Analysis and Implementations of Log Based Access Control with Multiple Attributes for Public Cloud Storage

Mr. Sanket G. Maraskolhe, Prof. M.S. Nimbarte
Department of Computer Engineering B.D.C.E Wardha

Abstract

This paper methodology helps solves the security issues in cloud IaaS (i.e. Infrastructure as a Service) which mainly includes use of cloud request processors and database servers. 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. Our framework employs multiple attribute authorities to share the load of user legitimacy verification. Meanwhile, in our scheme, a CA (Central Authority) is introduced to generate secret keys for legitimacy verified users. Unlike other multiauthority access control schemes, each of the authorities in our scheme manages the whole attribute set individually. To enhance security, we also propose an auditing mechanism to detect which AA (Attribute Authority) has incorrectly or maliciously performed the legitimacy verification procedure.

Keywords: *Cloud, IaaS, Security, CP-ABE, Access control*

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. 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 Ciphertext-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. 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 labeled with his/her own attributes.

Cloud basics

Cloud computing, or "the cloud", concentrates on expanding the viability of the imparted assets. Cloud assets are typically imparted by numerous clients as well as progressively reallocated for every interest and pay for every utilization premise.

This can work for dispensing assets to clients. For instance, a cloud machine that serves Indian clients amid Indian business hours with an application (e.g., email) may reallocate the same assets to serve China clients amid China's business hours with an alternate application (e.g., an application server). This methodology ought to build the utilization of processing power accordingly decreasing ecological harm which are needed for a mixed bag of capacities.

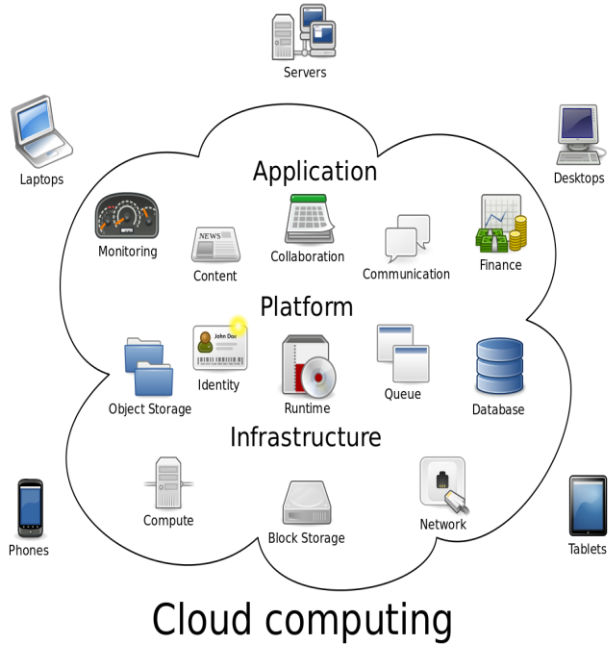

Fig : Basic Cloud structure

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 [1].

Then the first CP-ABE scheme was proposed by Benthencourt et al. in [2], but this scheme was proved secure only in the generic group model. Subsequently, some cryptographically stronger CP-ABE constructions [3] were proposed, but these schemes imposed some restrictions that the original CP-ABE does not have.

In [4], Waters proposed three efficient and practical CP-ABE schemes under stronger cryptographic assumptions as expressive as [4].

To improve efficiency of this encryption technique, Emura et al. [5] proposed a CP-ABE scheme with a constant ciphertext length. Unlike the above schemes which are only limited to express monotonic access structures, Obtrovsky et al. [5] proposed a more expressive CP-ABE scheme which can support non-monotonic access structures.

Recently, Hohenberger and Waters [6] proposed an online/offline ABE technique for CPABE which enables the user to do as much pre-computation as possible to save online computation. It’s a promising technique for resource-limited devices. In general, there are 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 involved to manage the universal attribute set, generate and distribute secret keys for all users.

In [7], the authors respectively proposed CP-ABE schemes with efficient attribute revocation capability for data outsourcing systems. Wu et al. [5] 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 [9] took the efficiency issue into consideration, but they mainly considered the computation complexity inside the cryptography algorithms rather than interaction protocols between different entities in the real world, such as the procedure of user legitimacy verification. To sum up, in single-authority schemes, the single-point performance bottleneck has not been widely addressed so far. To meet some scenarios where users' attributes come from multiple authorities, some multi-authority schemes have been proposed.

SYSTEM ARCHITECTURE

The proposed work is planned to be carried out in the following manner.

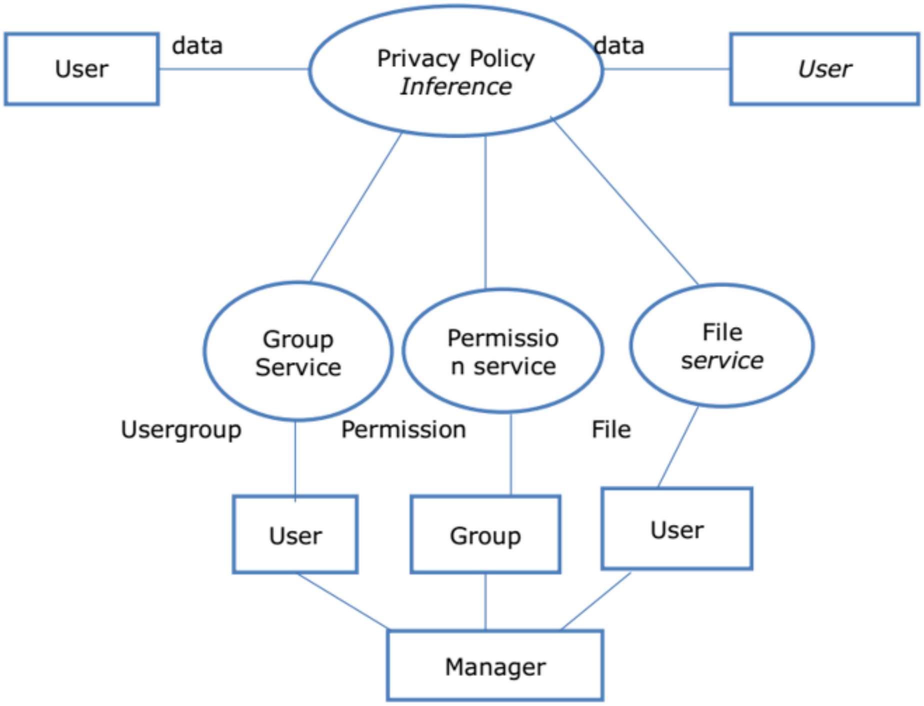

Fig 3.4: System Architecture

The system will work in a proper manner where the owner of the data will have the complete authority of accessing data and allotting the permissions to the other users in the organizations. In our scheme, we separate the procedure of user legitimacy verification from the secret key generation, and assign these two sub-procedures to two different kinds of authorities.

The owner will have full authority to create and assign the roles to the user only the owner will be able to access all the data and assign permissions and authorities to various users for their work.

The owner of the data will protect important classified information from unauthorized users by using the AES Encryption standard algorithm, and also by creating the group services and allotting permission for accessing any files.

Algorithm used : AES

- Key Expansions
  - For each round AES requires a separate 128-bit round key block plus one more. Initial Round
  - Add Round Key with a block of the round key, each byte of the state is combined using bitwise xor. 2) Rounds

  - Sub Bytes in this step each byte is replaced with another byte.
  - Shift Rows for a certain number of steps, the last three rows of the state are shifted cyclically.
  - Mix Columns a mixing operation which operates on the columns of the state, combining the four bytes in each column.
- Add Round Key
  - Final Round (no Mix Columns)
  - Sub Bytes
  - Shift Rows Add Round Key.

RESULT ANALYSIS

Experimental Result

The system in java. For testing we have hosted each entity on different machines. The cloud, CA, AA and TPA has core i-3 processor with 4 gb RAM. Client system has i3 processor with 2 gb ram. On every system java runtime environment JRE-1.7 is installed. For development i have used jdk 1.7 and IDE: Eclipse and Netbeans are used. For Database storage we have used mysql 5.3 database. For implementation of our system we have followed the business structure of users. Following is the system users structure with designation. Consider a scenario, if user wants to share data with manager and developer of department 1 and 2. Following attributes will be required to generate key.
Departmant1-manager Departmant1-Developer
Departmant1-manager Department2-Developer

Here the ABE algorithm is implemented and its performance is calculated. I have evaluated time required for token generation. The average time required for 10 users is 30 Mile Seconds. We are working on key distribution servers and key management. After complete system implementation I will evaluate the system performance with
- Upload download time for different files
- File share and key allotment times

File size in MB	Key Generation Time in Millisecond	Encryption time in Millisecond	Decryption time in Millisecond
1	219	5342	7949
2	213	8972	14321
3	214	14307	25379
4	229	20342	32572

Table. Performance Analysis

CONCLUSION

In this paper, a, to eliminate the single framework is proposed to 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. 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. Further performance analysis based on queuing theory showed the superiority of our scheme over the traditional CP-ABE based access control schemes for public cloud storage.

REFERENCES

[1] Kaiping Xue, Yingjie Xue, Jianan Hong," RAAC: Robust and Auditable Access Control with Multiple Attribute Authorities for Public Cloud Storage" IEEE ACCESS 2017

[2] 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.

[3] 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.

[4] 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.

[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," in Proceedings of 2015 IEEE Global Communications Conference (GLOBECOM 2015). IEEE, 2015, pp. 1–6.

[9] 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.

[10] A. Lewko and B. Waters, "Decentralizing attribute-based encryption," in Advances in Cryptology–EUROCRYPT 2011. Springer, 2011, pp. 568–588

[11] K. Yang, X. Jia, K. Ren, and B. Zhang, "DAC-MACS: Effective data access control for multi-authority cloud storage systems," in Proceedings of 2013 IEEE Conference on Computer Communications (INFOCOM 2013). IEEE, 2013, pp. 2895–2903.

[12] J. Chen and H. Ma, "Efficient decentralized attribute based access control for cloud storage with user revocation," in Proceedings of 2014 IEEE International Conference on Communications (ICC 2014). IEEE, 2014, pp. 3782–3787.

[13] M. Chase and S. S. Chow, "Improving privacy and security in multi-authority attribute-based encryption," in Proceedings of the 16th ACM conference on Computer and Communications Security (CCS 2009). ACM, 2009, pp. 121–130.

[14] M. Lippert, E. G. Karatsiolis, A. Wiesmaier, and J. A. Buchmann, "Directory based registration in public key infrastructures." in Proceedings of the 4th International Workshop for Applied PKI (IWAP 2005), 2005, pp. 17– 32.

[15] 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.

[16] S. Chokhani, W. Ford, R. Sabett, C. Merrill, and S. Wu, "Internet x.509 public key infrastructure certificate policy and certification practices framework," IETF RFC, RFC3647, 2003.

[17] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute based encryption for fine-grained access control of encrypted data," in Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS 2006). ACM, 2006, pp. 89–98.

[18] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext policy attribute-based encryption," in Proceedings of IEEE Symposium on Security and Privacy (S&P 2007). IEEE, 2007, pp. 321–334.

[19] V. Goyal, A. Jain, O. Pandey, and A. Sahai, "Bounded ciphertext policy attribute based encryption," in Automata, languages and programming. Springer, 2008, pp. 579–591.

[20] L. Cheung and C. Newport, "Provably secure ciphertext policy abe," in Proceedings of the 14th ACM Conference on Computer and Communications Security (CCS 2007). ACM, 2007, pp. 456–465