates the computation to the CSP and ensures fine grained access control. It adopts disjunctive normal form policy and the same domain master controls all attributes in one cooperative clause. So along with specific policies, the same attribute may be administrated by multiple domain masters. This makes it difficult to implement practically.

Moreover, this method doesn't support compound attributes efficiently. Attributes poses a major role in ABE and encryption of data is done under a set of attributes describing

the intended receivers. The secret key of these users is also associated with the attributes set for encryption. Attribute-based encryption schemes allow users to decrypt cipher-text as long as it has the attributes satisfying a threshold policy. Subsequent researches on ABE can roughly be classified based on the access policy, as the Key-Policy ABE (KP-ABE) and Ciphertext-Policy ABE (CP-ABE).

In KP-ABE[15], the ciphertext is associated with a set of attributes and the secret key is associated with the gain access to the tree. The encrypting party has no control over who has access to the data and can only define the set of descriptive attributes necessary to decrypt the ciphertext. There is a entrusted authority that generates the secret key, contributed the user submits the appropriate values for the attributes that constitute the accessibility tree. In CP-ABE, the ciphertext is associated with the accesstree.

TABLE I COMPARISON TABLE FOR DIFFERENT ACCESS CONTROL SCHEME

S.NO	PROBLEM STATEMENT	ACCESS CONTROL SCHEME	ADVANTAGES	DISADVANTAGES
1	protection of identity infomation, transaction histories and sensitive data[1]	Role based access control	A global certificate Authority Authorization Centre (AAC) to enhance the trust of access control for each user.	System can cause certain threats, probability of single point attack on AAC.
2	consistency of access authorization with the activated role of user[8]	Role based time bound access control model	User privacy preserved, prevention of unauthorized attacks by digital signature usage.	Key handling is difficult.
3	Protection of the Personal Information Identity (PII) against unauthorized disclosures. [13].	Privacy aware access control model	Flexible access control policy types, scalable as encryption and access control policy part are reliable and easy	Policies defined by the entities is not hidden even though data is hidden
4	To achieve data security and understand the data access policy in cloud storage services [11].	CP-ABE integrated with Identity Based Encryption (IBE) scheme	Robust data sharing security, succeeds in preserving the privacy of cloud users, efficient and dynamic user revocation	Computation complexity is high for the encryption and decryption.
5	Achieve Privacy-preserving access authority sharing. To guarantee data confidentiality And data integrity. [12]	SAPA – attribute based combined with proxy re-encryption scheme	Fine grained access control. Privacy preserving access policy, data anonymity, forward security	This is only a theoretical model not implemented in a real cloud environment
6	Rigidity in implementing complex access control Policies. [9]	Hierarchical identity based encryption and CP-ABE algorithms	Delegates the computation to the CSP and assures fine grained access control	Difficult to implement in real cloud environments
7	User needs to execute the whole decryption operation. Since mobile Devices, it is time-consuming and inefficient. [14]	MA-ABE algorithm	Supports fine grained access for multiple users	Computation time and complexity are high

IV. CONCLUSION

Many cloud access control schemes vary from the description of rules for the access control. For better service quality and security, there is a necessity for developing a privacy preserved access control models. Such a system needs to maintain the confidentiality and privacy of user's data in the public cloud from others. Also, there is a need for designing a high security access control scheme with little costs of computation, communication and storage. Here, the work focused on the analysis of various access control schemes of cloud.

REFERENCES

[1] Ziyuan Wang, "Security and Privacy Issues within the Cloud Computing", International conference on computational and information sciences,2011.

[2] Https://books.google.co.in/A Guide to Building Dependable Distributed Systems.

[3] D. E. Bell, Len LaPadula,"Secure Computer Systems: Mathematical Foundations", MITRE Technical Report 2547, Volume I

[4] Harris, S. Mike Meyers' CISSP (R) Certification Passport. 2002, p. 422.

[5] Suhendra, V. A Survey on Access Control Deployment. Vol. 259, 2011, pp. 11-20.

[6] Al-Kahtani, R. Sandhu. A Model for Attribute-Based User-Role Assignment. – In: ACSAC'02, IEEE Computer Society,

[7] Brucker, A., L. Brugger, P. Kearney, B. Wolff,"An Approach to Modular and Testable Security Models of Real-World Healthcare Applications", SACMAT'11.

[8] Zhang.R,L.Liu, J.Li, Z. Han,"RBTBAC: Secure Access and Management of EHR Data",e-HISec'2011.

[9] Wan.Z, J. Liu, R. H. Deng," HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing," IEEE Transactions on Information Forensics and Security, Vol. 7, April 2012, No 2, pp. 743-754.

[10] Jeremy.H,L.Ben,"Toward Hierarchical Identity-Based Encryption",EUROCRYPT 2002, Vol. 2332, pp. 466-481.

[11] Sue Huang, Yuan Luo," Achieve distributed, scalable and effective
Access control in cloud storage services", 2014.

[12] Liu.H, Q. Xiong, H.Ning, Laurence T. Yang," Shared Authority Based Privacy-Preserving Authentication Protocol in Cloud Computing", IEEE Transactions on parallel and distributed system, January 2015,

[13] M. Ed-daibouni, A. Lebbat, S. Tallal, H. Medromi, "A Formal Specification Approach of Privacy aware

Attribute Based Access Control (Pa-ABAC)
Model for Cloud Computing", 2014.

[14] D. Chen, L. Wan, C. Wang, Pan, Y.Ji," A multi-authority attribute-based encryptionScheme with pre-decryption", 7th international symposium on parallel architectures, algorithms and programming– 2015.

[15] Goyal, V., O. Pandey, A. Sahai, B.Waters. Attribute Based Encryption for Fine-Grained Access Control of Encrypted Data. – In: Proc. of 13th ACM Conference on Computer and Communications Security (CCS'06), November 2006.