A Survey on Access Control Models and Encryption Schemes for Cloud Storage System

Pooja B. Gajeli, Pratibha S. Yalagi

***Abstract*— The cloud storage service is the technology in cloud computing Architecture, which provides online storage services for data owners via the Internet and enables data owners to remotely store their data in to cloud. Providing security is most important need in the cloud storage system; For example, consider data owner share their data to the authorized user depends on their privilege, so the data must be protected against cloud service provider and also unauthorized users. Hence, there is a need to design authorization model and to protect data. As a part of the access control process, the authorization decision needs to be taken by data owner based on certain authorization model. An authorization model contains all required elements needed for the decision (e.g., subjects, objects, and roles) as well as their relations. This paper studies on number of access control models and encryption schemes which would helpful to implement authorization model and to protect data according the users requirement.**

***Index Terms*— Cloud storage, Access control models, Encryption, Re-encryption.**

I. INTRODUCTION

Cloud computing is a developing emerging technology and has been adopted on a large scale. One of the services of cloud computing used intensively is cloud storage system. In cloud, many data owners share their data to authorized user. This requires providing access control mechanism for authorized user to access data and also protecting the cloud service provider and unauthorized users. There are so many access control models to provide access control mechanism.

This paper reviews various access control models that are used to provide privileges by data owner to the authorized users .It also explains the different encryption techniques used to prevent the information from attackers. In access control models, ABAC (Attribute Based Access Control) is an existing model was modified in a multi-authority access in a cloud storage system for security as well as scalability [3]. Access Control Lists (ACLs) are oldest and basic access control [20].This model is not suitable for dynamic system. With an RBAC, The role can be assigned by their names, and also determine set of permissions to be granted to users [3].Role-based Access Control (RBAC) is a best access control model than the ACL paradigm [3].ABAC is particularly useful for position in which cloud or data owners want unanticipated users to be able to get access as long as have a attributes that meet certain criteria [3].In Policy Based Access Control(PBAC),An Risk-Adaptive Access Control (RAdAC) model is devised to bring adaptable, real-time, multi-authority, risk-aware access control to the enterprise[4]. Unlike RAdAC, PBAC and ABAC cannot adequately address the need for dynamism and changes in the risk levels.

The cloud storage and applications may needs definitive security tasks including data integrity, confidentiality, robustness, access control and privacy. Providing security in cloud storage is the challenging task. There are various cryptographic methods to provide security on data in a cloud storage system. The Access control models such as MAC, ABAC, PBAC, RBAC, RAdAC and encryption technique schemes such as proxy re-encryption (PRE) scheme, Identity based PRE, Attribute based PRE, Type based PRE, Key-private PRE and Time-Based PRE are discussed in the following section.

II. ACCESS CONTROL MODELS AND ENCRYPTION SCHEMES

A. Mandatory Access Control (MAC)

The MAC model has another name called as Latices-based Access Control model. This model which is described hard to implement and also more secure than DAC and ACLs [2]. In this model, system can assigns secure attribute to subject as well as object. Commonly, a subject cannot change the secure attributes of another subject i.e. the system can decide that the subject has rights to access the object by comparing the secure attributes of the subject as well as object [2]. The oldest DAC model and MAC model are both unsuitable for the data security needs of many organizational sectors [1], [2]. The RBAC is an alternative solution and supplement to old models DAC and MAC. However, The MAC is not a without genuine limitations. The position and security administration by the system with this model places limitations on user roles that are while to prevents the dynamic conversion of hidden policies, security policies, and require big parts of operating system and related service to be “reliability” and located out of the access control structure.

B. Role-based Access Control (RBAC)

With an RBAC, the roles can be accepted by their names, and they determine the sets of privileges to be granted to the users. In addition, it is efficient to check which users have access to a given privilege and what privileges have been granted to the given user. The defined number of roles can perform many users or user types, and roles can be allowed to users by improper group [3]. An RBAC must be strained to

Manuscript received October 22, 2016

handle dynamic changed attributes, such as time of day and also location.

C. Attribute Based Access Control (ABAC)

With an ABAC, there is no need to assign role names or role because this model is used as attributes. A potentially maximum number of attributes must be accepted and managed, and attributes must be selected by authority group. In addition, attributes have no meaning up to they are associated with user, association, or object, and it is not practical analysis to which users have access to a given privileges and also what privileges have been granted to a given user.

- Role-Based Access vs. Attribute-Based Access

Simplifying the ABAC concept may prove helpful [3]. If a user has many attributes; that attributes are reflected in the objects which are accessed by that user, then the access is granted to that user. Where as in model RBAC, the authority are granted to a user over roles must be and classify to resolve if desired access to be granted i.e. a user assign set of roles with an RBAC, while ABAC privileges can be achieved dynamically by ethic of user's attributes. In an RBAC model, privileges are defined an operation on object, so allowed only combinations of operations and object.

When both models ABAC and RBAC are examined together then premises goes like this:

• The RBAC has been widely supported and also provides organizational and security advantages.

• The ABAC is a modern, easy to implement, and hold real-time coincidental states as access control parameters.

• Both RBAC and ABAC models can be used by considering roles as a user attributes.

D. Policy Based Access Control (PBAC)

The existing models are does not support multi-policy and flexibility. The PBAC that is Policy Based Access Control is a different from other models which control session only for subject authority, PBAC discerns policy based access control by determining attribute to elaborate session property, application logic, performing different policy management method i.e. free from application logic, and proposing a self-reliant access control decision mechanism. As an issue, PBAC provides more flexible on restricting session, and makes great improvement on supporting of multi-policy [4]. As shown in table 1, the observation indicates that PBAC is the preferable and best to the present access control models for e.g. ACLs, MAC, RBAC, ABAC etc.

E. Risk-Adaptive Access Control (RAdAC)

Organizations and industries are not static; they constantly develop and respond to a variety of stimuli, which can include legal requirements, economic and also financial realities, market challenges, a various type of risk factors, and leadership styles [5]. Their dynamic nature means the policies that guide them must also be adaptable; this naturally enlarge to the organization's security and access control requirements as well. The security threats, injury, damage that organizations face are also dynamic, so they must be constantly assess the risk to their IT infrastructure and the related data[5]. Even the more advanced access control paradigms, such as ABAC, RBAC and PBAC cannot adequately address the need for dynamically and changing in the risk levels. The Risk-Adaptive Access Control (RAdAC) model was devised to bring real-time, flexible, risk-aware access control to the enterprise.

Finally, RAdAC faces various types of non-technical challenges, including those of policy and law for cloud or in an organization etc.Does deploying the RAdAC in certain environments violate law? Who is accountable if security breach were to occur, given that the decisions to allow or the deny access to a system are automated? Are the system owners, the RAdAC implementers and also administrators, and/or the RAdAC system designers eventually responsible if a breach were to occur? These questions must be addressed before RAdAC can be extensively deployed, and certainly before organizations feel congenial allowing RAdAC to control access to their sensitive information.

The figure 1 shows that complexity of increasing sharing requirements and data access drive the need for increasingly complex access control mechanisms and models. The DAC model is a basic and oldest model. It provides less policy and it does not suitable for dynamic system. The MAC model provide security level and its better than DAC. The RBAC and ABAC model are more increasing accessing policy for assigning privileges to the user than MAC and DAC model. The difference in RBAC and ABAC is that, the RBAC is based on subject policy and ABAC is based on attribute policy. The RAdAC and PBAC model provides dynamic policy. In that, RAdAC is more risk to implement and more flexibility than PBAC model.

Access Control Models

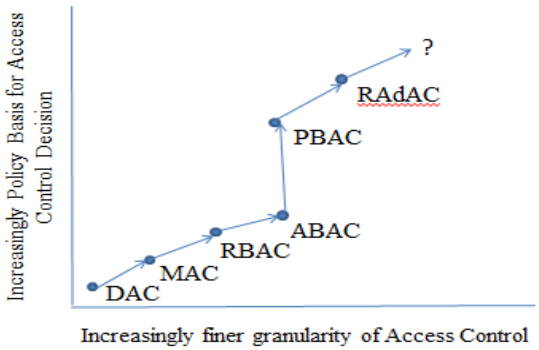

Figure1. Increasing process of Access Control Models

F. Proxy Re-encryption scheme

The proxy re-encryption techniques are proposed by Mambo and Okamoto [6] and Blaze et al. [7]. This re-encryption is a cryptographic technique which is translates the ciphertexts from one encryption key into another encryption key. It is useful to forward encrypted data without having to disclose the cleartexts to the prospective users. The re-encryption rule should be independent of key to prevent agree with private keys of the sender and also recipient. The main advantage of this PRE [8] technique i.e. they are unidirectional (e.g. Alice can delegate to Cheris without Cheris having delegate to her).They do not require delegators to disclose their entire secret key to anybody. An algorithm of proxy re-encryption transforms cipher text with PKA i.e. public key to another cipher text PKB by using the

re-encryption key RK A→B i.e. A is data owner and B is cloud storage. The server doesn't know the equivalent clear text, where PKA and PKB can be only decrypted with different key KA and KB respectively. Proxy re-encryption scheme has many applications in added with previous proposals [9], [10], [11], [12] for operating cryptographic operations on cloud storage limited devices, email forwarding, secure network file storage.

G. Type Based Proxy Re-encryption Scheme

This type of proxy re-encryption scheme is proposed by Tang [13]. This encryption scheme assures data confidentiality and fine gain access control. Type based proxy re-encryption enables delegator to implement fine grained policies with the one key pair without any trust on the proxy. In this scheme the delegator categorizes his ciphertexts into different subsets. Then the decryption of each subset is delegated to a specific delegate.The ciphertexts for delegator are generated based on delegator's public key and the message type which is used to identify the message subset. The type based PRE has the following properties.

1. The delegator needs only one key pair. So, key management problem can be reduced.
2. The delegator can choose appropriate proxy for a special delegate, which is based on the awareness of the delegation. Compromise of the one proxy key will only affect one subset of messages.

H. Key Private Proxy Re-encryption Scheme

This scheme is proposed by Ateniese et al. [8]. In a key private PRE it's impossible for set of colluding users and proxy to acquire the recipient of message from the ciphertext and the set of public keys. To achieve key private PRE is possible when the basic encryption scheme is the key-private. The privacy of key encryption provides key privacy under which the encryption was performed [14]. The KP-PRE scheme formulates the approach of the key privacy for the proxy re-encryption schemes, where the work of proxy which perform translation without differentiate the identities of the participating parties. In addition, to hide the contents of files from proxy, it's also useful to suppress metadata as much as possible. For example, we might want the proxy fileserver to re-encrypt important files for the certain recipients without the proxy recipient user's identity.

I. Identity Based Proxy Re-encryption Scheme

The identity based PRE scheme was introduced by Shamir [15]. In an identity based PRE scheme, arbitrary strings such as an email addresses or IP address can be used to form public keys for users. In an identity based encryption scheme, senders encrypt messages using recipient's identity (i.e. string) consider as a public key. For instance, Alice could encrypt message for Bob by just only using his email address that is key [16]. The identity based proxy re-encryption technique allows proxy to translate encryption of text under Cheris's identity into computed with the Alice's identity. The proxy uses re-encryption keys or proxy keys, to perform translation without learning the plaintext. The IB-PRE [17] scheme ensures that no reasonable set of colluding key holders will obtain advantage against users. The IBE has number of practical applications such as secure email forwarding, attribute-based delegations and an access control in networked file storage. This type of re-encryption schemes is used to realize the secrecy of data.

J. Attribute Based Proxy Re-encryption Scheme

The concept of AB-PRE was introduced by Sahai and Waters [18]. In this proxy re-encryption scheme, the semi-trusted proxy and some appropriate additional information can translate ciphertext with set of attributes into a new ciphertext with set of attributes into a new ciphertext under another the set of attributes on the same information. This encryption scheme, allows the encrypted data with fine-grained access control. The attribute based encryption is a generalization of IBE. The data provider can express how he or she wants to share data in the encryption algorithm itself. In an ABE scheme, the data is stored on the cloud storage i.e. storage server in encrypted form while various users are still allowed to decrypt different pieces of data as per the security requirement policy. This effectively removes the needs to rely on the storage server for prohibiting unauthorized data access.

J. Time Based Proxy Re-encryption Scheme

The basic approach of Time PRE scheme is that it permits every user's right to expire automatically after the pre-defined time period [19]. In case, the data owner goes offline at the computing of user revocations. The primary idea is to organize the view of time into the combination of both Proxy re-encryption (PRE) and Attribute based encryption (ABE) the time PRE technique allows the CSP to automatically data can re-encrypt without receiving any type of PRE keys from data owner. This scheme can avoid prospect security risks that are emerged with delay of issuing PRE keys.

TABLE II. Comparison of Encryption Schemes

Encryption schemes	**Advantages**	**Disadvantages**
PRE	It is secure against plain text attacker	Plaintext attack and Collusion problem
TB-PRE	Ciphertext Privacy Control and Semantic security	Encoding operations through encrypted messages is impossible
KP-PRE	Provides CCA Security	The privacy of key proof is more crucial than that of CPA security
IB-PRE	It is secure against adaptive Chosen ciphertext Attack	Difficult to find capable construct for the multi-use CCA secure IBE-PRE.
AB-PRE	Allows Fine-grained access control on the encrypted data	Flexibility and Average efficiency
TB-PRE	1.Scalable user revocation 2.Minimizes the workload of data owner	Requires valid time period to be same for whole attributes related with the user.

CONCLUSION

In this review paper, comparative study on access control models and encryption schemes is carried out to provide privileges to the user for accessing the data and to protect data in cloud storage. Comparatively the analyses shows that RAdAC and PBAC is more flexible models and have the ability of multi-policy backing and also RAdAC support dynamic policy.

In the cloud storage security is an important aspect of quality of service and security is another important factor for the protection of data. So, various proxy re-encryption techniques are used. This paper reviews various proxy re-encryption schemes used in the cloud storage system and the merits and demerits of algorithms have been discussed. The future work is to develop better PRE schemes which works in cloud storage i.e. distributed environment.

REFERENCES

[1] R. Anderson. Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley Computer Publishing, New York, New York, 2001.

[2] D. Bell and L. LaPadula. Secure computer system: Unified exposition and multics interpretation. TR M74-244, March 1976.

[3] E. Coyne and T. R. Weil, "Abac and rbac: Scalable, flexible, and auditable access management," IT Professional, vol. 15, no. 3, pp. 14–16, 2013.

[4] Lin Zhi,Wang Jing,Chen Xiao-su and Jia Lian-xing,"Research on Policy-based Access Control Model"IEEE Conference Publications,Year: 2009, Volume: 2,Pages: 164 - 167, DOI: 10.1109/NSWCTC.2009.313.

[5] B. Farroha and D. Farroha," Challenges of "operationalizing" dynamic system access control:Transitioning from ABAC to RAdAC", Systems Conference(SysCon),2012 IEEE International,Year:2012,Pages:1-7, DOI: 10.1109/SysCon. 2012.6189525.

[6] M. Mambo and E. Okamoto, "Proxy Cryptosystems:Delegation of the Power to Decrypt Ciphertexts",IEICE Trans. Fundamentals of Electronics, Comm. and Computer Sciences, 1997, pp. 54-63.

[7] M. Blaze, G. Bleumer, and M. Strauss,"Divertible Protocols and Atomic Proxy Cryptography", Proc.Int'l Conf. Theory and Application of Cryptographic Techniques ,1998, pp. 127-144.

[8] G. Ateniese, K. Benson, and S. Hohenberger, "Key-Private Proxy Re-Encryption", Proc. Topics in Cryptology, 2009, pp. 279-294.

[9] Matt Blaze, G. Bleumer, and M. Strauss, "Divertible protocols and atomic proxy cryptography", In Proceedings of Eurocrypt, 1998, pp. 127–144.

[10] Yevgeniy Dodis and Anca Ivan, "Proxy cryptography revisited". In Proceedings of the Tenth Network and Distributed System Security Symposium, February 2003.

[11] Markus Jakobsson, "On quorum controlled asymmetric proxy re-encryption", In Proceedings of Public Key Cryptography, 1999, pp. 112,121.

[12] Giuseppe Ateniese, Kevin Fu, Matthew Green, and Susan Hohenberger, " Improved Proxy Reencryption Schemes with Applications to Secure Distributed Storage" , In Proceedings of the 12th Annual Network and Distributed System Security Symposium, February 2005.

[13] Q. Tang, "Type-Based Proxy Re-Encryption and Its Construction", Proc. Ninth Int'l Conf. Cryptology in India, 2008, pp. 130-144.

[14] Mihir Bellare, Alexandra Boldyreva, Anand Desai,and David Pointcheval, "Key-privacy in public-key encryption", In ASIACRYPT, 2001, pp. 566-582.

[15] Shamir, "A Identity-based cryptosystems and signatures schemes", In Advances in Cryptology, 1984, pp. 47-53.

[16] Matthew Green and Giuseppe Ateniese, "Identity-Based Proxy Re-Encryption", ACNS 2007, pp. 288-306.

[17] Dan Boneh and Matthew K. Franklin. "Identity-based encryption from the Weil Pairing", In Advances in Cryptology (CRYPTO 2001), Springer, 2001, pp.213–229.

[18] A.Sahai and B.Waters,"Fuzzy Identity Based Encryption", Springer, 2005, pp. 457–473.

[19] Qin Liu, Guojun Wang and Jie Wu, "Time-Based Proxy Re-encryption Scheme for Secure Data Sharing in a Cloud Environment", Information Sciences, In Press, 2012.

[20] S. Pozo; A. J. Varela-Vaca; R. M. Gasca,"AFPL2, an Abstract Language for Firewall ACLs with NAT Support Dependability", 2009. DEPEND '09. Second International Conference on Year: 2009 ,Pages: 52 - 59, DOI:10.1109/DEPEND.2009.14

TABLE I. Comparison of Access Control Model

	features of implementation			**Analysis of performance**		
	Relationship of property and privilege	Description method of policy	Realization method of decision	Flexibility	Comprehensive Control	Multi-policy Supporting
DAC	No property description	Access control matrix	Integrated with application logic	Poor	Poor	No
MAC	Equal	Security level	Integrated with application logic	Limited	Poor	No
RBAC	Equal	Restriction of subject	Integrated with application logic	Good	Good	Limited
ABAC	Equal	Restriction of attribute	Integrated with application logic	Good	Good	Limited
PBAC	No relation	Independent policy language	Independent from application logic	Better	Better	Better
RAdAC	No relation	Independent Policy language	Independent from application logic	Best	Best	Best, support dynamic policy