International Journal of Information Processing, 6(1), 1-11, 2012
ISSN : 0973-8215
IK International Publishing House Pvt. Ltd., New Delhi, India

User-Centric Design for Privacy Preservation in Cloud Environment

Lijo V P[a] and Saidalavi Kalady[b]

[a]Department of Computer Science and Engineering, MES College of Engineering, Kuttippuram 679573, Kerala, India, Contact: paull.lijo@gmail.com

[b]Department of Computer Science and Engineering, National Institute of Technology, Calicut, Kerala, India, Contact: said@nitc.ac.in

Recently, Cloud computing attained its pace in most of the IT services. In cloud computing, the services are provided by some vendors and the customers are unaware about the storage and maintenance of their data. Logically speaking, the client has no control over the cloud. When the service providers process the data being provided by the customers, issues like privacy loss and data leakage may arise. This is an important barrier for the adoption of cloud services. A user-centric approach is essential to overcome this barrier. In this paper we present a solution which provides the control, over the data being submitted in the cloud, to the user. This proposed user-centric solution is implemented in the cloud application eyeOS as a working model.

Keywords : Cloud Computing, Cloud Security, Data Security, Privacy, SaaS.

1. INTRODUCTION

Cloud Computing helps to satisfy customers' computing needs by compute on some remote centralized facilities, instead on local computers. In this cloud, which have computing, storage utilities, computing environment, the users can utilize the services such as the computing and storage provided by some service providers. The users are unaware about where the computing element resides and how the stored data is being used. Since the users have no control over cloud, maintaining the levels of protection of sensitive data is a new challenge. This challenge become very significant when the cloud computing involves a cross-border data transfers.

Cloud computing has become very popular nowadays and majority of the IT companies pursuing in to the cloud. Even though cloud provides cost effective service to customers, the hackers feel it as a honey pot. While sharing same platform, there are chances of data leakage and privacy loss. To advance the cloud computing, users should take proactive measures to ensure security [1].

In cloud computing environment the services are carried out by the software on behalf of users. The users send their data, which may have sensitive information that helps to identify the user, to the cloud service and this data is processed by the application provided by the service provider, and the result is given back to the user. The cloud computing environment is suitable for business, as they can use hardware and software from cloud to meet their computing requirements at a low cost. In Software as a Service (SaaS), data is processed in decrypted form and the result may be stored in the machine as plain text. So, this scenario may lead to leakage of sensitive data from the cloud [2].

In SaaS, the user submit his data to the cloud machine for processing and the user has no control over the submitted data. So the user has no knowledge about where their data resides, how it is stored (as plain text or cipher

the key securely.

Presently eyeOS is available with nearly 60 applications, some of standard applications are from eyeOS core team and the remaining application are from eyeOS community. At least 15 applications such as calculator, calender, *etc.* are play with data that has no sensitive information. Those applications are using only static data. So, Client-Agent has no roll to protect these applications. Almost 30 applications use database and files for storing and retrieving data, and the data may contain sensitive informations. These applications can get assistance of the Client-Agent to preserve data security. In the remaining, most of applications are supporting networking related services and it tends to share files among different users. These applications may offer the features to share and modify one file simultaneously by a group of users. So the Client-Agent cannot manage this kind of application's security with it's present design, even though these applications handle sensitive information.

As a result, 75 % of applications which are needed data security in eyeOS get additional protection and assistance by Client-Agent. Client Agent is developed in PHP and its size is around 10 KB. Main focus while designing and implementation was only on security aspects and successfull completion of the main features of the Client-Agent. Optimization techniques can be used to reduce the size of the code.

6. CONCLUSIONS AND FUTURE WORK

A user-centric solution which provides the user control over the data being submitted in the cloud is introduced in this paper. This user-centric approach present a solution which incorporate a Client-Agent in cloud application which controls and manages data in the cloud. The Client-Agent makes sure that the data stored in the cloud is in encrypted form. And the to and fro data flow is under control of the Client-Agent. This ensures data security and may motivate the users to adopt the cloud applications without fear of data leakage and privacy loss. The implementation of the working model is helped to improve the privacy preservation features of the cloud application eyeOS.

As part of future work, we would like to investigate a solution for protecting data in the cloud without any cooperation of the cloud application, and to derive better key management method at cloud application for fine grained encryption to gain better security.

REFERENCES

1. Kaufman L M, Balaji Prabhakar and Abbas El Gamal. Data Security in the World of Cloud Computing, *in IEEE Security and Privacy,* 7(4):61-64, 2009.
2. Pearson S. Taking Account of Privacy when Designing Cloud Computing Services, *in IEEE ICSE Workshop on Software Engineering Challenges of Cloud Computing, CLOUD'09* pages 44-52, 2009.
3. Lin D, Squicciarini A. Data Protection Models for Service Provisioning in the Cloud, *Proceeding of the 15th ACM Symposium on Access Control Models and Technologies,* pages 183-192, 2010.
4. Mowbray M, Pearson S. A Client-based Privacy Manager for Cloud Computing, *Proceedings of the Fourth International ICST Conference on COMmunication System softWAre and middlewaRE,* pages 1-8, 2009.
5. Subashini S, Kavitha V. A Survey on Security issues in Service Delivery Models of Cloud Computing, *Journal of Network and Computer Applications,* Elsevier, 2010.
6. Wang C, Wang Q, Ren K and Lou W. Ensuring Data Storage Security in Cloud Computing, *17th IEEE International Workshop on Quality of Service, IWQoS* pages 1-9, 2009.
7. Singh M D, Krishna P R and Saxena A. A Cryptography based Privacy Preserving Solution to Mine Cloud Data, *Proceedings of the Third Annual ACM Bangalore Conference,* pages 1-4, 2010.
8. Wang W, Li Z, Owens R and Bhargava B. Secure and Efficient Access to Outsourced Data, *Proceedings of the 2009 ACM Workshop on Cloud Computing Security,* pages 55-66,

2009.

9. Kandukuri B R, Paturi V R and Rakshit A. Cloud Security Issues, *in IEEE International Conference on Services Computing,* pages 517-520, 2009.
10. Christodorescu M, Sailer R, Schales D L, Sgandurra D and Zamboni D. Cloud Security is not (just) Virtualization Security, *Cloud Computing Security Workshop, Chicago, IL,* November, 2009.
11. Lennon R G, Skår L A, Udnæs M, Berre A J, Zeid A, Roman D, Landre E and Van Den Heuvel W J. Best Practices in Cloud Computing: Designing for the Cloud, *Proceeding of the 24th ACM SIGPLAN Conference Companion on Object Oriented Programming systems Languages and Applications*, pages 775-776, 2009.
12. Ramgovind S, Eloff M M and Smith E. The Management of Security in Cloud Computing, *Information Security for South Africa (ISSA),* pages 1-7, August 2010.
13. Li W, Ping L and Pan X. Use Trust Management Module to Achieve Effective Security Mechanisms in Cloud Environment, *in International Conference on IEEE, Electronics and Information Engineering (ICEIE)*, 2010.
14. Sato H, Kanai A, and Tanimoto S. A Cloud Trust Model in a Security Aware Cloud, 2009.
15. Ram C P and Sreenivaasan G. Security as a Service (SasS): Securing user Data by Coprocessor and Distributing the Data, *in IEEE Trendz in Information Sciences and Computing (TISC)*, pages 152-155, 2010.
16. Chuang I, Li S H, Huang K C, Kuo Y H. An Effective Privacy Protection Scheme for Cloud Computing, *Advanced Communication Technology (ICACT) 13th IEEE International Conference,* pages 260-265, 2011.
17. Lombardi F and Di Pietro R. Transparent Security for Cloud, *Proceedings of the 2010 ACM Symposium on Applied Computing,* pages 414-415, ACM, 2010.
18. Xu J, Jinglei T, Dongjian H and Yang Z. Security Scheme for Sensitive Data in Management-type SaaS, *Procedings of the 2009 IEEE International Conference on Information Management, Innovation Management and Industrial Engineering,* pages 83-92, 2009.
19. Norte J C. Fiestas EyeOS Developer Manual per[EB/0L], http://blog.eyeos.org/en/2010/11/20/the-eyeos-user-manual/, *Translated in English by Douglas McKechie,* 2010.

Lijo V P is currently Assistant Professor, Department of Computer Science and Engineering, MES College of Engineering, Kuttippuram, Kerala. He obtained his Bachelor of Engineering from IFET College of Engineering, Villupuram, Tamil Nadu. He received his Masters degree in Computer Science and Engineering from National Institute of Technology, Calicut.

Saidalavi Kalady is currently Assistant Professor, Department of Computer Science and Engineering, NIT, Calicut, Kerala. He obtained his Bachelor of Engineering from T K M College of Engineering, Kollam, Kerala. He received his Masters degree in Computer Science and Engineering from Indian Institute of Science, Bangalore.