ATTRIBUTE BASED ACCESS CONTROL USING MULTIPLE AUTHORITIES

S.Manjula[1], P.Thanigesan[2]

[1,2]Computer Science and Engineering, Indira Institute of Engineering and Technology, Chennai, India

ABSTRACT

Data access control is a challenging issue in public cloud storage systems. Cipher text-policy Attribute-Based Encryption (CP-ABE) has been adopted as a promising technique to provide flexible, fine-grained and secure data access control for cloud storage with honest-but-curious cloud servers. However, in the existing CP-ABE schemes, the single attribute authority must execute the time-consuming user legitimacy verification and secret key distribution, and hence it results in a single-point performance bottleneck when a CP-ABE scheme is adopted in a large-scale cloud storage system.

Users may be stuck in the waiting queue for a long period to obtain their secret keys, thereby resulting in low-efficiency of the system. In this paper, we propose a novel heterogeneous framework to remove the problem of single-point performance bottleneck and provide a more efficient access control scheme with an auditing mechanism.

INTRODUCTION

Over View and Background

Cloud storage is a promising and important service paradigm in cloud computing. Benefits of using cloud storage include greater accessibility, higher reliability, rapid deployment and stronger protection, to name just a few. Despite the mentioned benefits, this paradigm also brings forth new challenges on data access control, which is a critical issue to ensure data security. Since cloud storage is operated by cloud service providers, who are usually outside the trusted domain of data owners, the traditional access control methods in the Client/Server model are not suitable in cloud storage environment. The data access control in cloud storage environment has thus become a challenging issue. To address the issue of data access control in cloud storage, there have been quite a few schemes proposed, among which Cipher text-Policy Attribute-Based Encryption (CP-ABE) is regarded as one of the most promising techniques. A salient feature of CP-ABE is that it grants data owners direct control power based on access policies, to provide flexible, fine-grained and secure access control for cloud storage systems.

Existing System

In CP-ABE schemes, the access control is achieved by using cryptography, where an owner's data is encrypted with an access structure over attributes, and a user's secret key is labelled with his/her own attributes. Only if the attributes associated with the user's secret key satisfy the access structure, can the user decrypt the corresponding ciphertext to obtain the plaintext. So far, the CP-ABE based access control schemes for cloud storage have been developed into two complementary categories, namely, single-authority scenario [5–9], and multiauthority scenario [10–12]. Although existing CP-ABE access control schemes have a lot of attractive features, they are neither robust nor efficient in key generation. Since there is only one authority in charge of all attributes in single-authority schemes, offline/crash of this authority makes all secret key requests unavailable during that period. The similar problem exists in multi-authority schemes, since each of multiple authorities manages a disjoint attribute set. In single-authority schemes, the only authority must verify the legitimacy of users' attributes before generating secret keys for them.

Disadvantages in Existing System

- Although existing CP-ABE access control schemes have a lot of attractive features, they are neither robust nor efficient in key generation.
- Since there is only one authority in charge of all attributes in single-authority schemes, offline/crash of this authority makes all secret key requests unavailable during that period.
- . In single-authority schemes, the only authority must verify the legitimacy of users' attributes before generating secret keys for them.
- As the access control system is associated with data security, and the only credential a user possess is his/her secret key associated with his/her attributes, the process of key issuing must be cautious. However, in the real world, the attributes are diverse. For example, to verify whether a user is able to drive may need an authority to give him/her a test to prove that he/she can drive. Thus he/she can get an attribute key.

Proposed System

- A straightforward idea to remove the single-point bottleneck is to allow multiple authorities to jointly manage the universal attribute set, in such a way that each of them is able to distribute secret keys to users independently.
- By adopting multiple authorities to share the load, the influence of the single-point bottleneck can be reduced to a certain extent. However, this solution will bring forth threats on security issues.
- Since there are multiple functionally identical authorities performing the same procedure.

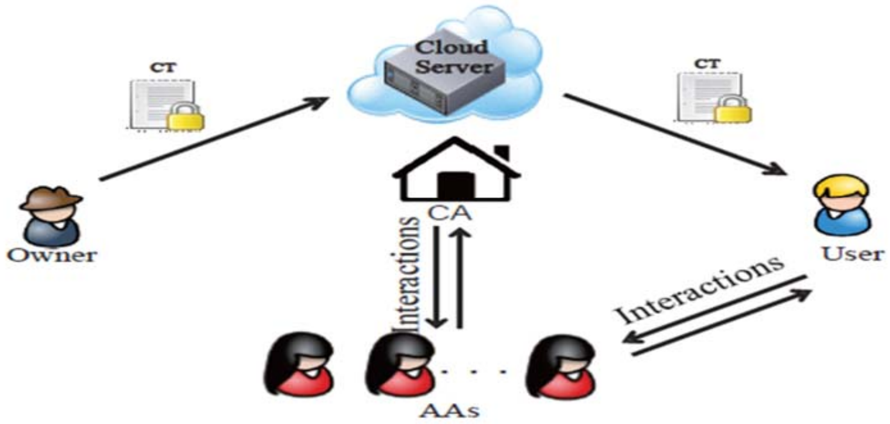
Advantages in Proposed System

It is hard to find the responsible authority if mistakes have been made or malicious behaviors have been implemented in the process of secret key generation and distribution. For example, an authority may falsely distribute secret keys beyond user's legitimate attribute set. Such weak point on security makes this straightforward idea hard to meet the security requirement of access control for public cloud storage. Our recent work, TMACS [15], is a threshold multi-authority CP-ABE access control scheme for public cloud storage, where multiple authorities jointly manage a uniform attribute set.

Actually it addresses the single-point bottleneck of performance and security, but introduces some additional overhead. Therefore, in this paper, we present a feasible solution which not only promotes efficiency and robustness, but also guarantees that the new solution is as secure as the original single-authority schemes. After the verification, it validates the credentials and forwards the certificate request to CA. Then, CA will generate a certificate for the user. Since the most heavy work of verification is performed by a selected *RA*, the load of *CA* can be largely reduced. However, the security of the scheme with single-*CA*/multi-*RAs* partly depends on the trustiness of multiple *RA*s.

SYSTEM IMPLEMENTATION

6.1 System Architecture



RESULT AND DISCUSSION

The data access control in cloud storage environment has thus become a challenging issue. To address the issue of data access control in cloud storage, there have been quite a few schemes proposed, among which *Cipher text-Policy Attribute-Based Encryption (CP-ABE)* is regarded as one of the most promising techniques. The similar problem exists in multi-authority schemes, since each of multiple authorities manages a disjoint attribute set. proposed three efficient and practical CP-ABE schemes under stronger cryptographic assumptions as expressive as To improve efficiency of this encryption technique, Euro et al. proposed a CP-ABE scheme with a constant cipher text length.

CONCLUSION AND FUTURE ENHANCEMENTS

Conclusion

This project presents a framework to integrate action aware based access control into DBMSs. An access control model is proposed to regulate the access to data performed by SQL queries based on the access purposes of the query to be executed, the types of actions that the query should execute on data and the categories of the data jointly accessed during the execution. The framework supports policy specification and enforcement. It has been defined to minimize policy enforcement overhead.

Future Enhancements

The enforcement is achieved through query rewriting. As future work we plan to:

1) build a toolkit supporting the integration of the proposed framework into different DBMSs,
2) extensively evaluate performance and dependability applying the framework to realistic case studies,
3) extend the framework integrating support for role based access control,
4) Integrate mechanisms to regulate the specification of data categories and policies and to manage policy, data and category updates.

REFERENCES

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, 2016.

[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 attributebased data sharing,” *IEEE Transactions on Knowledge and Data Engineering*, vol. 25, no. 10, pp. 2271–2282, 2013.

[6]. A. Sahai, H. Seyalioglu, and B. Waters, “Dynamic credentials and cipher text delegation for attribute-based encryption,” in Advances in Cryptology–CRYPTO 2012. Springer, 2012, pp. 199–217.

[7]. J. H. Seo and K. Emura, “Revocable identity-based encryption revisited: Security model and construction,” in Public-Key Cryptography–PKC 2013. Springer, 2013, pp. 216–234.

[8]. G. Anthes, “Security in the cloud,” Communications of the ACM, vol. 53, no. 11, pp. 16–18, 2010.