IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology
Vol. 3, Issue 6, June 2016

Secure Cloud Computing Using Decentralized Information Flow Control

Priyanka S. Mane[1], Yogesh B. Gurav [2]

ME Student, Dept of Computer Engineering, Padmabhooshan Vasantdada Patil Institute of Technology, Pune, Maharashtra, India[1]

Associate Professor, Dept of Computer Engineering, Padmabhooshan Vasantdada Patil Institute of Technology. Savitribai Phule Pune University, Maharashtra, India [2]

Abstract: There is major demand to introduce cloud computing in many organizations today. The reason is cloud's sharing infrastructure, multi-tenancy and huge storage facilities ensures increase in computing efficiency, flexibility, generality and cost effectiveness. But with this, organizations want that the computing platform should be secured and should satisfy all the important rules and regulations. So security is the key point for the success of cloud computing. It is examined that cloud computing is less satisfactory in providing security due to its heterogeneity. In this paper a solution named - Decentralized Information Flow Control (DIFC) is defined to solve the problem of security specifically of Software as a Service (SaaS) level. DIFC is a Mandatory Access Control method which is able to provide better security and integrity than is provided by other approaches available today. DIFC enforce general policies by using proper labeling and checking methods. DIFC gives a way to control and monitor the flow of data continuously according to the policy. Hence we believe that DIFC is a powerful tool to enhance SaaS cloud security and to help cloud providers to satisfy rules and regulations and audit this compliance with easy in future.

Keywords: Decentralized Information Flow Control, Cloud security, Access control, labeling.

I. INTRODUCTION

Cloud computing is a proven technology to meet the current needs of Information Technology field. Because of its fast, easy and on demand access to computing resources organizations are moving their data over cloud. But with this, organizations want that the computing platform should be secured and should satisfy all the important rules and regulations. So security is the key point for the success of cloud computing. Security is the challenging task in cloud computing. It stems from the fact that cloud infrastructure is combination of mixed tools and applications which are designed and developed by multiple teams with no integrated approach for assuring data security. For example, some providers may use virtualization [3] concept to isolate the data. Similarly, a data store may provide some other facilities for data isolation.

Traditional security methods such as cryptography[6] and Chinese wall[8] are used in cloud computing but does not meet security and are unable to provide efficiency, generality and flexibility required by cloud providers and tenants. To give better security, a solution, a data centric security method known a Decentralized Information Flow control (DIFC) in particular for Software as a Service (SaaS) cloud level is proposed. DIFC ensures high data security and data integrity. DIFC is a type of Mandatory Access Control (MAC)[2] model in which security policy (i.e labels) is defined at all levels in the system, usually specified by the administrators. DIFC is a MAC model which is originally developed from military information management methods. Such data centric security method gives security in many ways by controlling and tracking information flow. First, the data is stored in secret form to protect from leakage of confidential or sensitive information. Second, controlling the flow of information using access control by imposing policies or rules in the form of labels on the data which are usually specified by the administrator. Third, providing multi-tenancy with data integrity by sharing of resources and services, which is achieved by imposing checks to enforce policies. Fourth, accountability by tracking the flow of information across all services over the cloud which provide to log sensitive transactions. In this paper we proposed a Decentralized Information Flow Control model to enhance cloud security particularly for Software as a Service (SaaS) level. We describe the proposed DIFC system with its architecture and implementation. Performance of the DIFC system results in better security. Our contribution is despite of number of challenging issues in cloud environment our DIFC system leads in more secured and practical cloud computing.

We elaborate our work in four sections. Section II explains the literature survey. Section III explains the DIFC system and its structure. Section IV explains the implementation details. Finally we give conclusion in section V.

II. RELATED WORK

Literature Survey

This survey describes previous methods of information flow control which are given below.

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
Vol. 3, Issue 6, June 2016

1. Information flow control for secure cloud computing. [1]
A data centric security mechanism named decentralized information flow is developed to enchance cloud security. It impose security policies not only on the data but also on the principals of the system.

2. Information flow control for strong protection with flexible sharing in PaaS[2]
In this paper, practically shown IFC enabled middleware. This mechanism able to separate services and applications from their code, which helps to preserves security in cloud. The aim was to maintain end-to-end information flow control.

3. FlowR: Aspect Oriented Programming for Information Flow Control in Ruby[4]
Approach mentioned in this paper is nice solution to apply IFC when there is not any application running. This approach is not only for ruby but can be used for any OO language, which support AOP. IFC serves here as library. This mechanism requires less maintenance.

4. A Distributed Access Control Architecture for Cloud Computing [6]
This article explains distributed access control architecture for multitenant and virtualized environments. It is based on the rules from security management. The goal is to meet cloud users' access control requirements and to generate detailed specifications of such requirements. It uses an XML-based declaration of the access control policy. However, it must address several open challenges in order to implement a fully secure and trusted cloud environment.

5. Silver Lining: Enforcing Secure Information Flow at the Cloud Edge.[14]
SliverLine is the first development on Hadoop cloud information flow, which does not require any changes in cloud infrastructure. It is based on mandatory access control policies of information flow between resources.

In previous access control and security systems there is a lack of tracking i.e, accountability on what operations are performed on data in the cloud. A tenant should have the right to know if his data has been misused, mishandled by the provider, or transmitted to third parties without its consent. But unfortunately this is not considered in the previous system. The cloud interface may have a less subtle and comprehensive view of access control than is required for the application.

III. PROPOSED SYSTEM

Problem statement
To address cloud security and to protect user data stored on the cloud from leakage we propose a data-centric security method named "Decentralized Information Flow Control (DIFC)" which controls the flow of user information on the cloud with tracking the information flow.

Objectives of the proposed system
1. A simplified decentralized information flow control for secure cloud specially for SaaS cloud service layer.
2. Increase data security and maintain integrity of sensitive data.
3. Data isolation with multi-tenancy.
4. Information tracking and accountability.

Structure of the proposed DIFC system

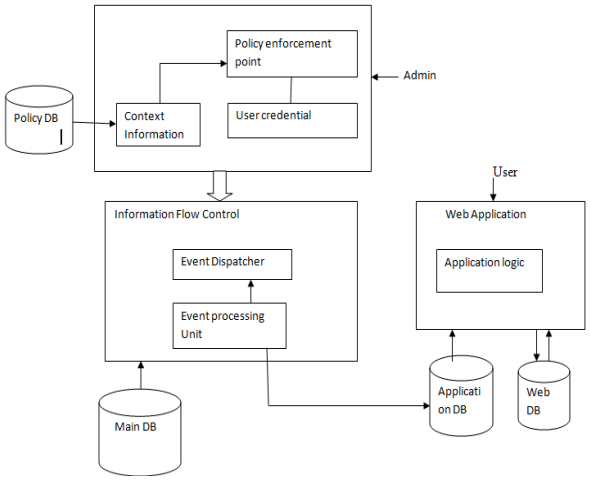

Figure 1.1: Structure of Decentralized Information Flow Control system.

Information flow control in decentralized form is type of a Mandatory Access Control system in which the security policies are defined for the overall system, usually done by the administrators. In DIFC policies are enforced by using proper labelling and checking methods. It gives protection to the data by assigning security policies (labels) with the data, in order to control and observe the flow of the data. The labels are also associated with the principals i.e. the users of the system. DIFC security policy allows relations which are true or satisfy, between the policy labels of the data and the policy labels of principals requesting to access the data. That is, data protection security policy checking schemes are based on comparing the label(s) assigned to the data and with the labels assigned to the principals. The labels are used to give both data confidentiality and integrity with "secrecy" and "quality" of data.

Functions of the system
1. Data Encryption – Data is stored in secret form to protect from leakage of confidential or sensitive information.
2. Access Control Management - Controlling the flow of information using access control by imposing policies or rules in the form of labels on the data which are usually specified by the administrator.
3. Multi-tenancy - providing data integrity by sharing of resources and services, this is achieved by imposing checks to enforce policies.
4. Data flow Tracking – provides accountability by tracking the flow of information across all services over the cloud which provide a way to log sensitive operations.

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
Vol. 3, Issue 6, June 2016

Project Contribution

1. In previous methods only encryption and decryption key is saved in database for access. But for more security as it can be easily available separate access key is generated for every request or operation on data.
2. Data centric security mechanism is used by providing both security policies at privilege level and using access key.

Algorithm used

1. A keyed-hash message authentication code (HMAC) algorithm is used for authentication which verifies the identity of a user who wishes to access information.

A keyed-hash message authentication code (HMAC) is a special type of message authentication code (MAC) involving a cryptographic hash function (hence the 'H') with combine with a secret cryptographic key.

This definition keyed-hash message authentication code (HMAC) is given as:

$$HMAC(K,m) = H\Big((K \oplus opad) \,||\, H\big((K \oplus ipad) \,||\, m\big)\Big)$$

2. Data is stored in encrypted form on the cloud by using AES Cryptographic algorithm.

The Advanced Encryption Standard or AES is a symmetric block cipher to protect classified information which is implemented in software and hardware throughout the world to encrypt sensitive data.

Mathematical Model

- **Definition 1**: [Cloud Instance] I denote the set of cloud instances, I = {i1,...,in}.
- **Definition 2**: [Security Group] G denote the set of security groups, G = {g1,..,gn}.
- **Definition 3**: [Conflict-of-Interest (COI) Class] C denote the set of COI classes, C = {c1 ... ,cn}.
- Based on the above definitions, we give the definition of objects as follows:
- **Definition 4**: [Objects] O denote the set of objects, O = {obj1,... , objn}.
- **Definition 5:** [Object Properties]
- OG i.e. O× G is a many-to-one cloud instance object to security group assignment relation.
- GC i.e. G × C is a many-to-one security group-to-COI class assignment relation.
- O → G is a function that maps a cloud instance object to a security group.
- 0 →C is a function that maps a cloud instance object to a COI class.
- **Definition 6** :[Subjects] S denote the set of subjects. S = {s1, ... ,sn}.
- **Definition 7 : [**Access Operations] Let ACC i.e. S × O be a subject-to-object access relation. A subject-to-object access relation can be represented by (sub, obj) € ACC, which means the subject has accessed the object.
- ACC → Boolean be a function that maps a subject-to object access relation to the boolean values true or false, where
- **- Access(sub, obj) = {true I (sub,obj) € ACC},**
  - Access(sub, obj) = {false I (sub, obj) €ACC}.
- **Definition 8 :** [Policy Specification] OA is a function mapping each subject to a set of objects,
- **OA(sub) = {obj € OAccess(sub, obj) = true}.**

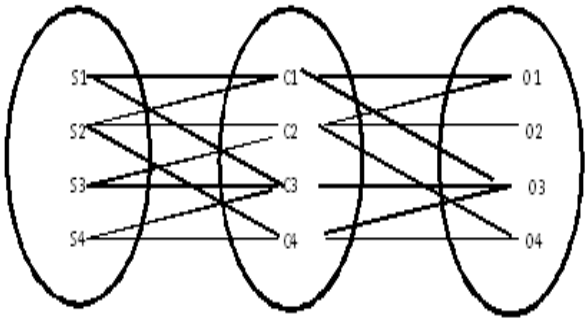

Figure 2.2 Venn diagram

S=Subjects
O= Objects
COI=Conflict of interest

IV. RESULT ANALYSIS

Experimental results:

1. User credential (Access policy) and Database policy – ensuring efficient information flow control and security.
2. Information tracking i.e. logs all the activities in detail which are carried on the cloud data by the users.
3. User information for authentication and trust.
4. Data is stored in encrypted form on the cloud enforcing data confidentiality

Performance Overhead of DIFC system

To determine DIFC overheads, we compared the DIFC implementation with non-IFC implementation. Our concern is the relative performance of the system. Using a workload of 300 requests, sent in immediate succession, we measured:

1. The DIFC-write measurement represents storage of data in secret form. This prevents unauthorized data leakage i.e. protection of sensitive data.
2. The DIFC-read measurement represents authenticated and authorized access to data by providing security policies (lables) both at data and principals.
3. Non-IFC represents common implementation. As there is no IFC enforcement, there is leakage of sensitive data i.e. on read and write.

Figure 2.1 shows the overhead of DIFC enforcement. The results shows that DIFC enforcement gives 13% overhead in performance time for the workload over Non-IFC, which is normal to handle and does not affect much on performance of the system. The DIFC scenario prevented leakage of sensitive data resulting in better security.

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
Vol. 3, Issue 6, June 2016

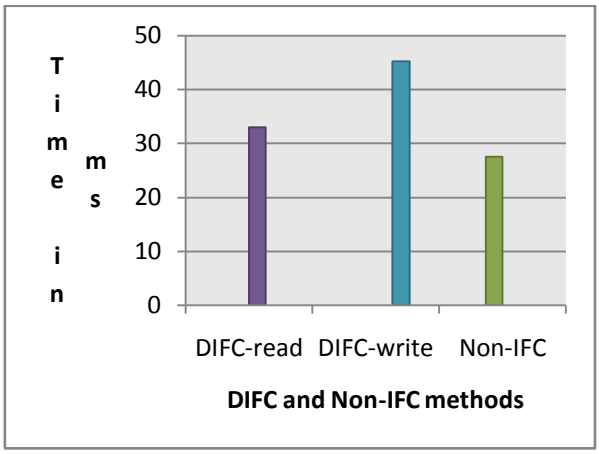

Figure 2.1 Performance evaluation between DIFC system and Non-IFC system for entire 300 request message workload (x-axis time in ms)

In order to validate the DIFC model, we compare it with other IFC models. The comparison is present in table 2.1. it also compared with a number of the information flow control models for cloud computing. The comparison is depend on security parameters. Before proposing the model, we have reviewed almost every proposed information flow control system for secure cloud. Most of them have not been validated or applied in a real cloud computing environment. Hence from the above comparison we can conclude that DIFC is the most appropriate and most suitable model for enhancing secure SaaS cloud computing.

Table 2.1 DIFC against other IFC models.

No.	Comparision parameters	FlowK	Silver Line	Message Middleware-IFC	FlowR	DIFC
1.	Privilege principle	N	N	N	N	Y
2.	Accountability	N	Y	Y	Y	Y
3.	Policy management	Y	Y	N	Y	Y
4.	Integrated with authentication functions	Y	Y	Y	N	Y
5.	Dealing with heterogeneity	Y	Y	Y	Y	Y
6.	Scalability	Y	N	Y	Y	Y

Y = Yes, N = No and N/A = Not applicable.

V. CONCLUSION

DIFC is able to provide ability for the developers to coordinate with the cloud provider and to control how user's sensitive data propagates on the cloud platform. DIFC is most suitable data centric mechanism for enhancing cloud security.

REFERENCES

[1] Jean Bacon, David Eyers, Thomas F. J.-M. Pasquier, Jatinder Singh, Ioannis Papagiannis, and Peter Pietzuch, Information Flow Control for Secure Cloud Computing, IEEE Transactions On Network And Service Management, Vol. 11, No. 1, March 2014.
[2] David Schultz, Barbara Liskov, IFDB: Decentralized Information Flow Control for Databases, ACM, Eurosys'13 April 15–17, 2013.
[3] l. Foster, C. Kesselman, J. Nick, and S. Tuecke. The physiology of the grid: An open grid services architecture for distributed systems integration. In Open Grid Service infrastructure WG, Global Grid Forum, volume 22, pages 1-5. Edinburgh, 2002.
[4] l. Foster, Y. Zhao, l. Raicu, and S. Lu. Cloud computing and grid computing 360-degree compared. ArXiv e-prints, 901:131, 2008.
[5] T. Ert. Service-oriented architecture: concepts, technology, and design. Prentice Hall PTR Upper Saddle River, NJ, USA, 2005.
[6] P. Barham, B. Dragovic, K. Fraser, S. Hand, T. Harris, A. Ho, R. Neugebauer, I. Pratt, and A. Warfield. Xen and the art of virtualization. In Proceedings of the nineteenth ACM symposium on Operating systems principles, page 177. ACM, 2003.
[7] M. Vouk. Cloud computing Issues, research and implementations. In 30th International Conference on Information Technology Intelaces, 2008. ITI 2008, pages 31-40, 2008.
[8] C. J. Millard, Ed., Cloud Computing Law. OUP, 2013.
[9] T. F. J.-M. Pasquier, J. Bacon, and D. Eyers, "FlowK: Information Flow Control for the Cloud," in 6th International Conference on Cloud Computing Technology and Science (CloudCom). IEEE, Dec 2014.
[10] J. Singh, T. Pasquier, J. Bacon, H. Ko, and D. Eyers, "20 Cloud Security Considerations for Supporting the Internet of Things," under review.
[11] J. McLean. Security models and information flow. 1990.
[12] Jatinder Singh, Thomas F. J.-M. Pasquier, Jean Bacon, "Integrating Messaging Middleware and Information Control", IEEE, 2015
[13] Ruoyu Wu, Gail-Joon Ahn, Hongxin Hu, Mukesh Singhal, " Information Flow Control For Cloud Computing", IEEE Conference publications , 2010.
[14] Safwan Mahmud Khan, Kevin W. Hamlen, Murat Kantarcioglu, "Silver Lining: Enforcing Secure Information Flow at the Cloud Edge", IEEE, March 2014, pp. 37-46.
[15] "ApacheHadoop",http://hadoop.apache.org,2013.
[16] Thomas F. J.-M. Pasquier, Jatinder Singh, Jean Bacon, "Information flow control for strong protection with flexible sharing in Paas", IEEE, 2015.
[17] Abdulrahaman A.Almutairi and Muhammad I. Sarfraz, saleh Basalamah, walid g. Aref Ghafoor, "A distributed access control architecture for cloud computing " ,IEEE, 2012, pp. 36-44.
[18] Thomas F. J.-M. Pasquier, J Bacon, "FlowR: Aspect Oriented Programming for Information Flow Control In Ruby", IEEE, 2014, pp. 37-47
[19] Abdulrahaman A.Almutairi and Muhammad I. Sarfraz, saleh Basalamah, walid g. Aref Ghafoor, "A distributed access control architecture for cloud computing " ,IEEE, 2012, pp. 36-44.