INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 4 ISSUE 1 (2018) PAGES 2757 - 2762
RECEIVED : 28.01.2018 PUBLISHED : 21.02.2018 Feb 21, 2018

RAAC: Robust and Auditable Access Control with Multiple Attribute Authorities for Public Cloud Storage

[1]M. Sujaritha, ME-CSE, Department of Computer Science, Vmkv engineering college, Salem.

[2]S. Senthil Kumar , Assistant professor, Department of Computer Science and Engineering, Vmkv engineering college, Salem.

[3]T. Narmadha, Assistant professor, Department of Computer Science and engineering, Vmkv engineering college, Salem.

ABSTRACT

Data access control is a challenging issue in public cloud storage systems. Ciphertext-Policy Attribute-Based Encryption (CP-ABE) has been maintain as a assuring technique to provide flexible, fine-grained and secure data access control for cloud storage with honest-but-interested cloud servers. However, in the existing CP-ABE schemes, the single attribute authority must execute the time-consuming user authority verification and secret key sharing, and hence it results in single-point performance congestion when a CP-ABE scheme is maintain in large-scale cloud storage system. Users may be fastening in the waiting queue for a long period to obtain their secret keys, thereby resulting in low-efficiency of the system. Although multi-authority access control schemes have been proposed, these schemes still cannot overcome the drawbacks of single-point congestion and low efficiency, due to the fact that each of the authorities still indivally manages a disjoint attribute set.In this project, I proposed a novel heterogeneous framework to remove the problem of single-point performance congestion and provide a more efficient access control scheme with an auditing mechanism. We implement Our framework employs multiple attribute authorities to share the load of user authority verification. And we use RC4 algorithm ,It requires a secure exchange of a shared key. Meanwhile, in our scheme, aCA (Central Authority) is introduced to generate secret keys for authority verified users. Unlike other multi-authority access control schemes, each of the authorities in our scheme manages the whole attribute set individually. To increase security, I also propose an auditing mechanism to detect which AA (Attribute Authority) has incorrectly or maliciously performed the authority verification procedure. Analysis shows that our system not only assurance the security requirements but also makes great performance increase on key generation.

1. INTRODUCTION

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. 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.

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 associated with driving ability . To deal with the verification of various attributes, the user may be required to be present to confirm them. Furthermore, the process to verify/assign attributes to users is usually difficult so that it normally employs administrators to manually handle the verification, as has mentioned, that the authenticity of registered data must be achieved by out-of-band (mostly manual) means. large system, there are always large numbers of users requesting secret keys. The inefficiency of the authority's service results in single-point performance bottleneck, which will cause system congestion such that users often cannot obtain their secret keys quickly, and have to wait in the system queue. This will significantly reduce the satisfaction of users experience to enjoy real-time services. On the other hand, if there is only one authority that issues secret keys for some particular attributes, and if the verification enforces users 'presence, it will bring about the other type of long service delay for users, since the authority maybe too far away from his/her home/workplace. As a result, single-point performance bottleneck problem affects the efficiency of secret key generation service and immensely degrades the utility of the existing schemes to conduct access control in large cloud storage systems. Furthermore, in multi-authority schemes, the same problem also exists due to the fact that multiple authorities separately maintain disjoint attribute subsets and issue secret keys associated with users' attributes within their own administration domain.

The 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, 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, is a threshold multi-authority CP-ABE access control scheme for public cloud storage, where multiple authorities jointly manage uniform attribute set.

2. RELATED WORK

Ciphertext-Policy Attribute-Based Encryption (CP-ABE) has so far been regarded as one of the most promising techniques for data access control in cloud storage systems. This technology offers users flexible, fine-grained and secure access control of outsourced data. It was first formulated by Goyal et al. in . Then the first CP-ABE scheme was proposed by Benthen court et al. in , but this scheme was proved secure only in the generic group model. Subsequently, some cryptographically stronger CP-ABE constructions were proposed, but these schemes imposed some restrictions that the original CP-ABE does not have. In , Waters proposed three efficient and practical CP-ABE schemes under stronger cryptographic assumptions as expressive as . To improve efficiency of this encryption technique, Emura et al. proposed a CP-ABE scheme with a constant ciphertext length. Unlike the above schemes which are only limited to express monotonic access structures, Obtrov sky et al. pro-posed a more expressive CP-ABE scheme which can support non-monotonic access structures.Two categories of CP-ABE schemes classified by the number of participating authorities in key distribution process. One category is the single-authority scheme, the other is multi-authority scheme. In single- authority schemes , only one authority is in- volved to manage the universal attribute set, generate and distribute secret keys for all users. In, the authors respectively proposed CP-ABE schemes with efficient attribute revocation capability for data outsourcing systems. proposed a Multi-message Ciphertext-Policy Attribute- Based Encryption(MCP-ABE) which encrypts multiple messages within one ciphertext so as to enforce flexible attribute-based access control on scalable media. The literatures took the efficiency issue into consideration, but they mainly considered the computation complexity inside the cryptography RC4 algorithms rather than interaction protocols between different entities in the real world, such as the procedure of user legitimacy verification. the first multi-authority scheme which allows multiple independent authorities to monitor attributes and distribute corresponding secret keys, but involves a central authority (CA). Subsequently, some multi-authority ABE schemes without CA have been proposed, such as . Since the first construction of CP-ABE, a great many multiauthority schemes have been conducted over CP-ABE. Mulleret al. proposed the first multi-authority CP-ABE scheme in which a user's secret key was issued by an arbitrary number of attribute authorities and a master authority. the authors proposed two efficient multi-authority CP-ABE schemes for data access control in cloud storage systems, where a central authority is only needed in system initialization phase. Based on the basic multi-authority architecture, some other literatures tried to address the user identity privacy issue , policy update , and the accountability to prevent key abusing. However, in above multi-authority schemes, multiple authorities separately manage disjoint attribute sets. That is to say, for each attribute, only one authority could issue secret keys associated with it. Therefore, in large-scale systems, the single-point performance bottleneck still exists in multi-authority schemes due to the property that each of the multiple authorities maintains only a disjoint subset of attributes.

3. LITERATURE SURVEY

An Attribute-Based Encryption (ABE) a promising technique for data access control in cloud storage is utilized in this project. Attribute-based encryption, especially for cipher text-policy attribute-based encryption, can fulfill the functionality of fine-grained access control in cloud storage systems. In the proposed scheme, any user can recover the outsourced data if and only if this user holds sufficient attribute secret keys with respect to the access policy and authorization key in regard to the outsourced data. Both the size of cipher text and the number of pairing operations in decryption are constant, which reduce the communication overhead and computation cost of the system. Residue Number Systems (RNS) are useful for distributing large dynamic range computations over small modular rings, which allows the speed up of computations. RNS algorithm will be used for the encryption and decryption process involved, which can be used to achieve performance improvement as the arithmetic involves smaller numbers and can be done in parallel. This ensures the system is very fast, most reliable and is executed with the least computational costs. the current day multi-authority attribute-based cloud systems are either insecure in attribute-level revocation or lack of efficiency in communication overhead and computation cost.As the cloud servers cannot be fully trusted and may attempt to access user data for illegal purpose, the concern about data security and privacy arises. One common method for alleviating this problem is to store data in encrypted form, which is more important for protecting sensitive user data. However, this brings forth new challenges: how to realize access control over encrypted data that is, sharing confidential data on cloud servers. Currently, role-based access control (RBAC) model is the most popular model used in enterprise systems; however, this model has severe security problems when applied to cloud systems. A classic RBAC model uses reference monitors running on data servers to implement authorization.

To achieve fine-grained and scalable data access control for BRs, we leverage attribute based encryption (ABE) techniques to encrypt all business file. We focus on the multiple data owner scenario, and divide the users in the BR system into multiple security domains that greatly reduces the key management complexity for owners and users. A high degree of data privacy is guaranteed simultaneously by exploiting multi-authority ABE. Automated Business solution resides in many stages of enhancement, which started from standalone application and moved into data centric web application. Globalizing business information makes application more efficient in level of usage. Due to reduce the investment cost and infrastructure maintenance pure web based services are converted into cloud based services. But cloud is dependent in third party investor, who are primary administer to have full control of business information. Due to lack of privacy in business information safety a huge requirement available and should be filled with anonymous data to prevent from any malicious thread. The solution is given for that problem in terms of cryptography. We adopt attribute-based encryption (ABE) as the main encryption primitive.

4. PROPOSED SYSTEM

We have been proposed a robust and efficient heterogeneous Framework with single CentralAuthority and multiple Attribute Authorities for public cloud storage. The heavy load of user legitimacy verification is shared by multiple AAs, each of which manages the universal Attribute set and is able to independently complete the user legitimacy verification, while CA is only responsible for computational tasks. On the best of our knowledge, this is the first work that proposes the heterogeneous access control framework to address the low efficiency and single-point performance bottleneck for cloud storage. I reconstruct the CP-ABE scheme. To fit our proposed framework and propose a robust and high –efficient access control scheme, meanwhile the scheme still preserves the fine granularity, flexibility and security features of CP-ABE. Proposed scheme includes an auditing mechanism that helps the system trace an AA's misbehavior on user's legitimacy verification. we implement RC4 algorithm this algorithm works in two-phases ,key setup and ciphering key setup . Attribute-based access control solution ensures that the end user will be authorized via an attribute secret key to the data on cloud server

5. RESULT ANALYSIS

The above mentioned, information in reality, the tedious procedure of user legitimacy verification is much more complicated than secret key generation. In our scheme, the load of legitimacy verification is shared among multiple AAs, while a much lighter computational task is assigned to the single CA. Thus, the efficiency of key distribution is improved. More Specifically, multiple AAs are standby for the legitimacy verification in the system. When there is a key request, an idle AA is selected by a scheduling algorithm to perform the verification and other AAs are standby to serve the subsequent user requests. the theoretical performance analysis as the following steps. Firstly, we model our system in queueing theory, and then we analyze the state probabilities to obtain the two important factors, the mean failure probability and the average waiting time for users. Finally, to show the significant performance improvement of our proposed RAAC, we compares it with single-AA system. It's important to note that, the comparison between RAAC and multi-authority systems is similar, since each authority independently manages.

CONCLUSION

This paper, we proposed a new framework, named RAAC, A detailed report algorithms to retrieve best keyword cover was presented. Best keyword cover query aims to recover spatial objects with respect to user's requirement. Algorithms are used to find answer to such query. a disjoint attribute subset. When a user requests secret keys with regard to one certain attribute subset, he/she has to go to the only and exclusive authority that issues secret keys with that attribute subset. 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 ofthe time-consuming legitimacy verification and standby for serving new arrivals of users' requests. We also proposed an auditing method to trace an attribute authority's potential misbehavior. We conducted detailed security and performance analysis to verify that our scheme is secure and efficient. The security analysis shows that our scheme could effectively resist to individual and colluded malicious users, as well as the honest-but-curious cloud servers. Besides, with the proposed auditing & tracing scheme, no AA could deny its misbehaved key distribution.

REFERENCE:

[1] P. Mell and T. Grance, "The NIST definition of cloudcomputing,"National Institute of Standards and Tech-nology Gaithersburg, 2011.

[2] Z. Fu, K. Ren, J. Shu, X. Sun, and F. Huang, "Enabling personalized search over encrypted outsourced data withefficiency improvement, "IEEE Transactions on Parallel& Distributed Systems, vol. 27, no. 9, pp. 2546–2559,2016.

[3] Z. Fu, X. Sun, S. Ji, and G. Xie, "Towards efficientcontent-aware search over encrypted outsourced data incloud," inin Proceedings of 2016 IEEE Conference onComputerCommunications (INFOCOM 2016). IEEE, 2016, pp. 1–9.

[4] K. Xue and P. Hong, "A dynamic secure group sharing framework in public cloud computing,"IEEE Transac-tions on Cloud Computing, vol. 2, no. 4, pp. 459–470,2014.

[5] 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.

[6] 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.

[7] J. Hur and D. K. Noh, “Attribute-based access control with efficient revocation in data outsourcing systems,” IEEE Transactions on Parallel and Distributed Systems, vol. 22, no. 7, pp. 1214–1221, 2011.

[8] J. Hong, K. Xue, W. Li, and Y. Xue, “TAFC: Time and attribute factors combined access control on time-sensitive data in public cloud,” inProceedings of 2015IEEE Global Communications Conference (GLOBECOM2015). IEEE, 2015, pp. 1–6.