International Journal of Global Engineering (IJGE) E- ISSN: 2456-3099

VOL 3 ISSUE 1 (2018) PAGES 17 - 22

Received: 15/07/2018. Published: 08/08/2018

ENFORCING ROLE-BASED ACCESS MANAGEMENT FOR SECURE KNOWLEDGE STORAGE WITHIN THE CLOUD

D.B.Shanmugam[1], S.Divya[2], K.Dhakshnamurthy[3] , S.Munusamy[4]

[1]Associate Professor, Department of MCA, Sri Balaji Chockalingam Engineering College , Arni

[1]dbshanmugam@gmail.com

[2]M.Phil, Research Scholar, Dr.M.G.R.Chockalingam Arts College, Arni.

[2] sdhivyaa93@gmail.com

[3]Assistant Professor, Department of BCA, King Nandhivarman College of Arts & science, Thellar

[3]kdmurthyarni@gmail.com

[4]Assistant Professor, Department of MCA, Sri Balaji Chockalingam Engineering College , Arni

[4]muns.samy@gmail.com

ABSTRACT

Cloud computing has attracted a lot of attention in recent times due to its ability to deliver resources corresponding to computing and storage to users on demand in an exceedingly efficient manner. thanks to the continual growth within the quantity of digital data that must be hold on, there's a transparent incentive for the service suppliers to explore outsourcing of users' information to the cloud. probably there may well be many advantages to storing information within the cloud. The cloud will give a scalable superior storage design, and might facilitate United States to considerably scale back the price of maintenance of individual services.In recent times, there has been increasing interest in storing data securely in the cloud environment. To provide owners of data stored in the cloud with flexible control over access to their data by other users, we propose a role-based encryption (RBE) scheme for secure cloud storage. Our scheme allows the owner of data to store it in an encrypted form in the cloud and to grant access to that data for users with specific roles. The scheme specifies a set of roles to which the users are assigned, with each role having a set of permissions. The data owner can encrypt the data and store it in the cloud in such a way that only users with specific roles can decrypt the data. Anyone else, including the cloud providers themselves, will not be able to decrypt the data. We describe such an RBE scheme using a broadcast encryption algorithm. The paper describes the security analysis of the proposed scheme and gives proofs showing that the proposed scheme is secure against attacks. We also analyse the efficiency and performance of our scheme and show that it has superior characteristics compared with other previously published schemes.

1. INTRODUCTION

Nowadays, the word "Cloud" is becoming increasingly popular in IT. It is very common to hear about Cloud Drive, Cloud Database, Cloud Server, Cloud Security and Cloud Ecosystem. Apparently, the "Cloud" here does not refer to a natural phenomenon. The meaning is short for "Cloud Computing" which is a new aggregated computing technology that is spreading rapidly from small area researching to large-

International Journal of Global Engineering (IJGE) E- ISSN: 2456-3099
VOL 3 ISSUE 1 (2018) PAGES 17 - 22
Received: 15/07/2018. Published: 08/08/2018

scale developing and utilizing. Obviously, the popularization of "Cloud" is not a coincidence but a demand from Internet market. In addition, it is going to be the foundation of Internet in the next generation and initiate the new pattern of Internet services.Thus, in order to catch the step of evolving "Cloud", it is necessary to have basic understanding in the concept of Cloud Computing. Nevertheless, the idea of Cloud Computing is still quite elusive and blurry for non-IT specialists. So, what exactly the Cloud Computing is? What are the key points to build a successful Cloud? What are the benefits and usage in our life and work? Are there any security issues with it and how can we solve them? Gradually, the mysteries of Cloud Computing will be uncovered in the thesis and presented in a methodic structure.The following chapters will focus on analyzing the essence of Cloud Computing, explaining the implementation of cloud, introducing the typical utilization of it, finally illustrating the primary security issues and certain methods or schemes to solve them. Cloud is not sets of hardware, software or services. It is the combination and integration of massive information technologies. In addition, the size of Cloud is growing since new developing technologies keep joining the group. Besides, the National Institute of Standards and Technology of U.S. Department of Commerce defined that "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources.

2. RELATED WORK

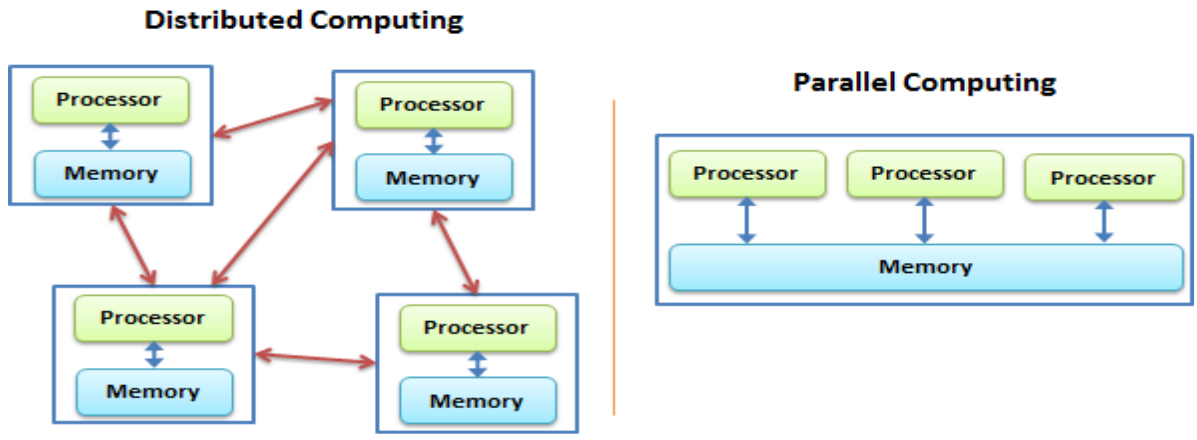

Figure 1. Distributed Computing and Parallel Computing

Moreover, Network Attached Storage (NAS) Technologies connect storage devices with a group of computers via standard network topology. NAS fulfills the need for rapidly increasing storage volumes, providing sufficient storage space for the connected hosts. Meanwhile, another Network Storage Technology is Storage Area Network (SAN), which utilizes Fiber Channel (FC) connects to a group of computers without standard topology, usually used in high volume storage environment. technology, from mainframe computer to client-server mode. Until now, many famous IT companies have utilized and deployed the research and development of Cloud Computing due to its potential of commercial value and revolutionary technology. Private cloud can be established by a company or a cloud service provider. Based on this hosted management, cloud service providers such as Sun and IBM are supposed to install, configure

International Journal of Global Engineering (IJGE) E- ISSN: 2456-3099
VOL 3 ISSUE 1 (2018) PAGES 17 - 22
Received: 15/07/2018. Published: 08/08/2018

and maintain the infrastructure to support the private cloud holding the business datacenter owned by a certain company. In this way, the usage of cloud resources are strongly controlled by the company, at the same time, the professional knowledge of building and running this environment can be acquired.

3. PROPOSED SYSTEM

Consumers can receive perfect services from computer infrastructure, which are called infrastructure as a service. The service based on Internet is part of IaaS such as storage and database. The best example to describe IaaS is there are hundreds to thousands Amazon EC2 virtual machines that process TB level documents in 36 hours in The New York Times. Without EC2, it will take days to months for New York Time to process those data.Usually, there are three ways to apply IaaS: public cloud, private cloud and hybrid cloud that have been mentioned before. Amazon EC2 utilizes public server pools in infrastructure. More private services will use a set of public or private server pools in a company's datacenter. If the datacenter environment of the company is used to make software development, in this way, the public, private and hybrid cloud are all available. Besides, the cost of EC2 used as temporary extensive resources is quite low and shortens the development or testing cycle. However, there are vulnerabilities in IaaS. For example, if a service provider offers a shared infrastructure, that is to say, some components or function like CPU cache and GPU, are not completely isolated to system users, this will lead to a consequence that when an attacker succeeds to breach in the system, all of the servers are exposed to him or her, even with hypervisor, some of the client operation systems can gain access to infrastructure that are not controllable. Therefore, a power partition and defense strategy has to be assigned. Some examples will be given for a better understanding of PaaS. The Internet giant Amazon is famous for providing the EC site to individuals. It rents out the system platform which originally built for themselves. Users can choose the operating system and middleware freely through this service that offers hardware and software platform. From 2006, Amazon EC pushed this service into market use.

Figure 2 Google Cloud Platform

4. ANALYSIS

International Journal of Global Engineering (IJGE) E- ISSN: 2456-3099
VOL 3 ISSUE 1 (2018) PAGES 17 - 22
Received: 15/07/2018. Published: 08/08/2018

The concept of BE was introduced by Fiat and Naor . In BE schemes, a broadcaster encrypts messages and transmits them to a group of users who are listening in a broadcast channel. Then they use their private keys to decrypt the transmissions. While encrypting the messages, the broadcaster can choose the set of users that is allowed to decrypt the messages. Following this original scheme, many other BE schemes have been proposed . These schemes require public parameters for every user, and every time a user wants to join or leave the system, the public parameters need to be updated. We note that these two polynomials remain the same in the decryption of two different messages if the identities of roles and users are not changed. Therefore, in the implementation, the user can keep these values as auxiliary information to help with decrypting messages. These values only need to be re-calculated when the predecessor roles of the specific role are changed or the permission is revoked from another user in the same role.

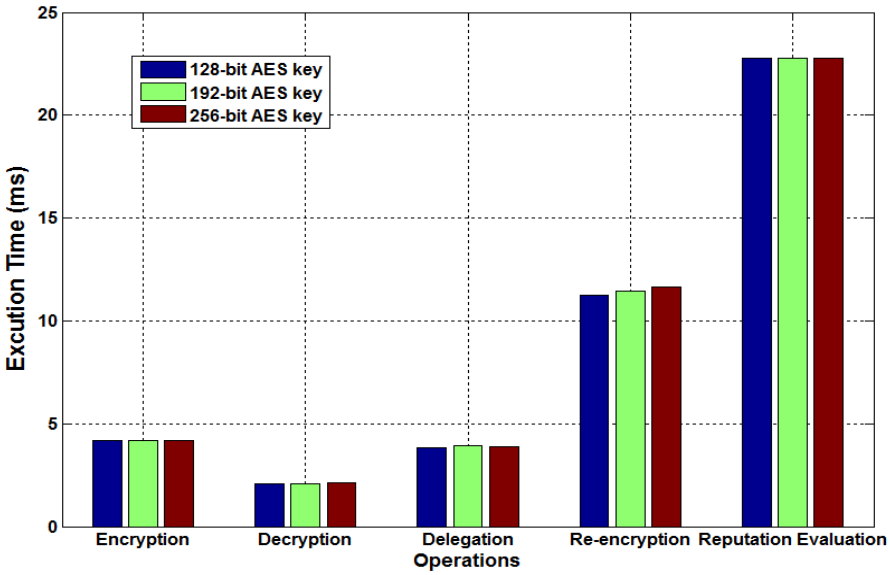

Fig.3. Execution time of Scheme Operations

One improvement we have in our scheme for PRE is to skip the re-encryption key generation process at RC, if the key of the user has been already generated before and the user's information remains unchanged. Fig.5.4 shows the request processing time at RC, including data policy checking reputation evaluation and re-encryption key generation, in two cases. In the first case, the RC generates a re-encryption key for every request if the requester satisfies the policy and reputation level. In the second case, RC directly fetches the already generated re-encryption key from the granted user's record. As shown in Fig.5.4, the higher the number of requests from the users who have the records at RC, the more efficiency improvement our scheme can achieve. In practice, the user could access cloud services multiple times. Thus, utilizing the existing re-encryption keys greatly helps the RC to improve its efficiency and capacity. In our performance test, we employed one RC for reputation management, and proved that the performance is negligibly affected by the number of RCs. As shown in Table XIII, Mechanism 1 and Mechanism 2 enable only one of the two access control methods which are reputation based or Individual TL based method.

International Journal of Global Engineering (IJGE) E- ISSN: 2456-3099
VOL 3 ISSUE 1 (2018) PAGES 17 - 22
Received: 15/07/2018. Published: 08/08/2018

CONCLUSION

In this thesis, we have considered security requirements for storage of information in the cloud and proposed a hybrid RBE scheme that combines role-based access control with encryption to address them. We have constructed a specific RBE scheme using the BE scheme described. We have conducted security analysis of our scheme and have given proofs to show that our scheme is secure against adaptive attack and revocable- ID attack. We have discussed the performance and efficiency of our scheme and have compared it with other previously related work. We have shown that our scheme has several superior characteristics such as constant size ciphertext and decryption key, efficient user revocation and user management, and the ability to handle role hierarchies. We have also considered some aspects that can be optimized to achieve efficient implementation. We believe that the proposed scheme is suitable for large scale systems, especially in the context of achieving user-centric secure information storage in a cloud computing environment. To provide further administrative convenience and scalability, we are currently developing an administrative model for our RBE scheme.

REFERENCES

[1] Delerablée, C. (2007) Identity-based Broadcast Encryption with Constant Size Ciphertexts and Private Keys. ASIACRYPT, Kuching, Malaysia, December 2–6, pp. 200–215. Springer, Berlin.

[2] Vimercati, S., Foresti, S., Jajodia, S., Paraboschi, S. and Samarati, P. (2007) Over-encryption: Management of Access Control Evolution on Outsourced Data. VLDB, University of Vienna, Austria, September 23–27, pp. 123–134. ACM, New York.

[3] Zych, A., Petkovic, M. and Jonker, W. (2008) Efficient key management for cryptographically enforced access control. Comput. Stand. Interfaces, 30, 410–417.

[4] Blundo, C., Cimato, S., di Vimercati, S.D.C., Santis, A.D., Foresti, S., Paraboschi, S. and Samarati, P. (2009) Efficient Key Management for Enforcing Access Control in Outsourced Scenarios. SEC, Pafos, Cyprus, May 18–20, pp. 364–375. Springer, Berlin.

[5] Atallah, M.J., Frikken, K.B. and Blanton, M. (2005) Dynamic and Efficient Key Management for Access Hierarchies. ACM Conf. Computer and Communications Security, Alexandria, VA, USA, November 7–11, pp. 190–202. ACM, NewYork.

[6] Goyal, V., Pandey, O., Sahai, A. andWaters, B. (2006) Attributebased Encryption for Fine-grained Access Control of Encrypted Data. ACM Conf. Computer and Communications Security, Alexandria,VA, USA, October 30–November 3, pp. 89–98.ACM, NewYork.

[7] Bethencourt, J., Sahai,A. andWaters, B. (2007) Ciphertext-policy Attribute-based Encryption. IEEE Symp. Security and Privacy, Oakland, CA, USA, May 20–23, pp. 321–334. IEEE Computer Society, Los Alamitos.

[8] Cheung, L. and Newport, C.C. (2007) Provably Secure Ciphertext PolicyAbe.ACMConf. Computer and Communications Security, Alexandria, VA, USA, October 28–31, pp. 456–465. ACM, NewYork.

[9] Ibraimi, L., Tang, Q., Hartel, P.H. and Jonker, W. (2009) Efficient and Provable Secure Ciphertext-policy Attributebased Encryption Schemes. ISPEC, Xi'an, China, April 13–15, pp. 1–12. Springer, Berlin.

[10] Emura, K., Miyaji, A., Nomura, A., Omote, K. and Soshi, M. (2009) A Ciphertext-policy Attribute-based Encryption Scheme with Constant Ciphertext Length. ISPEC, Xi'an, China, April 13–15, Lecture Notes in Computer Science 5451, pp. 13–23. Springer, Berlin.

[11] Zhu, Y., Ahn, G.-J., Hu, H. and Wang, H. (2010) Cryptographic Role-based Security Mechanisms Based on Role-key Hierarchy. ASIACCS, Beijing, China, April 13–16, pp. 314–319. ACM, NewYork.

[12] Fiat, A. and Naor, M. (1993) Broadcast Encryption. CRYPTO, Santa Barbara, CA, USA, August 22–26, pp. 480–491. Springer, NewYork.

[13] Garay, J.A., Staddon, J. and Wool, A. (2000) Long-lived Broadcast Encryption. CRYPTO, Santa Barbara, CA, USA, August 20–24, pp. 333–352. Springer, NewYork.