ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 10, October 2014

Accountable Contract Signing Protocol for Secure Data Sharing In Multiuser Untrusted Clouds

K.Suneel Kumar Reddy[1], S.J.Saritha [2]

Student, Department of CSE, JNTUACEP, Pulivendula, India [1]

Assistant. Professor, Department of CSE, JNTUACEP, Pulivendula, India[2]

Abstract: Recent computing model that has become important is known as cloud computing which has various services like Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) and Mining as a Service (MaaS). Widely used service among them is the storage service. When a company outsources its data to cloud and the data owners are maintained in the form of groups and members, it is essential to have secure mechanisms in place as the groups are very dynamic. Secure and scalable access to the data by data owners is very important in this context. Every member in a group is able to access his data and he is treated as owner to that data. This member can switch to different group when he moves to other team in future. This way there are instances in which group members move groups and the change dynamics are more. In this scenario it is challenging job to maintain groups and share data in privacy preserving fashion. Recently Recently Liu et al. proposed a scheme for secure multi-owner data sharing. In this paper we implemented an application that simulates the environment where groups and members are dynamically managed with security aspects fulfilled. The empirical results reveal that the application is useful and can be explored to use in real cloud.

Index Terms – Cloud computing, multi-owner data sharing, security

I. INTRODUCTION

Cloud computing has become a reality and there are many cloud service providers offering various services such as Infrastructure as a Service (IaaS), Platform as a Service (Paas), Software as a Service (SaaS) and Mining as a Service (MaaS). There has been increased use of cloud computing services as they are affordable, thanks to virtualization technology in which cloud is built. Virtualization technology made the cloud computing cheaper for commoditizing computing resources. Though cloud is providing great business opportunities and other facilities, security is the major concern as the cloud is treated to be untrusted. Many security schemes came into existence as explored in [1], [2] and [3]. Security in single-owner context is explored in [4]. Single owner does mean that a file is owned by only one person who is known as data owner. The data owner has rights to access data.

In this paper we explored the multi-owner environment in the presence of dynamic groups. We considered a company with employees working on various projects. The related employees are grouped together so as to manage easily. Each group has a group manager. All the group members of a group have rights to access a common file. In other words they have rights to shared data as far as they belong to that group. Members may be revoked by group manager from the corresponding group when employee leaves organization or moves to different project within the group. We built a prototype application based on the concepts conceived from [5] which demonstrates the proof of concept.

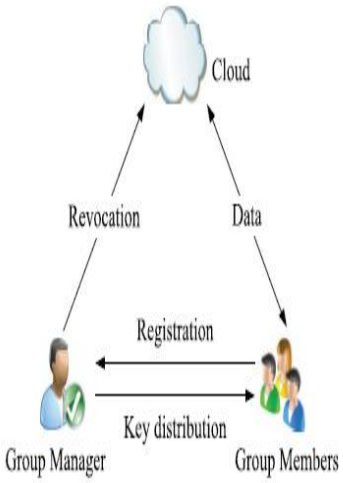

Figure 1 – Multi-owner data sharing environment with dynamic groups

The implementation is based on the overview given in Figure 1. The remainder of this paper is structured as follows. Section II provides review of literature. Section III provides details of proposed system. Section IV presents the implementation of a prototype. Section VI provides experimental results while section VI concludes the paper.

II. RELATED WORK

This section review the literature on the prior works related to data sharing in cloud computing environment.

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 10, October 2014

There were many researchers found related to storage security. For instance, in [3] cryptographic storage systems were reviewed where the data present in the form of files of an operating system is divided into number of chunks and that is secure using cryptographic algorithms. In [6] efficient security mechanisms were provided using NNL construction. In [2] also a security system was built that divides tiles into two parts called as data part and metadata part. An encryption technique named KP-ABE was proposed in [4] for securing cloud data storage. In [1] proxy re-encryption concept was explored in order to help data owners to share data in secure environment and encrypt data before sending it to cloud. It also supports data dynamics on the secured data.

In [7] a scheme known as secure provenance was proposed where group of people can access data securely. In this research each user is allowed to have two keys namely attribute key and signature key in dynamic group environment. Thus it was able to make use of attribute based encryption. In this paper a scenario with groups and members based on certain guidelines of a company are considered for building a system that mimics the multi-user data sharing in cloud computing environment in secure and scalable fashion.

III. PROPOSED SYSTEMFOR MULTI-OWNER DATA SHARING

We proposed a system that can help multiple data owners to share common data across the members. Group can have multiple members and each member can involve in data dynamics. Each group is managed by a group manager who takes care of adding new members and revoking them as per the requirements of the organization. The members of group can upload files and share them to other members and also perform operations on them. They can have full access to the system as per the access rights given. There is no time and geographical restrictions as the system is kept in cloud. The group managers can provide access rights and revoke them to and from group members. This environment warrants high security as multiple users are given common data. The job of group manager is crucial in protecting the data and also ensures that unauthorized employee can not have access to data. As per the company guidelines all employees who are part of groups can have their work done. The mechanism used in this paper are influenced by the work done by Lie et al. [5] where more details can be found. Figure 2 shows the flow of the system with respect to group manager and group members.

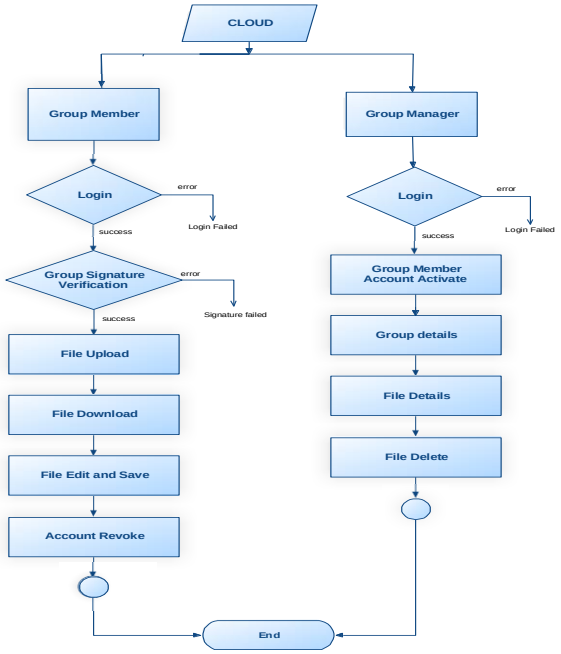

Figure 2 – The flow of activities of group manager and group member

As shown in Figure 2, it is evident that both group manager and group member have certain activities that can be performed. Both users are having access to data. However, group members can gain access to the data of that group only. The multi-owner data access concept considers each member in a group as the owner (one of the owners) of data and the part of data can be manipulated by that member. The members are dynamic in nature as employees may join and leave company.

IV. IMPLEMENTATION

The application is a customer cloud simulator which has been built in Java/J2EE platform. The environment used to build the application is a PC with 4 GB RAM, core 2 dual processor running Windows 7 operating system. The basis for the functionality of the system is the USE CASE diagram modeled as part of requirement analysis. The diagram is shown in Figure 3 which reflects two kinds of users such as group manager and group member having varied access to various functionalities of the system.

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 10, October 2014

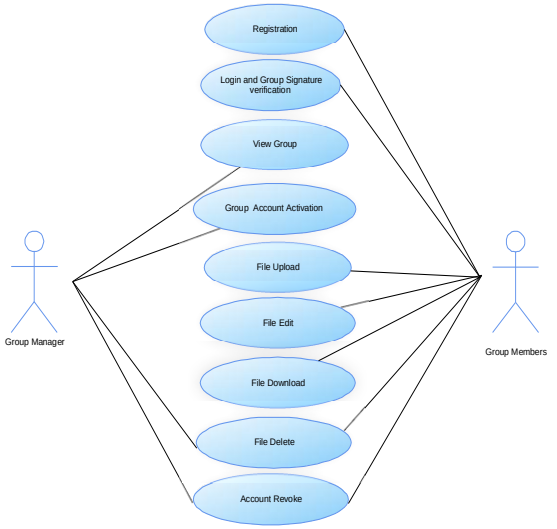

Figure 3 – USE CASE diagram showing important functionalities of the system

Every user account needs to be activated by group manager. Though the group member is registered with the system, it needs to be activated by group manager. Revocation of group members can be done by group manager as per the situations arise with respect to group members leaving the company. Figure 4 shows some of the operations of group member.

Figure 4 – Some of the group member operations

Group members can have data dynamics besides security aspects. Only authorized people can gain access to the data and perform operations on specific files for which they are authorized. The group managers also have certain activities to be performed. Their operations are presented in Figure 5.

Figure 5 – Some of the group manager operations

As seen in Figure 5, group managers can perform all operations of group members but also additional activities like activating new users and revoking existing users based on the dynamics of employees in company. Every user is part of a group and group can have access to certain data which can be manipulated by group members.

V. EXPERIMENTALRESULTS

We have made experiments with the proposed application and the results are compared with that of ODBE. The experiments are made in terms of client side communication cost and the number of revoked users with respect to generating 10 MB file and 100 MB file; computational cost of client side and the number of revoked users with respect to accessing 10MB and 100 MB files.

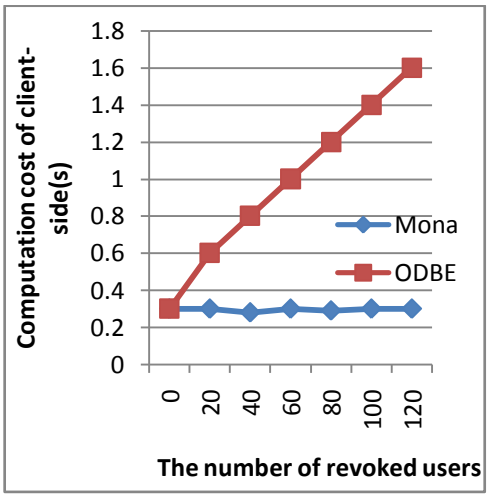

Figure 6 – Computational cost for file generation (10 MB)

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 10, October 2014

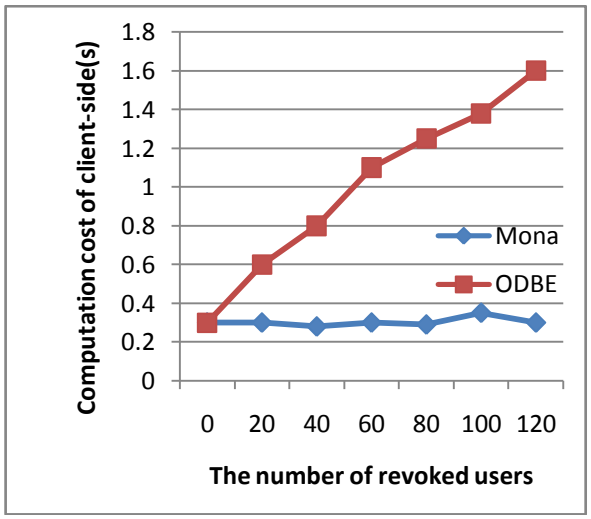

Figure 7 – Computational cost for file generation (100 MB)

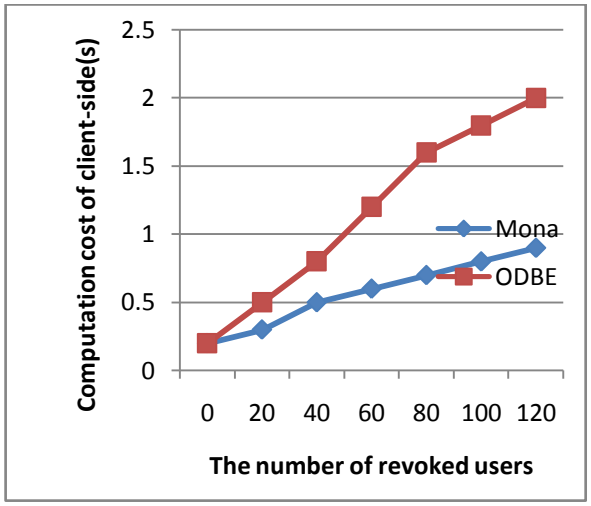

Figure 8 – Computational cost for file accessing (10 MB)

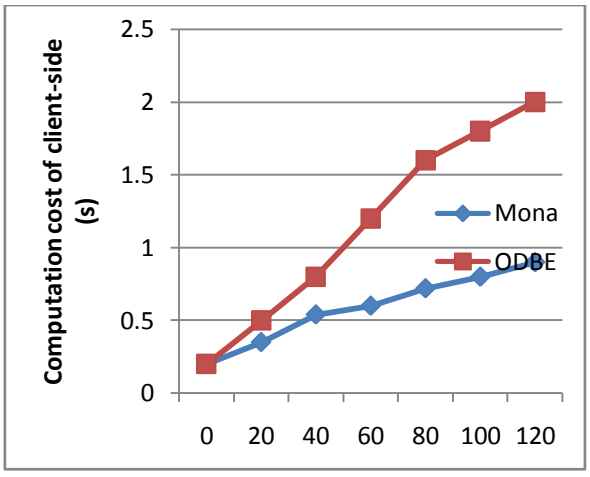

Figure 9 – Computational cost for file accessing (100 MB)

As can be seen in Figure 6, 7, 8 and 9, it is evident that the file generation and file access performance is presented. As the size of file grows, the computation cost is increased. However, the access time is always lesser than the file generation time.

VI. CONCLUSIONS AND FUTURE WORK

In this paper we focused on the challenges in dynamic sharing of data in multi-user environment. The cloud computing environment has provision or maintaining groups and each group consists of number of related users. It can be assumed that a company with many departments can have various groups and each group with members. The groups are highly dynamic in nature as new members can join groups and existing users can be revoked from groups. Group manager takes care of the maintenance of group dynamics based on the employees joining or leaving groups. Both group members and group managers can involve in data dynamics. Recently in [5] the security aspects of such model are explored. In multi-owner data sharing in cloud computing secure communications and access policies are employed. We built a prototype application that demonstrates the proof of concept. The empirical results are encouraging. In future we would like to implement a tool that facilitates formal technical communication among teams with social networking feature.

REFERENCES

[1] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage," Proc. Network and Distributed Systems Security Symp. (NDSS), pp. 29-43, 2005.

[2]E. Goh, H. Shacham, N. Modadugu, and D. Boneh, "Sirius: Securing Remote Untrusted Storage," Proc. Network and Distributed Systems Security Symp. (NDSS), pp. 131-145, 2003.

[3] M. allahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu,"Plutus: Scalable Secure File Sharing on Untrusted torage," Proc. USENIX Conf. File and Storage Technologies, pp. 29-42, 2003.

[4] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing," Proc. IEEE INFOCOM, pp. 534-542, 2010.

[5] Xuefeng Liu, Yuqing Zhang, Member, IEEE, Boyang Wang, and Jingbo Yan, Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud, IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 24, NO. 6, JUNE 2013.

[6] D. Naor, M. Naor, and J.B. Lotspiech, "Revocation and Tracing Schemes for Stateless Receivers," Proc. Ann. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 41-62, 2001.

[7] R. Lu, X. Lin, X. Liang, and X. Shen, "Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing," Proc. ACM Symp. Information, Computer and Comm. Security, pp. 282-292, 2010.