IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Vol.-6, Issue-5, May 2018 E-ISSN: 2347-2693

Privacy Preserving Public Auditing with Data Storage Security in Cloud Computing : An Overview

R. Manimegalai[1*], .A. Priyadharshini[2]

[1] Department of Computer Science,Rathinam College of Arts and Science,Coimbatore-21
[2] Department of Computer Science,Rathinam College of Arts and Science,Coimbatore-21

[*]*Corresponding Author: mmegalai217@gmail.com*

Available online at: www.ijcseonline.org

Accepted: 17May/2018, Published: 31/May/2018

Abstract— Cloud computing is an Internet-based computing pattern through which shared resources are provided to devices on demand. In order to provide safe and secure operation propose a hierarchical attribute based access control scheme by extending cipher text-policy attribute-based encryption (CP-ABE) with a hierarchical structure of multi authorities and exploiting attribute-based signature (ABS). The proposed scheme not only achieves scalability due to its hierarchical structure, but also inherits fine-grained access control with authentication in supporting write privilege on outsourced data in cloud computing. In addition, we decouple the task of policy management from security enforcement by using the extensible access control markup language (XACML) framework. Extensive analysis shows that our scheme is both efficient and scalable in dealing with access control for out- sourced data in cloud computing.

Keywords—CP-ABE,ABS,XACML

I. INTRODUCTION

Cloud computing consists of three distinct types of computing services delivered remotely to clients via the internet[1]. Clients pay a fee to providers for service, to access a systems that deliver software as a service, platforms as a service and infrastructure as a service to subscribers. Clients who need the cloud services have advantage for their business needs. Cloud computing is an Internet-based computing pattern through which shared resources are provided to devices on demand[1]. It's an emerging but promising paradigm to integrating mobile devices into cloud computing, and the integration performs in the cloud based hierarchical multi-user data-shared environment[1]. With integrating into cloud computing, security issues such as data confidentiality and user authority may arise in the mobile cloud computing system, and it is concerned as the main constraints to the developments of mobile cloud computing[1].

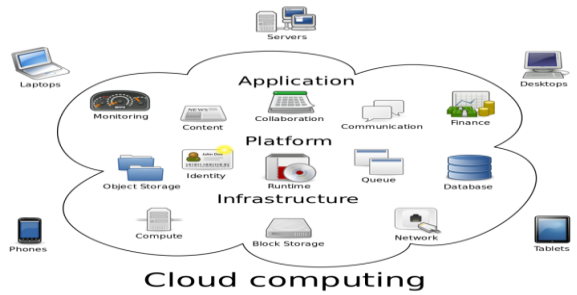


Fig.1 :Cloud Computing

II. EXISTING SYSTEM

Assuming that a company develops a weather monitor application which aims to share real-time weather information such as temperature, humidity, pictures, and precise location information and so on to other users of the application. And the application utilizes the user-cloud-user model instead of peer to-peer model so that the users can get classified and demanded information. Another feature of the application is that the users are divided into different hierarchies, depending on which users can get different sensing data, and users with higher privilege level can, of course, get access to more specific and more frequently updated information. In order to meet what the application requires, security issues of the whole system should not be ignored, among all security issues the most important two security issues in such model can be divided into two parts: authority of application users and the confidentiality of sensing data. Those issues can be solved by providing methods of access control. Attribute Based Encryption (ABE) is a recent cryptographic primitive which has been used for access control

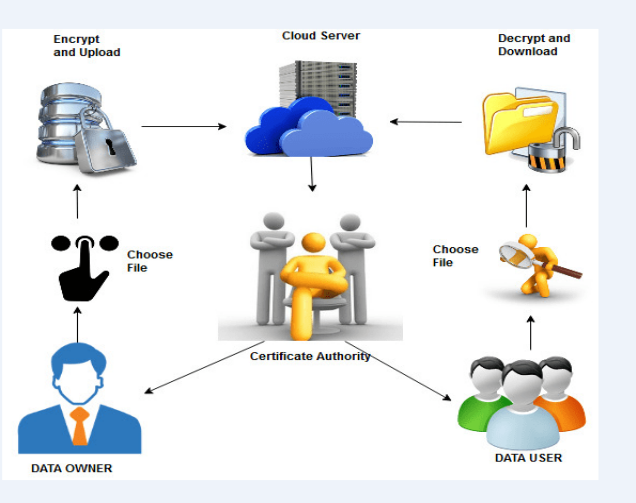
III. DEFINITION OF THE PROBLEM

- Encryptor cannot decide who can decrypt the encrypted data.
- It can only choose descriptive attributes for the data, and has no choice but to trust the key issuer.

- ABE is not naturally suitable to certain applications

IV. OUR CONTRIBUTIONS

CP-ABE (Ciphertext-Policy Attribute-Based Encryption) with hidden access control policy enables data owners to share their encrypted data using cloud storage with authorized users while keeping the access control policies blinded[2]. However, a mechanism to prevent users from achieving successive access to a data owner's certain number of data objects, which present a conflict of interest or whose combination thereof is sensitive, has yet to be studied[2]. In this paper, we analyze the underlying relations among these particular data objects, introduce the concept of the sensitive data set constraint, and propose a CP-ABE access control scheme with hidden attributes for the sensitive data set constraint[2]. This scheme incorporates extensible, partially hidden constraint policy[2]. In our scheme, due to the separation of duty principle, the duties of enforcing the access control policy and the constraint policy are divided into two independent entities to enhance security[2]. The hidden constraint policy provides flexibility in that the data owner can partially change the sensitive data set constraint structure after the system has been set up[2]. With this extension, we achieve a scheme with multiple, independent attribute authorities, in which revocation of specific users (e.g. with IDi) from the system with all of their attributes is possible without updates of attribute public and secret keys (neither periodically, nor after revocation event)[3]. We avoid re-encryption of all cipher texts the 2 access structures of which contain a subset of attributes of the revoked user[3]. The revocation right can be given directly to the encryptor, just like the right to define the access structure which fits to the cloud computing scenario[3].



V. PROPOSED SYSTEM

In this system, propose a hierarchical attribute-set-based encryption (HASBE) scheme for access control in cloud computing. HASBE extends the cipher text-policy attribute- set-based encryption (CP-ASBE, or ASBE for short) scheme with a hierarchical structure of system users So as to achieve scalable, flexible and fine-grained access control. The property of this scheme is more applicable to the environment of enterprises sharing data in the cloud. We integrate XACML framework based on the proposed scheme, which helps the scheme scale better with more data and more policies, to achieve high performance.

VI. ADVANTAGES

- Low initial capital investment
- Shorter start-up time for new services
- Lower maintenance and operation costs
- Higher utilization through virtualization
- Easier disaster recovery

VII. CONCLUSION

In this paper conclude that scheme with hierarchical structure has to achieve scalable, flexible and fine-grained access control and also the environment of enterprises sharing data in the cloud. By using the XACML framework helps the scheme scale better with more data and more policies to achieve low costs, high utilization, High Performance.

REFERENCES

[1] https://apprenda.com/library/cloud/introduction-to-cloud-computing/

[2] https://www.hindawi.com/journals/scn/2017/2713595/

[3] https://eprint.iacr.org/2014/612.pdf

[4] R. Nallakumar, N. Sengottaiyan, S. Nithya, "A Survey of Task Scheduling Methods in Cloud Computing", International Journal of Computer Sciences and Engineering, Vol.2, Issue.10, pp.9-13, 2014. https://www.hindawi.com/journals/scn/2017/2713595/

[5] S. Roschke, et aI., "Intrusion Detection in the Cloud," presented at the Eighth IEEE International Conference on Dependable, AutonomIc and Secure Computing, Chengdu, China, 2009.

[6] B.P. Rimal, Choi Eunmi, I. Lumb, "A Taxonomy and Survey of Cloud Computing Systems", Intl. Joint Conference on INC, IMS and IDC, 2009, pp. 44-51,Seoul, Aug, 2009. DOI: 10.1109/NCM.2009.218

[7] B. R. Kandukuri, R. Paturi V, A. Rakshit, "Cloud Security Issues", In Proceedings of IEEE International Conference on Services Computing, pp. 517-520, 2009. K. Elissa, "Title of paper if known," unpublished.

[8] Cloud Computing. Wikipdia. Available at http://en.wikipedia.org/wiki/Cloud_computing

[9] Cong Wang, Qian Wang, KuiRen, and Wenjing Lou, "Ensuring Data Storage Security in Cloud Computing," 17th International workshop on Quality of Service, USA, pp.1-9, July 13-15, 2009, ISBN: 978-1-4244-3875-4

[10] C. Weinhardt, A. Anandasivam, B. Blau, and J. Stosser."Business Models in the Service World."IT Professional, vol. 11, pp. 28-33, 2009.

[11] B. Patel, S. Patel, "Various Load Balancing Algorithms in cloud computing", International Journal of Advanced Research in Computer Science and Software Engineering, Vol¬.1, Issue.¬2 pp.23-29, 2015.

Authors Profile

Mrs. R.Manimegalai is an Assistant Professor in Department of Computer Science, Rathinam College of Arts and Science,Eachanari,Coimbatore. She is having more than 7 years of Teaching experience and 2 years of Research experience. His core area of research is Data Mining, Image Processing, Soft Computing.

Mrs. A.Priyadharshini is an Assistant Professor in Department of Computer Science, Rathinam College of Arts and Science,Eachanari,Coimbatore. She is having more than 2 years of Teaching experience and 2 years of Research experience. His core area of research is Network Security.

