Scientific Journal of Impact Factor (SJIF): 5.71
e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 5, Issue 02, February -2018

# Public Cloud Storage Security

*Balaji.S[1], B.Akshay Prasad[2], Professor Dr.R.Prasanna Kumar[3]*

*[1]Computer Science and Engineering, S.A. Engineering College,*
*[2]Computer Science and Engineering, S.A. Engineering College,*
*[3]Computer Science and Engineering, S.A. Engineering College*

**Abstract—** *Data access control is one of the most challenging issue in public cloud storage. Ciphertext policy attribute based encryption algorithm has been implemented because it is a promising technique to provide fine grained and secure data access control for cloud storage(public) with cloud servers. Presently, ciphertext policy attribute based encryption, the single attribute authority must execute the time consuming user validation, verification and secret key distribution, and hence it results in a single point performance overhead. when a ciphertext policy attribute based encryption scheme is implemented in real-time public cloud storage, users have to wait in the waiting queue for a significant amount of time to obtain respective secret key, therefore it costs the efficiency of the system. Although multi-authority access control schemes have been discovered but these schemes still cannot overcome the disadvantages of single-point overhead and low efficiency, due to this fact each of the authorities still manage a different attribute set.*

## I. INTRODUCTION

Cloud storage is the most widely used and productive service in cloud computing. Advantages of using cloud storage is higher accessibility, greater reliability, instant deployment and superior protection. Apart from these benefits, it also brings new challenges to data access control. Data access control is a critical issue, in ensuring data security. Public cloud storage is generally maintained by cloud service providers (CSP), Cloud service providers are not trusted by the data owners, the traditional data access control methods in the Client/Server system are not feasible in cloud storage system. The data access control in cloud storage system has thus became a challenging issue.

To solve the problem of access control in cloud storage ciphertext policy attribute based encryption is considered as the most promising techniques. A salient feature of ciphertext policy attribute based encryption is that it gives the data owners direct control rights according to the access policies, to give flexible and secure access control for cloud storage archtecture. In ciphertext policy attribute based encryption scheme, the access control is attained by cryptography method, In cryptography an owner's confidential data is encrypted with access tree over attribute and secret key is labelled according to their particular attributes. If the attribute associated with the client or user's secret key satisfy the access tree, then the user can decrypt the corresponding ciphertext to obtain the required plaintext. Until now, the ciphertext policy attribute based encryption based access control schemes for public cloud storage have been developed into two different types. Single authority scenario, and multi authority scenario. Even though existing ciphertext policy attribute based encryption access control schemes have a lot of exciting features, they are neither efficient in key generation nor robust. Here there is only one authority in charge of all attributes. In single authority scheme, crash or offline of the authority makes all secret key requests unavailable during that period. A straight forward idea is to remove the single point bottleneck this allow multiple authorities to jointly maintain the universal attribute set, just so that each of them is able to serve secret keys to respective users independently. By implementing multiple authorities to share the load, the severity of the single point bottleneck can be reduced to a some extent. However, this solution will bring lots of threats in security issues. As there are multiple functionally identical authorities performing the similar procedure, it is impossible to find the responsible authority if some mistakes have been made or some malicious behaviours have been implemented in the process of secret key distribution and secret key generation. For instance, an authority may distribute secret keys beyond user's legitimate attribute set. Such a breach in the security makes this straight forward idea hard to meet the security requirement of access control for cloud storage. Recently, TMACS, is a threshold multi authority ciphertext policy attribute based encryption access control scheme for cloud storage, where multiple authorities jointly manage a uniform attribute set. Actually it addresses the single point bottleneck of security and performance, but introduces some additional overhead. Therefore, we present a feasible solution which not only gives robustness and efficiency, but also guarantees that the solution is as secure as the original single-authority schemes.

## II. LITERATURE SURVEY

In the paper titled "Enabling personalized search over encrypted outsourced data with efficiency improvement", proposed by Z. Fu, K. Ren, J. Shu, X. Sun, and F. Huang [1]- The searchable encryption scheme overt the outsourced data has become the hot research field in cloud computing. The existing work on the outsourced data follow a model called " one size fits all" and it ignore personalized search intentions. We are in need to search an encryption scheme with supports a personalized search to improve user search experience which is a challenging task till now. For the first time, this paper has proposed to solve the problem of personalized keyword search over encrypted data (PRSE).

 

Semantic ontology WordNet, which helps in building a user interest model. This is done by analysing the user's search history. To overcome the shortcoming of "one size fit all".

In the paper titled "Towards efficient content-aware search over encrypted outsourced data in cloud", proposed by Z. Fu, X. Sun, S. Ji, and G. Xie [2] - The increase in the use of cloud computing has made an abrupt growth in the number of users in the cloud. The data are always been encrypted to prevent intruders. Many schemes are proposed to search the encrypted data using the keywords. A keyword based search scheme which ignores the semantic representation of users and it cannot meet the search intention of users. This paper proposes an innovative search scheme based on semantic relationship and concept hierarchy. To be specific, this scheme first indexes the document and then this trapdoor which is based on the concept of hierarchy. In order to improve the search efficiency this paper uses a tree based index structure which is used to organize all document index vector. The result is based on the real world data which shows the scheme is efficient than before.

In the paper titled "A dynamic secure group sharing framework in public cloud computing", proposed by K. Xue and P. Hong [3]- The privacy and the security of group sharing have become the two major issues because of the popularity of group data sharing in the public cloud. The cloud cannot be a trusted third party because of its semi-trust nature. So the traditional security model cannot straightforwardly generalize into the clouds which based on group sharing. The framework holds proxy signature and enhanced TGDH and a proxy re-encryption . The group leader can efficiently transfer the privilege to their group members by applying a proxy signature technique. The TGDH scheme allows the group members to negotiate and update the key pairs by the help of cloud servers. Computational intensive operations can be delegated to the cloud servers by adopting proxy re-encryption.

In the paper titled "Attribute-based access to scalable media in cloud-assisted content sharing", proposed by Y. Wu, Z. Wei, and H. Deng [4]- A Multi-message Ciphertext policy Attribute-Based Encryption is the technique proposed by this paper. It employs the MCP-ABE to design the access control mechanism for sharing media based on the consumers attribute. MCP-ABE allows content provider to designate access policy and encrypt the messages, this makes the scheme more efficient. This paper also shows how to support the resources mobile devices by using offloading computational operations without compromising data privacy.

In the paper titled "Improving security and efficiency in attribute based data sharing", proposed by J. Hur [5]- Even though the existing data sharing system proposes to encrypt the data before sharing , the multiparty access control has become a challenging issue. This paper proposes a secure data sharing in OSN which is based on cipher-text policy proxy encryption and sharing secret. This scheme allows the user to customize the access policy to protect the sensitive data of the user. It also presents a multiparty control model that enables the disseminators to upgrade their access policies of cipher text. It develops decryption which reduces the computational overhead. This gives the referring capability on the result from the OSNs service provider.

In the paper titled "Cipher text policy attribute-based encryption", proposed by J. Bethencourt, A. Sahai, and B. Waters [6]- In a distributed system the user should be only allowed to access only if they posses certain credentials. The only method to enforce such policies is to employ a trusted server for storing the data. If the server storing the data is comprised then the confidentiality will also be comprised. This paper proposes a system to realise complex access control. By applying this technique the data can be kept confidential even though the server is untrusted. Previous techniques uses attributes to encrypt the data and built the policies according to the user need. This method is same as the traditional method in concept wise such as role-based access control.

In the paper titled "TMACS: A robust and verifiable threshold multi-authority access control system in public cloud storage", proposed by W. Li, K. Xue, Y. Xue, and J. Hong [7] - A promising cryptographic tool is Attribute-based Encryption which guarantees the data owners to control their data. The ABE involves an authority to maintain the attribute set .That is used to bring a single-point bottleneck on security and performance. Some multi-authority system is proposed, in which the authorities are separately maintained. This paper they conduct a threshold of multi-authority, CP-ABE access named as TMACS. In which the authorities jointly manage the attributes. In TMACS the master key can be shared among the authorities. The analysis about the security and performance shows that TMACS is not only verify when t authorities are comprised, but it also robust when less then authorities mentioned. By efficiently combining the traditional scheme with TMACS, we derive a new hybrid one that satisfies the attributes coming from different authorities.

In the paper titled "Efficient decentralized attribute based access control for cloud storage with user revocation", proposed by J. Chen and H. Ma [8]- The existing systems provide way to access the data if the user produces the authenticating credentials for authenticating the user in the server. If this has to be compromised then the security will also get compromised. We propose a cipher-text policy attribute based encryption which is a complex structure to provide access only to authenticated user. This will keep the cipher text protected even if the server is not trustworthy and prevents collision attacks. The attributes of the proposed system describes the user credentials. The decryption is done for users who can encrypt.

In the paper titled "DAC-MACS: Effective data access control for multi-authority cloud storage systems", proposed by K. Yang, X. Jia, K. Ren, and B. Zhang [9]- The most challenging issue in cloud storage is Data access control which can be addressed using cipher text-policy Attribute, enforces data access control. But sometimes user's temporary states are considered for making user policies. So this idea was proposed which takes up location of user and permanent states. This method does not require any additional revocation technologies where the security and performance are increased.

 

In the paper titled "LABAC: A location-aware attribute-based access control scheme for cloud storage", proposed by Y. Xue, J. Hong, W. Li, K. Xue, and P. Hong [10]- Outsourcing data to cloud makes the user free up their storage and share them easily with others. But privacy and the security are to be considered. Also, to support fine grained access and taking up the concern of security is not possible. No schemes can consider all this and provide a fine grained access with time sensitive data publishing. The time release encryption is merged with the CP-ABE a TAFC is produced which addresses all the issues in the traditional system taking into account the times which produces secure and efficient OSNs.

**III.COMPARISION TABLE**

| S. No | TOPIC | TECHNOLOGIES | INFERENCE | ADVANTAGES | DISADVANTAGES |
|---|---|---|---|---|---|
| 1 | Enabling personalized search over encrypted outsourced data with efficiency improvement | semantic ontology WordNet | A user interest model for individual user by analysing the user's search history, and adopt a scoring mechanism to express user interest smartly. | Very efficient and effective. | Does not have hierarchy and semantic relationship. |
| 2 | Towards efficient content-aware search over encrypted outsourced data in cloud | Hierarchy and the semantic relationship between concepts in the encrypted datasets. | At first it indexes the documents and builds trapdoor based on the concept hierarchy. | more efficient than previous scheme | This technique is not dynamic |
| 3 | A dynamic secure group sharing framework in public cloud computing | Proxy signature, enhanced TGDH and proxy re-encryption | The framework combines proxy signature, enhanced TGDH and proxy re-encryption together into a protocol. By applying the proxy signature technique, the group leader can effectively grant the privilege of group management to one or more chosen group members. | Highly efficient and satisfies the security requirements for public cloud based secure group sharing. | Encrypted data cannot be kept confidential if the storage server is untrusted. |
| 4 | Attribute-based access to scalable media in cloud-assisted content sharing | Multi-message Ciphertext Policy Attribute-Based Encryption (MCP-ABE) technique | Supports resource-limited mobile devices by offloading computational intensive operations to cloud servers while without compromising data privacy. | Efficient and flexible | Robustness is not achieved |

 

| | | | | | |
|---|---|---|---|---|---|
| 5 | Improving security and efficiency in attributebased data sharing | Cipher text-policy attribute-based proxy re-encryption and secret sharing | Presents a multiparty access control model, which enables the disseminator to update the access policy of cipher text if their attributes satisfy the existing access policy. | An efficient attribute revocation method that achieves both forward and backward secrecy | Is not Secure against collusion attacks |
| 6 | Cipher text policy attribute-based encryption | Cipher text-policy attribute-based encryption | If any server storing the data is compromised, then the confidentiality of the data will be compromised. In this paper we present a system for realizing complex access control on encrypted data that we call ciphertext-policy attribute-based encryption. | Encrypted data can be kept confidential even if the storage server is untrusted. Secure against collusion attacks | Requires central authority and global coordination among multiple authorities. |
| 7 | TMACS: A robust and verifiable threshold multi-authority access control system in public cloud storage | Threshold multi-authority CP-ABE access control scheme | In TMACS, taking advantage of (t,n ) threshold secret sharing, the master key can be shared among multiple authorities, and a legal user can generate his/her secret key by interacting with any t authorities. Security and performance analysis results show that TMACS is not only verifiable secure when less than t authorities are compromised, but also robust when no less than t authorities are alive in the system. | Security and system-level robustness is achieved. | Encrypted data cannot be kept confidential if the storage server is untrusted. |

 

| | | | | | |
|---|---|---|---|---|---|
| 8 | Efficient decentralized attribute based access control for cloud storage with user revocation | Decentralized cipher text-policy attribute-based encryption access control scheme | Conventional ABE schemes depend on a single authority to issue secret keys for all of users, which is very impractical in a large-scale cloud. A decentralized ABE scheme should not rely on a central authority and can eliminate the need for collaborative computation. | Does not require any central authority and global coordination among multiple authorities. | Encrypted data cannot be kept confidential if the storage server is untrusted. |
| 9 | DAC-MACS: Effective data access control for multi-authority cloud storage systems | Multi-authority CP-ABE scheme | DAC-MACS (Data Access Control for Multi-Authority Cloud Storage), an effective and secure data access control scheme with efficient decryption and revocation. | An efficient attribute revocation method that can achieve both forward security and backward security. | Not flexible in terms of users attributes and locations |
| 10 | LABAC: A location-aware attribute-based access control scheme for cloud storage | Location-aware attribute-based access control mechanism (LABAC) for cloud | Data access control is a challenging issue in cloud storage. Ciphertext-Policy Attribute-based Encryption (CP-ABE) is a potential cryptographic technique to address the above issue, which is able to enforce data access control based on users' permanent characteristics | Data owners can flexibly combine both users' attributes and locations to implement a fine-grained control of their data | Security and system-level robustness is not achieved. |

## IV.CONCLUSION

In this paper, we proposed a new framework, named RAAC, to eliminate the single-point performance bottleneck of the existing CP-ABE schemes. By effectively reformulating CPABE cryptographic technique into our novel framework, our proposed scheme provides a fine-grained, robust and efficient access control with one-CA/multi-AAs for public cloud storage. Our scheme employs multiple AAs to share the load of the time-consuming legitimacy verification and standby for serving new arrivals of users requests.

 

**REFERENCES**

[1] Z. Fu, K. Ren, J. Shu, X. Sun, and F. Huang, "Enabling personalized search over encrypted outsourced data with efficiency improvement," IEEE Transactions on Parallel & Distributed Systems, vol. 27, no. 9, pp. 2546–2559,
[2] Z. Fu, X. Sun, S. Ji, and G. Xie, "Towards efficient content-aware search over encrypted outsourced data in cloud," in in Proceedings of 2016 IEEE Conference on Computer Communications (INFOCOM 2016). IEEE, 2016, pp. 1–9.
[3] K. Xue and P. Hong, "A dynamic secure group sharing framework in public cloud computing," IEEE Transactions on Cloud Computing, vol. 2, no. 4, pp. 459–470, 2014.
[4] Y. Wu, Z. Wei, and H. Deng, "Attribute-based access to scalable media in cloud-assisted content sharing," IEEE Transactions on Multimedia, vol. 15, no. 4, pp. 778–788, 2013.
[5] J. Hur, "Improving security and efficiency in attribute based data sharing," IEEE Transactions on Knowledge and Data Engineering, vol. 25, no. 10, pp. 2271–2282, 2013.
[6] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertextpolicy attribute-based encryption," in Proceedings of IEEE Symposium on Security and Privacy (S&P 2007). IEEE, 2007, pp. 321–334.
[7] W. Li, K. Xue, Y. Xue, and J. Hong, "TMACS: A robust and verifiable threshold multi-authority access control system in public cloud storage," IEEE Transactions on Parallel & Distributed Systems, vol. 27, no. 5, pp. 1484– 1496, 2016.
[8] J. Chen and H. Ma, "Efficient decentralized attributebased access control for cloud storage with user revocation," in Proceedings of 2014 IEEE International Conference on Communications (ICC 2014). IEEE, 2014, pp. 3782–3787.
[9] K. Yang, X. Jia, K. Ren, and B. Zhang, "DAC-MACS: Effective data access control for multi-authority cloud.
[10] Y. Xue, J. Hong, W. Li, K. Xue, and P. Hong, "LABAC: A location-aware attribute-based access control scheme for cloud storage," in Proceedings of 2016 IEEE Global Communications Conference (GLOBECOM 2016). IEEE, 2016, pp. 1–6.

 