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
IMPACT FACTOR: 6.199

IJCSMC, Vol. 8, Issue. 6, June 2019, pg.95 – 99

SECURE DATA SHARING ON CLOUD USING TRANSPARENCY SERVICE MODEL

Madhu B R; M Sindhu; H A Aravinda; Aishwarya S; Nesara A M

Department of Computer Science and Engineering
School of Engineering and Technology, Jain University, Bangalore, Karnataka, India

Abstract— Cloud technology enables data-sharing capabilities, which benefits the user through greater productivity and efficiency. However, the Cloud is susceptible to many privacy and security vulnerabilities. Thus, there is a strong demand for data owners to not only ensure that their data kept private and secure in the Cloud, but also have control over their own data.
If meta-data is compromised, then unapproved access to the client data is possible. For the protection of client data, we present a Transparency Service Model in this research project. TSM provides a mechanism where cloud provider configures the service on the cloud by giving the service information about the cloud storage devices that would contain the data. It is then responsibility of the TSM to store data on those devices and cloud provider no longer has direct access to data storage on those devices.
Keywords— Transparency service model, IaaS (Infrastructure as a service), Cloud service provider

I. INTRODUCTION

Today cloud computing has emerged as a field of great innovation in the computer world. Still various issues persist in this field with data security and data privacy. This is because; the cloud provider has access to the data and monitors the client's information. Due to this reason, the data owners strongly demand to keep their data private and secure on the cloud. The users also desire to have control over the data contents that they share with other users. Therefore, it becomes necessary to have a cryptographically enhanced access control over the shared data. For the protection of client data, we present a Transparency Service Model in this research project. TSM provides a mechanism where cloud provider configures the service on the cloud by giving the service information about the cloud storage devices that would exist the data. It is then responsibility of the TSM to store data on those devices and cloud providers no longer direct access to data storage on those devices.
The cloud system has various security threats and risks. Few of which are mentioned below:

i. Malware Injection: With this threat, the exploiters try to inject malicious programs, codes or services in the cloud.
ii. Spoofing: It is another type of attack mainly used to spoof Meta data information.
iii. Service Hijacking: In this thread the hackers can hack into a web service hosted on the cloud and install malicious software to get valuable user data and information.
iv. Threat from Insiders, Shared Resource Problems, Vulnerabilities, Access Control

© 2019, IJCSMC All Rights Reserved

II. PROPOSED WORK

Transparency Service Model (TSM) is a service that needs to be configured on the cloud system and that would be used by the customers of the cloud to store data on the cloud in a transparent manner. It provides a mechanism where cloud provider configures the service on the cloud by giving the service information about the cloud storage devices that would hold data. It is then responsibility of the TSM to store data on those devices and cloud providers no longer direct access to data storage on those devices.

Service architecture is simple the TSM has been implemented as a layer between the cloud infrastructure and the user. Whenever user needs to save or retrieve a data item from cloud infrastructure he must interact with the TSM. TSM acts as interface between the cloud and the user. Fig below tries to provide an overview of the architecture of the TSM. As cleared by the Fig below whenever user needs to interact with the cloud infrastructure for saving or retrieving files he must interface with the TSM.

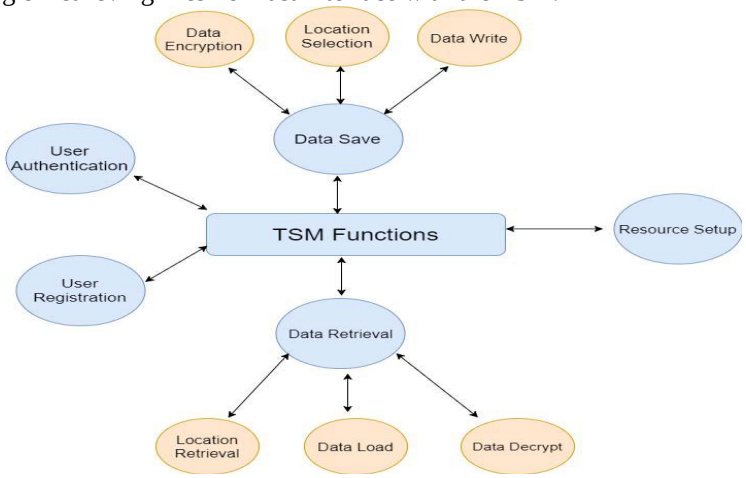

Fig 1: Flow chart

TSM Functions

Major functions of the TSM Application are:

i. **User Registration** – Here users register with service and create their respective profile.

ii. **User Authentication** – Here users verify their credentials with provided in the registration process.

iii. **Data Save** - Here users save their data to the databases.

iv. **Data Retrieval** – Here users retrieve the saved data from their resources.

v. **Resource Setup** - Here resources are set on the provider side. This function allows the provider to add the underlying resources.

III. WORKING

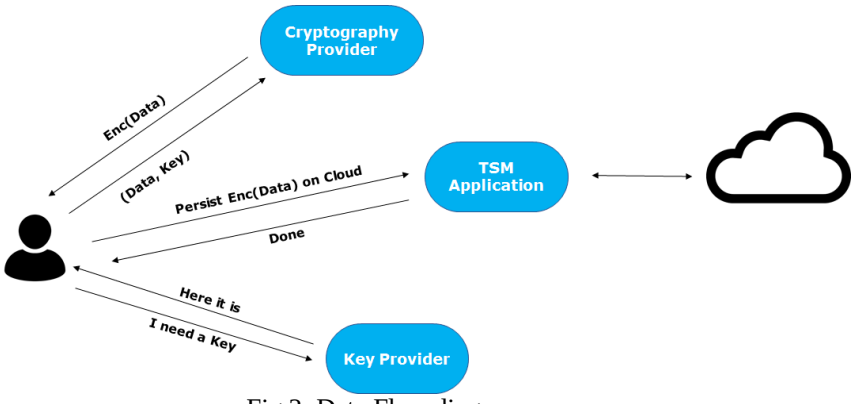

Fig 2: Data Flow diagram

© 2019, IJCSMC All Rights Reserved

1) Key Provider

This portal enables the end user to perform couple of operations with reference to the encryption keys.

i. Key Generation Operation: This component provides the user with a feature where they can generate a new key of required length. This is used while writing a new data to the cloud. The user must just invoke the below URL and specify the mentioned parameters to the URL.

ii. Key Retrieval Operation: This component provides the user with a feature where they can retrieve the key they have generated earlier. This is used while reading the data stored on cloud. The user must just invoke the below URL and specify the mentioned parameters to the URL.

2) Cryptography Provider

This portal enables the user to perform the cryptographic operations on the inputted data. The users perform the below two operations with reference to this portal.

i. Encryption Operations: This component provides the user with a feature where they can perform the encryption of the given input data. Before invoking these components, the user must have already generated the unique key for encryption using the Key Provider component we described earlier. This is used while writing a new data to the cloud. The user must just invoke the below URL and specify the mentioned parameters to the URL.

ii. Decryption Operations: This component provides the user with a feature where they can perform the decryption of the given input data. Before invoking these components, the user must have already generated the unique key for encryption using the Key Provider component we described earlier. This is used while writing reading the existing data from the cloud. The user must just invoke the below URL and specify the mentioned parameters to the URL.

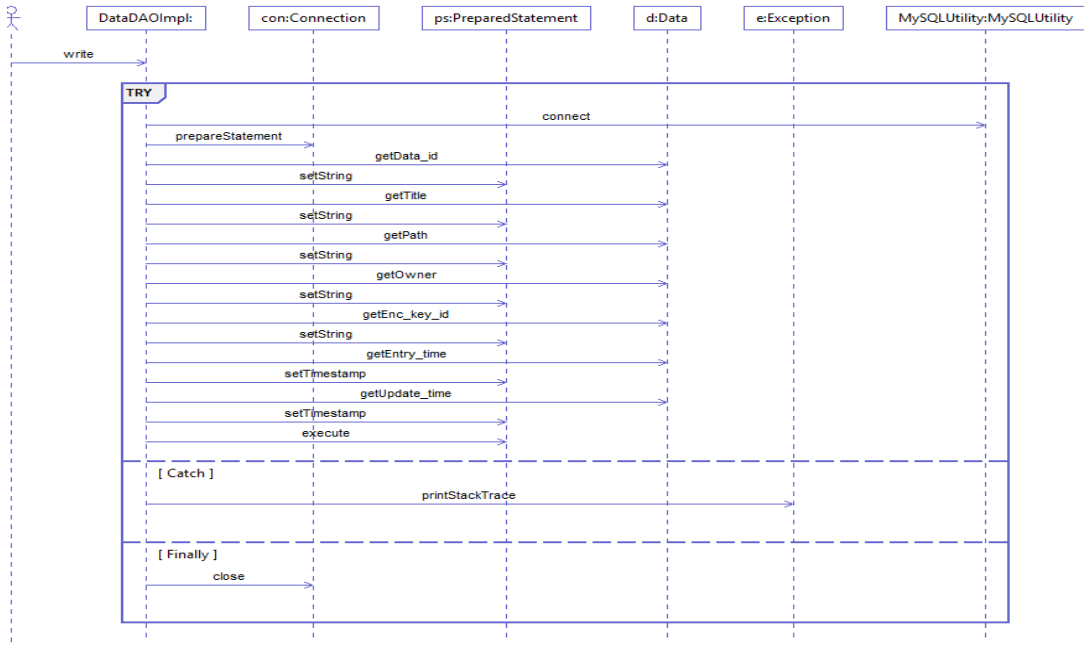

Fig 3: Logic flow diagram

3) TSM Application

TSM Application module provides the following functionalities to the end users.

i. Register a new seller/ buyer account
ii. Login to an existing account
iii. Logout from the session
iv. Edit the existing Profile
v. Change Password for security issues
vi. Forgot Password and receive the current password over an email
vii. Delete an existing Account

© 2019, IJCSMC All Rights Reserved

Apart from this TSM is also responsible for following operations.

i. Data Write Operation: TSM Application performs the data write operation to the cloud storage space. The structured data will be persisted in the MySQL instance of the cloud application deployed in any of the cloud service provider; whereas the unstructured data uploaded, using a browse button will be persisted on the cloud storage file system. The customer first will have to select the data model indicating the type of the data to be written on to the cloud. After selecting the data model, the user will be provided with an interface where they provide the key value pairs for the data models. The data written by the user will be encrypted using the AES (Advanced Encryption Standard) cryptography. To do this, the transparency service model contacts the key provider to get the key and then uses this key and the inputted data to perform encryption with the help of the cryptography provider.

ii. Data Read Operation: In this operation the end users will be able to see the list of all the data they had written on to the cloud storage space in the previous section. The list of all the data will be retrieved from the MySQL instance and from the cloud storage file system of the cloud storage space and then be displayed on the HTML interface. The user can then perform the data decryption of the data using the Advanced Encryption Standard (AES) cryptography. To do this, the transparency service model uses the Key ID stored in MySQL, gets the actual key for decryption from the Key provider, and sends the key and the cipher text to the cryptography provider to perform the decryption operation. The user will then be able to perform the data update operation or the data delete operation in case needed.

iii. Data Share Operation: In this operation the users will be able to share their data with other registered users and can access the data shared with their from other registered users. While sharing the data, the owner must specify the level of access to be granted to the shared user. The access level will be either read-only access or read-write access. The data owners will have a privilege of changing the access levels on the shared data at any point of time.

IV. CONCLUSION

In this project, we have proposed a model to solve the problem of data security and privacy in cloud computing by hiding information from the cloud providers and their employees. Basic purpose of the model was to take over the responsibility of saving and retrieving data from the cloud and doing it in such a way that only the model knows where data of certain user resides and that it can only be accessed by using security mechanism provided in the model.

REFERENCES

[1]. Neal Leavitt, "Is cloud computing really ready for prime time?," in IEEE Computer Society, 2009.

[2]. W. Itani, A Kayssi, and A Chehab, "Privacy as a service: Privacy-aware data storage and processing in cloud computing architectures, "IEEE conference on Dependable, Autonomic and Secure Computing, DASC '09, pp 711–716, December 2009.

[3]. M. Jensen, J. Schwenk, N. Gruschka, and L.L. Iacono, "On technical security issues in cloud computing," in IEEE International Conference on Cloud Computing, CLOUD '09, pp. 109–116, September 2009.

[4]. Meiko Jensen, Nils Gruschka, and Ralph HerkenhÃner. A, " A survey of attacks on web services," in Journal of Computer Science - Research and Development, pp. 185–197, 2009.

[5]. Cong Wang, Qian Wang, Kui Ren, and Wenjing Lou, " Ensuring data storage security in cloud computing," in 17th Internation Workshop on Quality of Service, IWQoS, pp 1–9, July 2009.

[6]. Cong Wang, Qian Wang, Kui Ren, and Wenjing Lou, "Privacy preserving public auditing for data storage security in cloud computing," in Proceedings IEEE INFOCOM, pp 1–9, March 2010.

[7]. Ronald L. Krutz and Russell Dean Vines, "Cloud Security: A Comprehensive Guide to Secure Cloud Computing," Wiley Publishing, 2010.

[8]. W. A. Jansen, "Cloud Hooks: Security and Privacy Issues in Cloud Computing," in 44th Hawaii International Conference on System Sciences, pp. 1–10, Koloa, Hawaii, January 2011.

[9]. Rongxing Lu, Xiaodong Lin, Xiaohui Liang, and Xuemin Shen, "Secure provenance: The essential of bread and butter of data forensics in cloud computing, " in Proceedings of 5th ACM Symposium on Information, Computer and Communications Security, ASIACCS '10, pp. 282– 292, 2010 Peter Mell and Timothy Grance. The nist definition of cloud computing. Technical Report 800-145, National Institute of Standards and Technology (NIST), Gaithersburg, MD, September 2011.

[10]. S. Subashini and V. Kavitha, " Review: A survey on security issues in service delivery models of cloud computing, " in Journal of Network and Computer Applications,pp. 1–11, January 2011.

© 2019, IJCSMC All Rights Reserved

[11]. Ardagna, Danilo, Giuliano Casale, Michele Ciavotta, Juan F Perez and Weikun Wang, Quality-of-service in cloud computing:modeling techniquesand their applications," in Journal of Internet Services and Applications, 2014.
[12]. Alan T Litchfield and Jacqui Althouse, "A systematic review of cloud computing, big data and databases on the cloud," in Proceedings of the Americas Conference on Information Systems, pp 1–19, 2014.
[13]. Monjur Ahmed, Alan T Litchfield and Chandan Sharma, "A distributed security model for cloud computing," in Proceedings of the Americas Conference on Information Systems, 2016.
[14]. Z. Masetic, K. Hajdarevic, N. Dogru. Cloud Computing Threats Classification Model Based on the Detection Feasibility of Machine Learning Algorithms," in 40th International Conference on Information and Technology, Electronics and Microelectronics, 2017.

© 2019, IJCSMC All Rights Reserved