International Journal of Technical Innovation in Modern Engineering & Science (IJTIMES)
Impact Factor: 5.22 (SJIF-2017), e-ISSN: 2455-2585
Volume 4, Issue 10, October-2018

HEALTHY MONITORING OF ADMISSIONS CONTROL WITH MULTI-LEVEL AUTHORITY FOR PUBLIC CLOUD STORAGE-ENVIRONMENT

QAMAR AHMED[1] DR. JANGALA SASI KIRAN[2]

PG Scholar, Dept of CSE[1]
Professor, Dept of CSE & Principal[2]
Farah Institute of Technology, Hyderabad, R.R. District, Telangana State, India – 501503

ABSTRACT: Control of access to data is a difficult problem in public cloud storage systems. Cryptographic encryption (CP-ABE) was adopted as a promising way to provide control over access to flexible, reliable and secure cloud storage data with honest but colorful cloud servers. However, in the current CP-ABE schemes, the only attribute of the authority must be carried out to verify the legitimacy of the user and the timing of key distribution, which leads to suffocation and a point when the program is adopted CP-ABE in - system storage, cloud users can be caught in the queue waiting period Long time to get their keys, resulting in low system efficiency. Although motion control schemes propose multiple wills, these schemes can not yet overcome single-point bottlenecks and decrease their efficiency, due to the fact that each of the authorities continues to independently manage a set of separate attributes. In this document, we propose a new heterogeneous framework to eliminate the one-point performance bottleneck problem and provide a more efficient access control scheme with an audit mechanism. Our framework employs multiple authority authorities to share and verify the user's legitimacy. Meanwhile, in our scheme, CA (Central Authority) is provided to generate secret keys for legitimate users to verify. Unlike other multi-center access control systems, each authority in our system manages the complete set of attributes individually. To improve security, we also suggest an audit mechanism to detect any AA (attribute authority) that has incorrectly or maliciously verified the legitimacy. The analysis shows that our system not only guarantees the security requirements but also significantly improves the performance in the generation of keys.

Keywords: Cloud storage, Access control, Auditing, CPABE.

I. INTRODUCTION

Inspired by heterogeneous architecture with single CA and multiple RAs, we propose a Strong access control scheme (SAAC) for general cloud storage to enhance performance while maintaining the flexibility and precise characteristics of the AVE. In our plan, we separate the procedures for verifying the user's legitimacy from the secret key generation, and assigning these sub-processes to two different types of authorities. There are many authorities (powers specific attributes, AA), each of which is responsible for a full set of features and can perform independent verification of the user's legitimacy [1]. At the same time, there is one reliable global authority (called Central Authority, California) responsible for generating and distributing secret keys. Before you generate and distribute secret keys, one AAs is selected to validate the user attributes and then creates an intermediary key to send to the CA. CA creates the user's secret key based on the intermediary key received, without further verification. In this way, many AAs can work in parallel to share the burden of long-term forensic verification and reserve status to eliminate the single-point bottleneck in performance. At the same time, the AA selected is not responsible for generating final passwords for users. Instead, it creates intermediate keys associated with user attributes that are implicitly associated with their own identity, and send them to the certification authority. With the help of intermediate keys, CA can not only create secret keys for legitimate users, but also follow an AA error or malicious behavior to improve security. To deal with the performance of a single point, there is the main distribution in the current charts, and we suggest a solid and inefficient framework for one CA (central power) and AA for public cloud storage. The heavy burden of validating the user's legitimacy is shared by many AAs, each of which runs a set of universal features and can independently complete the validation of the user's legitimacy, while the CA is only responsible for the computational tasks. As far as we know, this is the first function proposed by the heterogeneous access control framework to address low efficiency and one bottleneck storage bottleneck crisis [2]. We are rebuilding the CP-ABE plan to adapt it to our proposed framework and propose a strong and effective access control scheme. The system still retains the uniqueness, flexibility and security features of the CPABE. Our plan includes an audit mechanism that helps the system to track AA misconduct in verifying the legitimacy of the user.

2. IMPLEMENTATION

System Framework: We suggest a hierarchical framework with a CA and multiple AAs to eliminate the bottleneck problem of single-point performance and improve system efficiency. In the proposed SAAC scheme, the key generation procedure is

divided into two subprojects: 1) user validation, 2) generation and generation of the secret key [3]. Our plan consists of five stages, namely System Configuration, Encryption, Key Generation, Decryption, Audit and Follow-up. Our system design model includes five entities: central authority (CA), multiple attribute authorities (AA), many data owners (owners), many data consumers (users), cloud service provider with multiple servers in Cloud.

The Central Authority: Central authority is responsible for the entire system. It is responsible for building the system by configuring the system parameters and generating a generic key for each feature set of general attributes. In the system initialization phase, each user is assigned a unique unit and each authority has a unique help attribute. For a user password request, CA is responsible for creating user secret keys based on the recipient's intermediate key associated with the user's legitimate attributes verified by AA. As an administrator of the entire system, CA has the ability to track any AAIncorrectly or maliciously verifies the user and gives them groups of illegal attributes, creating the secret key associated with the user's set of attributes without further verification. The secret key is created by using the Secure Sender key safely from AA.

Attribute Authorities: Multiple AA to eliminate the bottleneck problem in the performance of single point and improve system efficiency. The Referral Authorities (AA) are responsible for verifying the legitimacy of the user and generating intermediate keys for users whose legitimacy is verified. Unlike most existing multi-power schemes where each AA runs a set of separate attributes respectively, our proposed scheme involves several sharing parties responsible for validating the user's legitimacy and each AA can perform this process for any user independently [4]. When AA is selected, it will verify the legitimate attributes of the users through manual work protocols or authentication, and will create an intermediary key associated with the verified features of their legitimacy. The middle key is a new concept to help CA create keys.

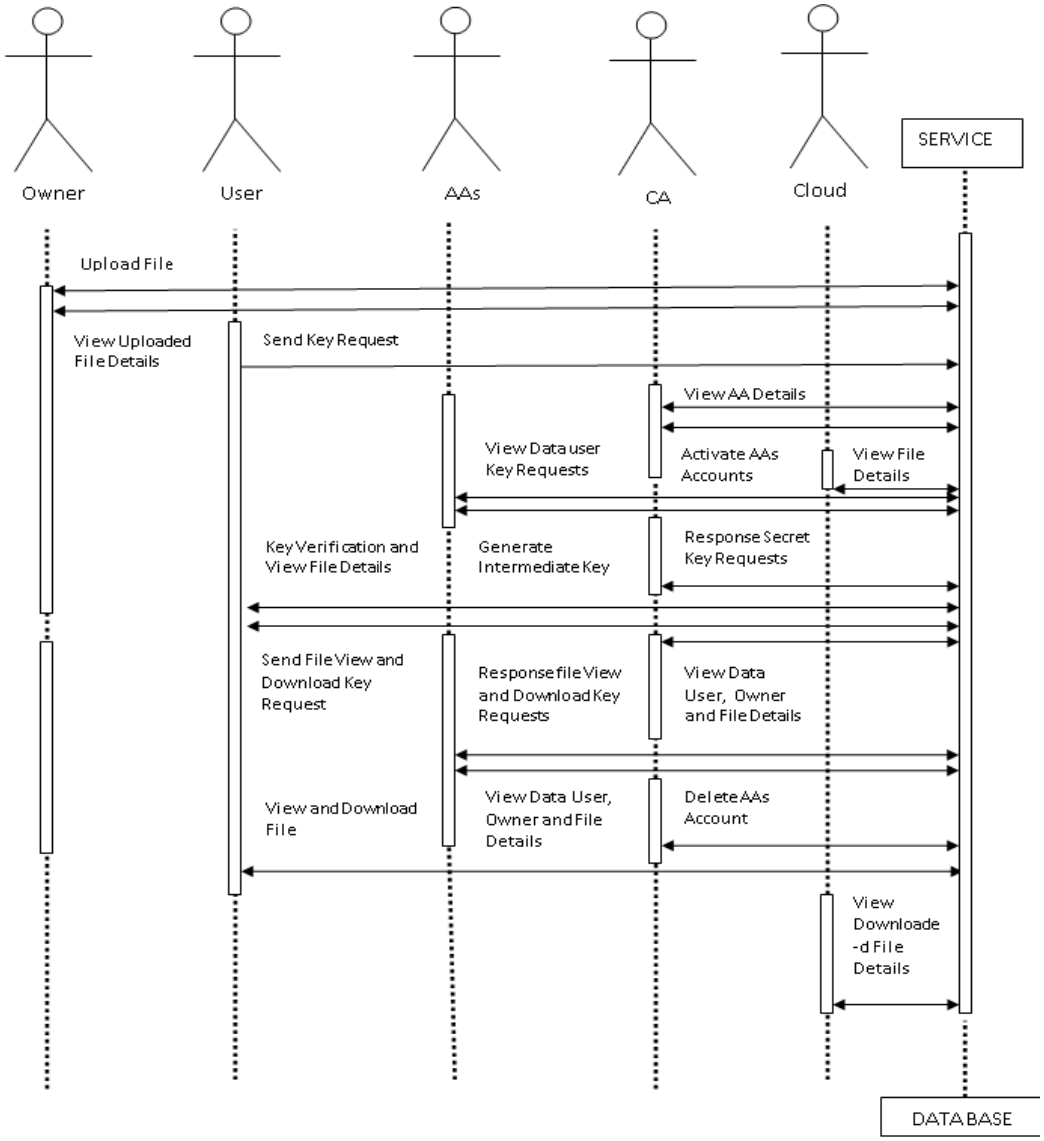

Fig 1: Workflow Diagram

3. RELATED SURVEY

Enabling personalized search over encrypted outsourced data with efficiency improvement: In cloud computing, the external data search encryption system is an active search area. However, most of the encrypted search work through external cloud data follows a "one size fits all" model and ignores the intention of dedicated search. In addition, most of them only support accurate searches of keywords, which greatly affects the user's data and user experience [5]. How to design a search encryption system that supports personalized search and improves the user's search experience is still a very difficult task. In this document, for the first time, we examine and solve the problem of multilanguage search in a personal way through encrypted data (PRSE) while maintaining privacy in cloud computing. With the help of WordNet's Ontology model, we created a model of user interest for the individual user by analyzing the user's search history and adopting a registration mechanism to express the user's interest intelligently.

Towards efficient content-aware search over encrypted outsourced data in cloud: With the increasing adoption of cloud computing, a growing number of users outsource their datasets into cloud. The datasets usually are encrypted before outsourcing to preserve the privacy. However, the common practice of encryption makes the effective utilization difficult, for example, search the given keywords in the encrypted datasets. Many schemes are proposed to make encrypted data searchable based on keywords. However, keyword-based search schemes ignore the semantic representation information of user's retrieval, and cannot completely meet with users search intention. Therefore, how to design a content-based search scheme and make semantic search more effective and context-aware is a difficult challenge. In this paper, we proposed an innovative semantic search scheme based on the concept hierarchy and the semantic relationship between concepts in the encrypted datasets. More specifically, our scheme first indexes the documents and builds trapdoor based on the concept hierarchy. To further improve the search efficiency, we utilize a tree-based index structure to organize all the document index vectors.

A dynamic secure group sharing framework in public cloud computing: With the popularity of sharing data in the public cloud computing group, privacy and security have become two large common data sets. The cloud provider cannot be treated as a trusted third party due to its semi-reliable nature, and therefore traditional security models cannot be integrated directly into peer-based group exchange frames [6]. In this document, we propose a new framework for the exchange of public cloud insurance groups, which can effectively benefit from servers in the cloud, but does not have the exposure of confidential data to the attackers and the cloud provider. It combines the framework between the agent and the enhanced TGDH signature and re-agent encryption in the protocol. Through the signing agent technology application, the group leader can grant the privilege of effectively managing the group of one or more of the chosen members of the group.

4. CONCLUSION

We proposed a new framework, called SAAC, to eliminate the bottleneck in the performance of a point of the current CP-ABE schemes. By redefining CPABE encryption technology in our new framework, our proposed plan provides strong, effective, high-quality control with global CA / multi-AA cloud storage. Our plan uses many AAs to share the long burden of legitimacy verification and wait to meet the new demands of users. We have also proposed an audit method to track the possible misconduct of the attribute authority. We perform a detailed security and performance analysis to verify that our scheme is safe and effective [7]. The security analysis shows that our plan can effectively withstand collusion and individual malicious users, as well as honest but strange servers in the cloud. In addition, with the proposed audit and monitoring plan, no anonymous company can deny its distribution of the incorrect code. Additional performance analysis based on queuing theory showed that we were superior to traditional CP-ABE access control schemes for public storage in the cloud [8].

5. REFERENCES

[1] Z. Fu, X. Sun, S. Ji, and G. Xin, "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.

[2] 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.

[3] 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.

[4] J. Hong, K. Xue, W. Li, and Y. Xue, "TAFC: Time and attribute factors combined access control on timesensitive data in public cloud," in Proceedings of 2015 IEEE Global Communications Conference (GLOBECOM 2015). IEEE, 2015, pp. 1–6.

[5] 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.

[6] 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.

[7] 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.
[8] 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.

AUTHOR PROFILE



Mr. QAMAR AHMED is a PG Scholar, Dept of CSE, Farah Institute of Technology, Hyderabad, R.R. District, Telangana State – 501503. His Research includes Cloud Computing, Security & IoT.



Dr. J. Sasi Kiran Graduated in B.Tech [EIE] from JNTU Hyd. He received Masters Degree in M.Tech Computers and Communications from Bharath University, Chennai
And M.Tech CSE from JNTUH Hyderabad. He received Ph.D degree in Computer Science from University of Mysore, Mysore. At Present he is working as Professor in CSE and Principal in Farah Institute of Technology, Chevella, R.R. Dist Telangana State, India. His research interests include Image Processing, Cloud Computing and Network Security. He has published several research papers till now in various National, International Conferences, Proceedings and Journals.