Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 12, December 2014, pg.126 – 132

RESEARCH ARTICLE

A Methodology for Assigning Access Control to Public Clouds

[1]Prince Kumar Piyush, [2]A.Ganesh Kumar

Assistant Professor, Department of CSE, Gokul Institute of Technology and Sciences, Piridi village.
Bobbili mandalam ,Vizianagaram dt. Jntu kakinada university A.P, India[1]
Student, Department of CSE, Gokul Institute of Technology and Sciences, Piridi village.
Bobbili mandalam ,Vizianagaram dt. Jntu kakinada university A.P, India[2]

[1] bambamy9@gmail.com, [2] ganeshkumar_gokul@gmail.com

Abstract-- With the emergence of cloud computing technology and its ability to provide various services at affordable prices has become an important catalyst for many organizations to outsource their data to public cloud. The data owners might allow other users to gain access to their data. In this context, it is important to provide end to end data security to data. In this paper, our focus was on building an architecture that supports perfect communication between data owners, cloud servers and users. The users gain access to data as per the policies presented by the data owners. The data owners encrypt data and send it to cloud. The data owners also delegate access control policies to public cloud where re-encryption of data is taken place. Thus the users of the data can access data in perfectly secure environment. The experiments reveal that the proposed approach is very useful in securing outsourced data and still give access to various users based on the deleted access control policies to public cloud.

I.INTRODUCTION

Cloud computing is an emerging technology that paved way for potential commoditization of computing resources. This technology is on top of virtualization that makes the cloud offerings affordable. With the advent of mobile and hand held devices and innovations with underlying mobile technologies and the ubiquitous nature of mobiles, cloud computing expands to mobile devices as well. This led to mobile cloud computing where mobile devices are associated with cloud computing and leverage benefits of cloud. As people of all walks of life are using mobile devices, the mobility feature of the devices can have tremendous impact on usage of cloud computing. There is steady growth rate projected with respect to mobile cloud computing in future. As mobile devices are energy and

resource constrained, they are vulnerable to various security threats. Unless these threats are addressed, mobile cloud computing cannot be adapted easily. This paper throws light into the mobile cloud computing, its architecture, issues involved and solutions. The insights obtained through review of important papers can help in making well informed decisions with respect to mobile cloud computing and its applications in the real world.

Cloud computing is the technology that realizes the dream of commoditizing computing resources in similar fashion to electricity and water. In fact cloud computing enables users to access huge computing resources. This new model of computing helps people and organizations to access computing resources in pay as you use fashion. Thus the model avoids the need for capital investment. It has got service models like Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). Its deployment models include private cloud, public cloud, community cloud and hybrid cloud. Mobile Cloud Computing (MCC) is the cloud computing where mobile devices are involved.

In this paper our focus in on delegating access control to public cloud. Towards this end we built a prototype application that demonstrates the proof of concept. The delegated access control makes it a suitable model in public cloud where data owners can give access to their data to multiple users. The remainder of this paper is structured as follows. Section II reviews literature on prior works. Section III presents the proposed approach. Section IV presents the prototype application and various user activities. Section V presents experimental results while section VI concludes the paper.

II.RELATED WORKS

From the review of literature many insights were ascertained. The insights obtained from the review of literature [1]-[10] are as follows.

Cryptography is one of the techniques that are widely used in the real world for securing applications. However, cryptography when applied to cloud data dynamics yield to performance issues. Policy based content dissemination [9] is another approach that came into existence in 2010. Later access control policies came into existence. In this paper also we tried access control which is deleted to public cloud. Delegated access control is also studied in [10]. Securing dissemination of XML documents was explored in [8]. While publishing data security of data using cryptography is the focus in [7].

Access control in cloud is also explored in [6] and similar kind of research was carried out in [5]. Broadcast encryption mechanism was explored in [4] where encryption is applied to broadcasting. Oblivious attribute certificates concept was used in [3] for securing data. In similar fashion attribute based security is provided in [2] in terms of group key management. Stateful anonymous credentials were explored in [1].

In this paper our focus in on delegating access control to public cloud. Towards this end we built a prototype application that demonstrates the proof of concept. The delegated access control makes it a suitable model in public cloud where data owners can give access to their data to multiple users.

III.PROPOSED ACCESS CONTROL METHODOLOGY

The proposed approach towards building a system that helps in delegating access control to public cloud is described in this section. Identity provider gives identity tokens to users. With these users register with owner using identity tokens. Users also register with cloud and get secrets from both cloud and owner. Using the secrets, users can perform download and decrypt operations.

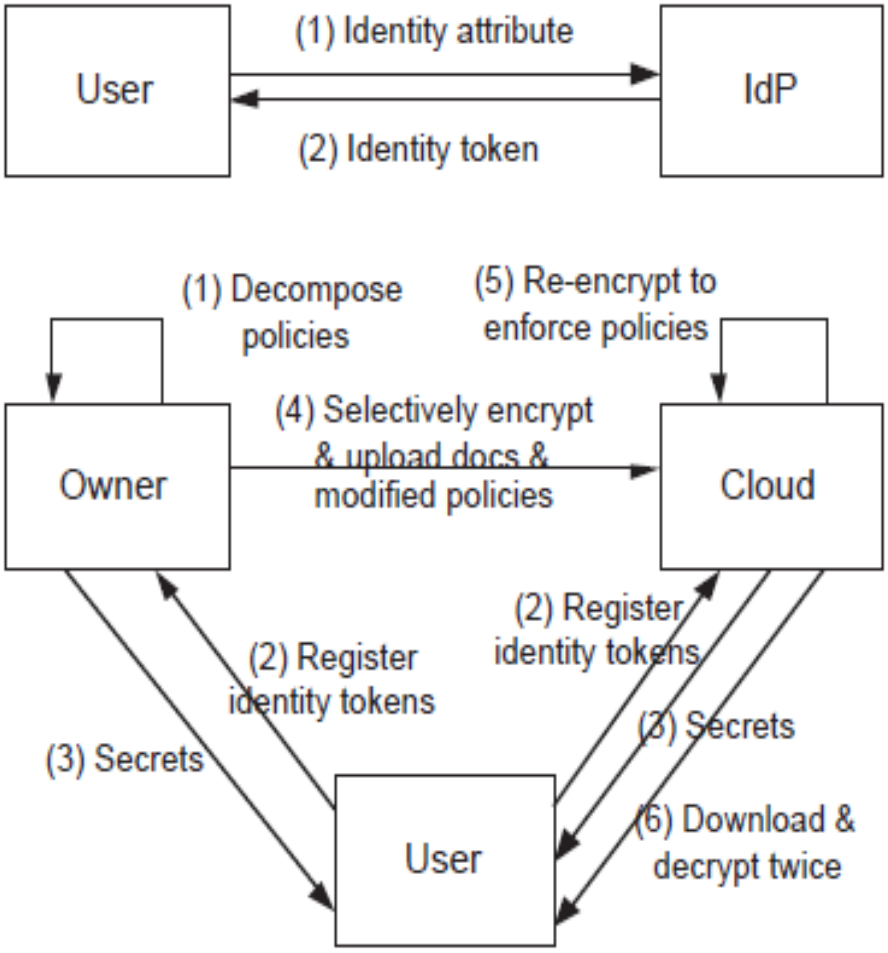

Figure 1 – Overview of the proposed methodology

The data owner is able to decompose files and encrypt them before sending to cloud. The data owner also provides delegation policies to cloud that will help in making best access control policies. The cloud encrypts the content in order to enforce policies.

IV.PROTOTYPE APPLICATION

A prototype application is implemented in order to demonstrate the proof of concept. The application facilitates three kinds of users namely data owner, admin and user. They have specific functionalities as presented in Figure 2.

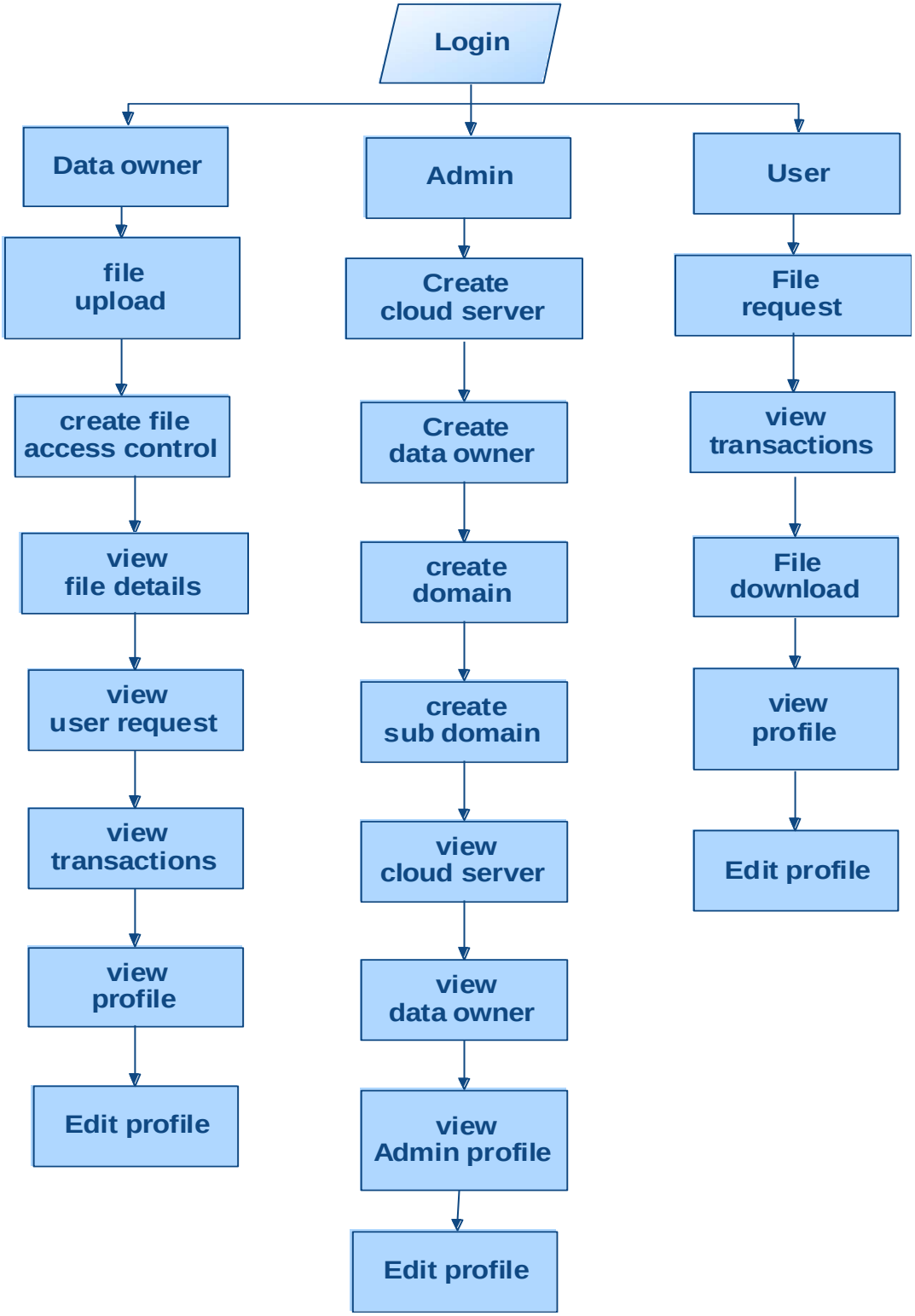

Figure 2 – The functionalities of prototype in terms of user activities

As can be seen in Figure2, it is understood that data owner has activities such as file upload, create file access control, view file details, view user request, view transactions, view profile and edit profile. The admin user has activities like creating cloud server, creating data owner, creating domain, creating sub domain, viewing cloud

servers, viewing data owners, viewing admin profile and editing it. The user has the activities like file request, view transactions, file download, view profile, and edit profile.

V.EXPERIMENTAL RESULTS

Experiments are made in terms of average time taken to generate keys and to derive keys and comparing the results of the two approaches. The results revealed that the proposed approach is more effective.

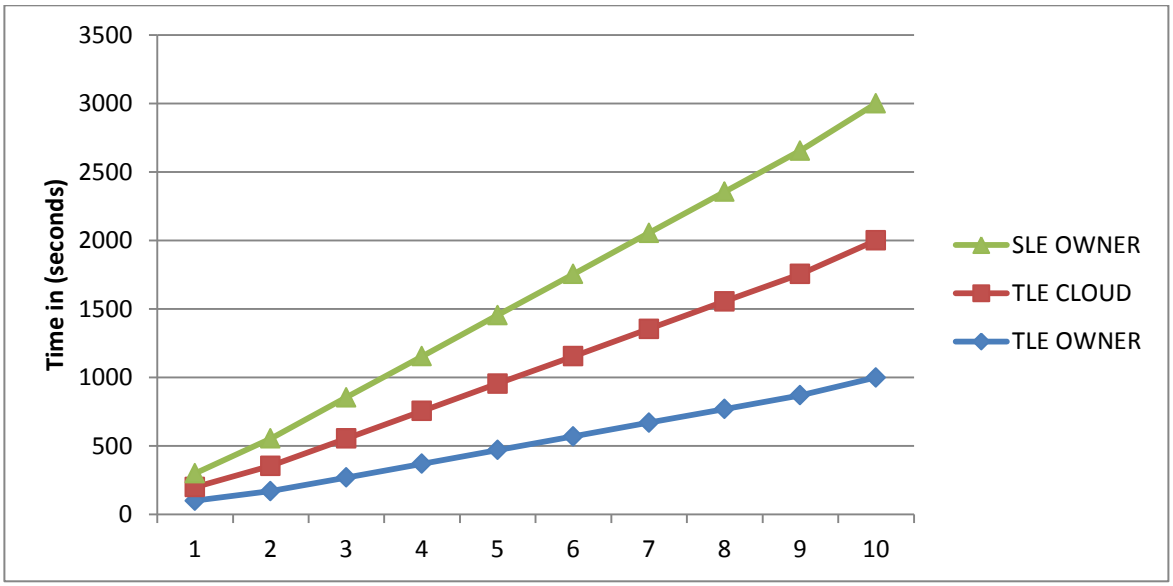

Figure 3 – Performance comparison in terms of average time for keys generation

As can be seen in Figure3, it is evident that the proposed approaches do take less time for generation of security keys.

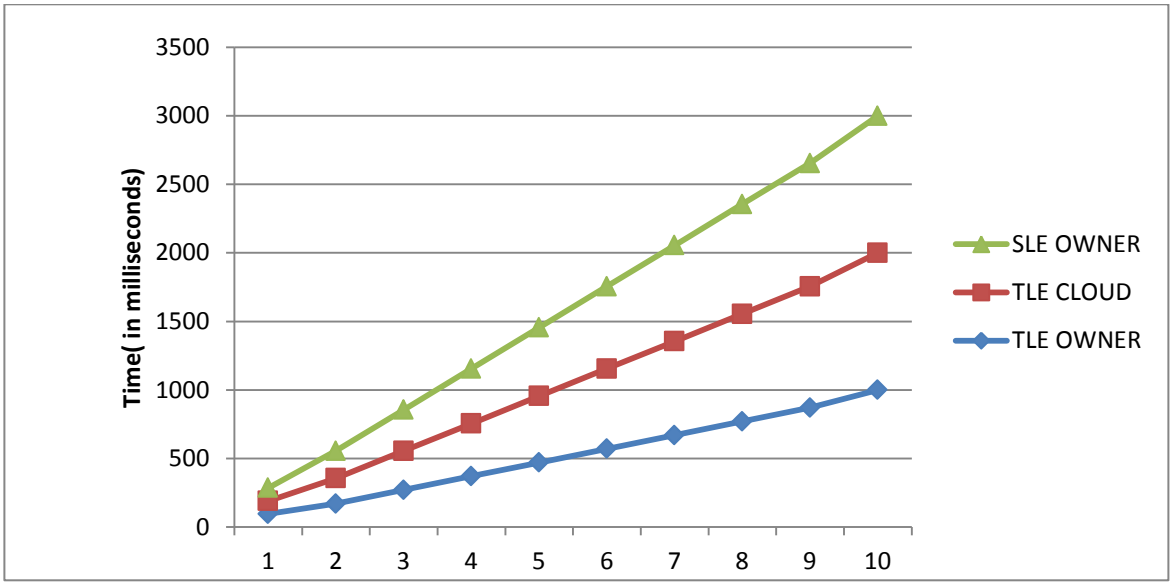

Figure 4 - Performance comparison in terms of average time deriving keys

As can be seen in Figure4, it is evident that the proposed approaches do take less time for generation of security keys.

VI.CONCLUSIONS AND FUTURE WORK

In this paper we studied the security of outsourced data. We came to know many techniques that existed in literature for data security. Our focus in this paper is to ensure privacy preserving data access to multiple users. The data owners protect data and send to cloud server. The data owner also provides access control polices to public cloud. In other words, the data owner is delegating the access control policies to public cloud. Thus the public cloud follows the polices and let users or subscribers of the data owner to gain access to the data in secure environment. In fact, the data is decomposed and encrypted at owner's side and then re-encryption takes place at public cloud. The delegated access control policies are applied by the cloud and as per this the users are given access to the data. Thus the proposed methodology helps data owners to give access to users with controlled access and privacy to the data. The empirical results are encouraging. In future we implement the methodology in real public cloud as this paper simulates the proof of concept.

REFERENCES

[1] S. Coull, M. Green, and S. Hohenberger, "Controlling access to an oblivious database using stateful anonymous credentials," in Irvine: Proceedings of the 12th International Conference on Practice and Theory in Public Key Cryptography. Berlin, Heidelberg: Springer-Verlag, 2009, pp. 501–520.

[2] M. Nabeel and E. Bertino, "Attribute based group key management," IEEE Transactions on Dependable and Secure Computing, 2012.

[3] J. Li and N. Li, "OACerts: Oblivious attribute certificates," IEEE Transactions on Dependable and Secure Computing, vol. 3, no. 4, pp. 340–352, 2006.

[4] A. Fiat and M. Naor, "Broadcast encryption," in Proceedings of the 13th Annual International Cryptology Conference on Advances in Cryptology, ser. CRYPTO '93. London, UK: Springer-Verlag, 1994, pp. 480–491.

[5] S. D. C. di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati, "Over-encryption: Management of access control evolution on outsourced data," in Proceedings of the 33rd International Conference on Very Large Data Bases, ser. VLDB '07. VLDB Endowment, 2007, pp. 123–134.

[6] M. Nabeel, E. Bertino, M. Kantarcioglu, and B. M. Thuraisingham, "Towards privacy preserving access control in the cloud," in Proceedings of the 7th International Conference on Collaborative Computing: Networking, Applications and Worksharing, ser. CollaborateCom '11, 2011, pp. 172–180.

[7] G. Miklau and D. Suciu, "Controlling access to published data using cryptography," in VLDB '2003: Proceedings of the 29th international conference on Very large data bases. VLDB Endowment, 2003, pp. 898–909

[8] E. Bertino and E. Ferrari, "Secure and selective dissemination of XML documents," ACM Trans. Inf. Syst. Secur., vol. 5, no. 3, pp. 290–331, 2002.

[9] N. Shang, M. Nabeel, F. Paci, and E. Bertino, "A privacypreserving approach to policy-based content dissemination," in ICDE '10: Proceedings of the 2010 IEEE 26th International Conference on Data Engineering, 2010.

[10] M. Nabeel and E. Bertino, "Privacy preserving delegated access control in the storage as a service model," in EEE International Conference on Information Reuse and Integration (IRI), 2012.

AUTHORS

Prince Kumar Piyush is currently working towards his M.Tech degree in Gokul Institute of Technology and Sciences, Piridi village, Bobbili mandalam ,Vizianagaram dt, A.P, India. His research interests include Data Mining and cloud computing.

A.Ganesh Kumar is working as an Assistant professor Gokul Institute of Technology and Sciences, Piridi village, Bobbili mandalam ,Vizianagaram dt, A.P,India. His main research interests are data mining and big data mining.

