International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 06 Issue: 04 | April - 2022 Impact Factor: 7.185 ISSN: 2582-3930

Flexible Data Access Control Based on Trust and Reputation in Cloud Computing

Poojasree k c[1] and Dr. Murugan R[2]

[1]Student, Department of Master of Computer Applications School of Computer Science IT, Jain Deemed to Be University, Jayanagar 9th Block, Bengaluru, Karnataka– 560041, India.

[2]MCA Coordinator, Department of Master of Computer Applications School of Computer Science & IT, Jain Deemed to Be University, Jayanagar 9 th Block, Bengaluru, Karnataka– 560041, India.

Abstract - Cloud computing is gaining more essential cue its abundant services in data storage and retrieval. Individuals and institutions seeks cloud server as a storage medium to reduce their storage burden under local devices. As the cloud service providers are considered to be untrusted, users generally store their crucial data in an encrypted form. Data need to be accessed by other entities for fulfilling an expected service. Thus it is necessary to propose an efficient model to provide data access control on cloud data. Though many existing system studied the data access in various techniques. There is no work available based on user's trust level, they still lacks a practical solution to control cloud data access based on trust and reputation. Trust plays an important role in data sharing. Proposed work, efficiently handles data access in cloud computing based on trust evaluated by the data owner and/or reputations generated by a number of reputation centers in a flexible manner by applying Attribue-Based Encryption. Context-aware trust and reputation evaluation is used in order to support various control scenarios and strategies.

Keywords: CSP,RC,QoS,CP-ABE,PRE

1.INTRODUCTION

In cloud computing, a scheme for controlling data access flexibly based on trust and reputation. We propose multi-dimensional controls for cloud data access based on the data owner's policies and strategies. To be more specific, the data owner encrypts its data using a symmetric secret key K. To support various control strategies, this encryption key can be divided into multiple parts. For example, in order to ensure data security and privacy in a variety of situations, the data owner can control data access based on either individual trust evaluation or reputation generated by multiple RCs, or both. In much more specifics, the secret encryption key K is made up of several parts. The data owner encrypts different parts of K with different encryption keys that are handled by the data owner and a number of reputation centres (RCs) in different contexts based on different reputation properties. Later on, the data owner and/or RCs can control data access based on the data encryption method handled by the data owner. Specifically, the contributions inspire securing cloud data by controlling its access in a flexible manner based on the trust and reputation evaluated by the data owner and/or multiple reputation centres.

2.RELATED WORK

With rapid development of cloud computing, more and more enterprises will outsource their sensitive data for sharing in a cloud. To keep the shared data confidential against untrusted cloud service providers (CSPs), a natural way is to store only the encrypted data in a cloud. The key problems of this approach include establishing access control for the encrypted data, and revoking the access rights from users when they are no longer authorized to access the encrypted data. This paper aims to solve both problems. First, we propose a hierarchical attribute-based encryption scheme (HABE) by combining a hierarchical identity-based encryption (HIBE) system and a ciphertext-policy attribute- based

encryption (CP-ABE) system, so as to provide not only fine-grained access control, but also full delegation and high performance. Then, we propose a scalable revocation scheme by applying proxy re-encryption (PRE) and lazy re-encryption (LRE) to the HABE scheme, so as to efficiently revoke access rights from users.

3.PROPOSED SYSTEM

To propose a scheme to flexibly control data access based on trust and reputation in cloud computing multi-dimensional controls on cloud data access based on the policies and strategies set by the data owner.Data owner encrypts its data with a symmetric secret key K. This encryption key can be divided into multiple parts in order to support various control strategies.Data owner can control its data access based on either individual trust evaluation or reputation generated by multiple RCs or according to both above in order to highly ensure data security and privacy in various situations. Securing cloud data by controlling its access based on the trust and reputation evaluated by the data owner and/or multiple reputation centers in a flexible manner access the application, once they are untrusted or illegitimate transactions.

4.PROPOSED ALGORITHM

Step 1: Input the public key PK, the master key MK, and a unique user identity u.

Step2 : It chooses a random secret $mk \in \mathbb{Z}$ And outputs a public user key $pk\_u =$ g, that will be used to issue secret attribute keys for u , and a secret user key

Step 3: data owner uploads file to cloud, a symmetric key K for data encryption and is performed by the data owner. In our implementation, Advanced Encryption Standard (AES) is applied.

Step 4: User 'u' gives request for data/file, user device whenever user u would like to control the access of its data based on individual trust evaluation. The algorithm checks the TL related policies

Step 5: Reputation center is contacted, RC evaluates u's reputation and checks if it satisfies with M's access policy AA. Based on the reputation level, RC generates $rk\_RC \rightarrow u2$ if access is allowed; meanwhile, if $u1$ is contacted, it checks the eligibility of $u2$ in order to generate a personalized secret key $sk\_(TL, u1, u2)$ for $u!$ to decrypt CK.

Step 6: CSP allows $u2$ to access requested data by providing corresponding encrypted data CT and encrypted keys ($CK1$ and $CK0$) to $u2$.

5.MODULES

- Reputation center
- Assigning trust value
- Assigning Reputation value
- Data requisition
- User blacklist

Reputation center

Reputation center (RC) that has functions and capability that the user does not have and is trusted to generate and provide reputation certificates for system entities regarding different data access contexts. RC is a trusted party for reputation generation in different data access contexts. It can collect sufficient information to conduct accurate reputation evaluation, thus provide accurate reputation information of each system entity. RC is always available for registration and authorization of data access rights. But RC is not allowed to access the stored data by CSPs. RCs and CSPs don't collude with each other due to business reasons since collusion may make both of them lose profits.

Assigning trust value

Individual Trust Level (TL) is the trust evaluated by a data owner based on personal interaction and experiences. Trust into discrete levels according to its value, e.g., TL represents the i-th level of TL, $i \in$ (0, 1) , where 1 is the maximum level of TL. To effectively secure private data over the cloud, we

resort to controlling the data access based on trust levels assessed by the data owner by applying ABE. The advance is the owner can issue to a number of eligible users by performing encryption computation only once. But different users cannot collude with each other because their decryption keys are personalized.

Assigning reputation value

Reputation Value (RV) is the trust evaluated by a reputation center based on public feedback and extensive performance monitoring and reporting. (t) denotes the reputation value of entity e at time t. $(t) \in [0, 1]$, scaling from fully disreputable to fully reputable.

Data requisition

Multi-dimensional data access control based on individual trust evaluated by the data owner and/or public reputation evaluated by one or more RCs during the fulfillment of a cloud service. Taking two-dimensional control as an example, the data owner encrypts its data with a symmetric secret key $K0$ and security key K1. It respectively encrypts $K0$ with RC's public key pk_RC and $K1$ with a public attribute key pk_TL with regard to an individual trust attribute. It uploads the encrypted data and the above two encrypted partial keys to CSP. When a user requests accessing the data, the CSP checks if the user (i.e., a requestor) is in a greylist. If the check is negative, CSP forwards its request to RC and the data owner based on the owner's access policy. RC checks the user's reputation and generates a re-encryption key for the user to decrypt $K0$ if it is eligible based on the policy defined by the data owner Meanwhile, the owner issues a personalized secret key to the requestor to allow it to get $K1$ if its trust level satisfies the access policy. By achieving both $K0$ and $K1$, the requestor can access the encrypted data.

User blacklist

Cloud user that interacts with CSPs for consuming various services (e.g., data storage and data access). The user can be a data owner or a data requester. Users are not only human beings, but also CSPs. Each CSP has its own data center for data storage, a resource center that can offer various services and a management center that is responsible for service request and provision. In case that the requestor is not eligible to access the data (e.g., the reputation/trust level of the requestor is below a threshold), RC and/or the data owner will inform CSP to put it into a greylist.

6.RESULTS

In the implemented experiments, we focus on the developing an secure and trusted application, in which data owner can outsource data to cloud server after encryption. The implementation is carried out in JAVA 1.7 with Jsp and HTML as front end and MySQL server as backend.Due to large-scale data management, CSP‟s computational load should not be heavy from its efficiency point of view. Proposed scheme can release the re-encryption load of CSP. If the re- encryption has been conducted and the reputation of the data requestor remains, CSP doesn‟t need to repeat this operation. Thus, text files are used in the experimental study to reduce the load on encryption and key generation.In the proposed scheme, data access is controlled by the trust individually evaluated by the data owner, and/or public reputations valuated by one or more RCs. Note that other control attributes or reputation properties can be applied in the schema.

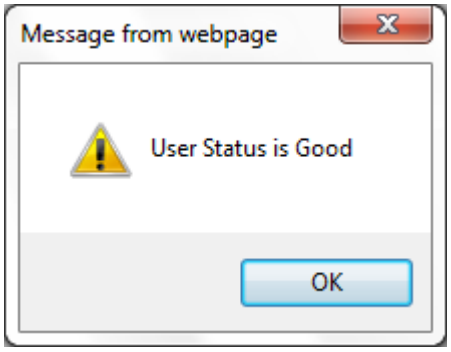

Fig6.1 Message from webpage

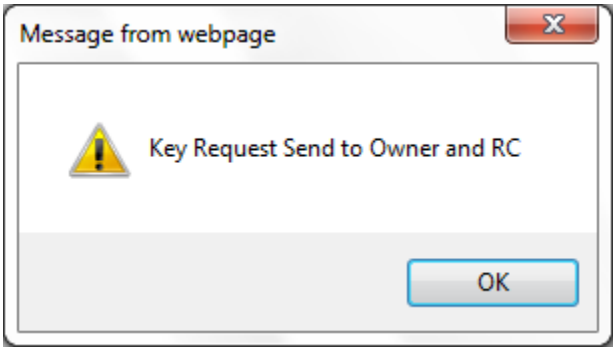

Fig6.2 Key request from RC

Fig6.3 User Re-decrypt file content

Fig6.4 File encryption by data owner

8.CONCLUSION

A cloud data access control is proposed based on trust and reputation. The scheme incorporates with a trust/reputation management framework for securing cloud computing by applying ABE, PRE and a reputation-based revocation mechanism. This scheme can flexibly support controlling cloud data access based on trust and reputation in order to support various access strategies and scenarios. Meanwhile, it also achieves low communication and computation costs. The cloud service can be automatically secured since the related cryptographic keys can be automatically generated.The security of the proposed scheme based on the security of ABE and PRE.This scheme realizes the access control of encrypted data where user's private keys are specified by a set of attributes and a party encrypting data can specify a policy over these attributes specifying which users are able to decrypt.Access control found to be a significant mechanism for protecting confidentiality and privacy in cloud computing, coming with suitable model that could reduce computation complexities at content owner as well as resolve the information leakage at the cloud server and outsiders, which need continuous attention and further enhancement makes the researches in this field to get more and more intensive.

9.REFERENCES

[1] R. Chow, et al., "Controlling data in the cloud: outsourcing computation without outsourcing control", Proc. of the ACM Workshop on Cloud Computing Security, 2009, pp. 85–90.

[2] S. Kamara, K. Lauter, "Cryptographic cloud storage", Proc. of Financial Cryptography and Data Security (FC), 2010, pp. 136–149.

[3] Q. Liu, C. Tan, J. Wu, G. Wang, "Efficient information retrieval for ranked queries in cost-

effective cloud environments", Proc. Of INFOCOM, 2012, pp. 2581-2585.

[4] M. Kallahalla, et al., "Plutus: Scalable secure file sharing on untrusted storage", Proc. of the USENIX Conference on File and Storage Technologies (FAST), 2003, pp. 29–42.

[5] E. Goh, H. Shacham, N. Modadugu, D. Boneh, "Sirius: Securing remote untrusted storage", Proc. of NDSS, 2003, pp. 131–145.

[6] J. Bethencourt, A. Sahai, B. Waters, "Ciphertext-policy attribute based encryption", Proc. of IEEE S&P, 2007, pp. 321–334.

[7] V. Goyal, O. Pandey, A. Sahai, B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data", Proc. of the 13th ACM CCS, 2006, pp. 89–98.

[8] S. Muller, S. Katzenbeisser, C. Eckert, "Distributed attribute-based encryption", Proc. of the 11th Annual Int. Conf. on Information Security and Cryptology, 2008, pp. 20–36.

[9] A. Sahai, B. Waters, "Fuzzy identity-based encryption", Proc. of 24th International Conference on the Theory and Application of Cryptographic Techniques, 2005, pp. 457–473.

[10] M. Pirretti, P. Traynor, P. McDaniel, B. Waters, "Secure attribute based systems", Journal of Computer Security, vol. 18, no. 5, pp. 799–837, 2010.

[11] M. Blaze, G. Bleumer, M. Strauss, "Divertible protocols and atomic proxy cryptography", Proc. of EUROCRYPT, 1998, pp. 127–144.