International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 4 Issue 5, May 2015

Study on Securing Private Data in Hybrid Cloud

Falguni M Panchal
MCA Sem – VI (CBGS)
Institute of Management and computer Studies
Thane

Manali V Mulik
MCA Sem – VI (CBGS)
Institute of Management and computer Studies
& Research Thane

Abstract - **The cloud computing immerges as a new computing technology where all required services are available as a service. In a cloud environment, location of data is generally maintained by a third party (service provider/vendor) and hence an individual has no control over its own data. In this context, data privacy is an important issue for cloud computing both in terms of legal compliance and user trust. In this paper, an approach for data privacy in hybrid cloud environment is focused. Initially, a data privacy model for cloud computing is provided in which sensitive and non-sensitive data are maintained separately. In order to maintain data privacy, an authentication monitor is introduced in this privacy model. Finally, the authentication algorithm is implemented in a very small setup cloud environment and experimental results are provided at the end of the paper.**

Keywords - Authentication algorithm, Cloud computing, Data Privacy, Security, Sensitive data.

I. INTRODUCTION

The cloud computing is an emerging computing technology in which all required services are available as a service; paradigm shifts from distributed system to virtual centralization. It aims to share data, calculations, and services transparently among users of a massive grid. Software, platform and infrastructure as a service, are three main service delivery models for cloud computing. Cloud computing is a promising computing paradigm which recently has drawn extensive attention from both academia and industry. The basic concept of service oriented architecture has been used in system architecture
and an attempt has been made to put it into cloud system.
Enterprise architecture is considered as an example of system architecture and the relationship among three main computing paradigms like cluster computing, grid computing and cloud computing have been shown.

II. LITERATURE SURVEY

Privacy and security are important issues for cloud computing both in terms of legal compliance and user trust. Paper [1] presented an elaborated study of IaaS (infrastructure as a service) components' security and vulnerabilities and countermeasures are determined. A security model for IaaS (SMI) to guide security assessment and enhancement in IaaS layer is also proposed in [1]. In [2], data security in the world of cloud computing is focused while [3] presented PaaS (Privacy as a Service), a set of security protocols for ensuring the privacy and legal compliance of customer data in cloud computing architecture.

In [4], some security issues that have to be included in SLA are proposed while the privacy challenges that software engineers face when targeting the cloud as their production environment to offer services are assessed, and key design principles to address these are suggested. An approach for data privacy in cloud computing is introduced in [8]. Paper [9] provides some privacy preserving technologies used in cloud computing services. In [11], a secure scalable data access control in cloud computing is focused. In [10], a collaborative trust model of firewall-through based on cloud environment is proposed. However, the problem of simultaneously achieving security, privacy and data confidentiality of access control is really challenging and still remains unresolved.

Due to different diverse architecture of cloud computing, providing security and data privacy in cloud computing is a trivial task. This mechanism also ensures that the private and sensitive data of an enterprise in a cloud environment are to be stored and maintained within the enterprise itself for globally distributed enterprises.

III. DATA PRIVACY MODEL FOR CLOUD COMPUTING

The concept of Cloud Computing evolved from several concepts of virtualization, distributed computing, cluster, grid and utility computing. Computing resources are dynamically provided to the cloud customer based upon the Service Level Agreement (SLA) established between the service provider and the customer. Basically three main services are provided by the cloud provider; Platform as a service (PaaS), Software as a Service (SaaS), and Infrastructure as a service (IaaS). The user can get any of the above services by paying charges to the provider. There are three different types of cloud, namely, Private cloud, Public Cloud, and Hybrid cloud. In case of private cloud, the infrastructure for implementing the cloud is completely controlled by the customer himself. Since the data resides and processed within the customers private network,

ISSN: 2278 – 1323

these data are more secured than that of the public cloud. In case of public cloud, data are stored anywhere in the cloud and the customer may not have any knowledge about where the data is stored. This is a potential threat to the sensitive data used by the customers. In contrast, a large amount of data needs to be stored by an organization (customer), where all of them are not sensitive.

In a cloud environment, it is most suitable that a small amount of data is sensitive and need to keep within own control and the remaining large amount of insensitive data may be managed by the public cloud. In this context, it is necessary to separate sensitive and insensitive data for a particular customer. However, another problem arises when the processes running somewhere in the public cloud and using the sensitive data. The process may be internal or external to the organization. In order to address these problem, the following privacy model for cloud computing is considered in this paper.

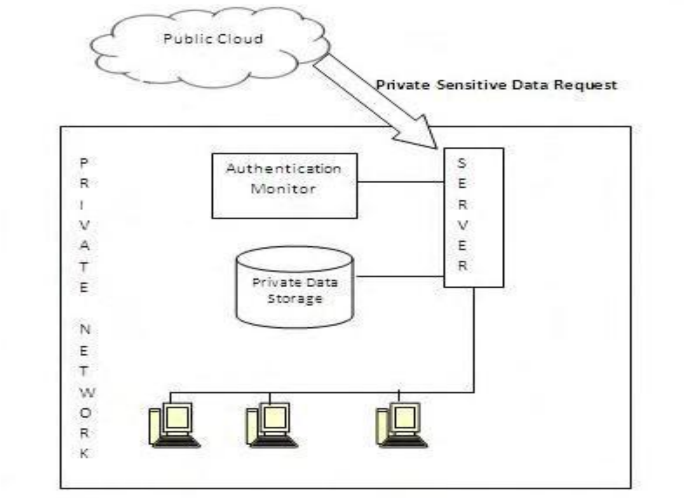

Figure 1: Privacy Model for Cloud Computing

Hence, the proposed privacy model is based on the existing model of cloud computing with advancement. Like the existing model of cloud computing, it has two main components, namely Cloud provider, and Cloud customer. The advancement or up gradation to the existing cloud model is made by introducing the idea of separating the sensitive and non-sensitive data of an organization in an existing hybrid cloud model. In this model, the customer can uses two level categories of data; Private Sensitive Data (PSD) and Public Non-Sensitive Data (PNSD). It has been assumed that Private Sensitive Data (PSD) need not to be accessed from computers outside of the organization, i.e. external to the organization. The Private Sensitive Data (PSD), which is obviously of lesser amount, should be stored within the organization’s own private network, so that the organization has full control over these data.

For any access request to Private Sensitive Data (PSD), it should pass through an authentication procedure. In this model, an Authentication Monitor is introduced which is responsible for identifying whether the access requests to Private Sensitive Data (PSD) is external or internal to the organization and provides the gate way to the server connected with Private Data Storage. This model also considers the globally distributed structure of an organization connected via internet.

IV. ROLE OF AUTHENTICATION MONITOR

In order to maintain data security in cloud computing, two different types of data access request is considered in this work, namely, confidential request and public request. Confidential request are those that want to access the Private Sensitive Data (PSD) where as public request are those that want to access Public Non-Sensitive Data (PNSD) of an organization. Moreover, the requests are also categorized by origin with respect to an organization, namely, Internal Request (IR) and External Request (ER). The request originated from internal terminals of an organization is known as internal request while the request originated from external terminals to an organization is known as external request. The categorized data are stored accordingly to internal or external storage at the time of uploading. The complete taxonomy of requests is listed in the following figure.

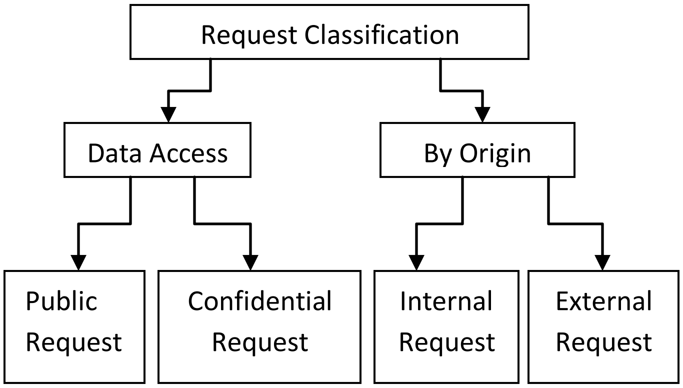

Figure 2: Taxonomy of Requests

In this privacy model, Private Sensitive Data (PSD) is to be stored and controlled by the organization itself where as Public Non-Sensitive Data (PNSD) is to be stored and maintained by the public cloud. Thus, any request to public data is to be handled by the public cloud, but the confidential requests are to be directed to the organization's private network. The Authentication Monitor attached with the server owned by the organization receives and check all the requests to verify whether it is internal or external. Only internal requests are granted and external requests are simply rejected.

V. AN ALGORITHM FOR CHECKING AUTHENTICATION

A variation of Message Authentication Code (MAC) is used here to authenticate the message as well as to verify whether the access request is internal or external to the organization. The brief description of the authentication algorithm from sender side as well as receiver side is as follows.

Assumption:

For every globally distributed private cloud of the same enterprise has a unique key for MAC, say, K_{CID}. All the private clouds have these set of keys, i.e., the set of keys are shared internally.

Similarly, all the private cloud have a shared encryption key set, say, $\{PU_{CID,}\ PR_{CID}\}$, for encrypting the request message.

When a terminal of one private network sends a data accessing request to other private network the following steps will be followed in order to ensure data privacy.

SENDER side:

Step 1: The MAC is produced from Request Message by K_{CID} and the MAC are used.
Step 2: The Request Message is encrypted by the shared encryption key set $\{PU_{CID,}\ PR_{CID}\}$.
Step 3: The encrypted Request Message and the MAC from original Request Message sent together to the intended receiver.

RECEIVER side:

Step 1: When the receiver receives this pair, it first decrypts the request message to get original request message.
Step 2: Then it produces the MAC from the original request message using the set of $\{K_{CIDi}\}$. Since K_{CID} is within the set of $\{K_{CID\ i}\}$ at least one of the key producing MAC will match with the received MAC and thus, $K_{CID\ I}$ determines the origin of request.
Step 3: If the request is internal the decrypted request message is used to process further. If the MAC does not match at all the request is simply rejected.

VI. SUGGESTIONS ON HYBRID CLOUD SECURITY

1.Ask the right questions of your public cloud providers. Choosing the right public cloud provider is essential. You must ask them specifically what data protection features they deploy, as well as how they handle replication, backup and disaster recovery. Technologies that can help increase security include private virtual LANs that isolate virtual machines and separate network and server administrative duties. Also, don't be hesitant to ask about the technology they use in their data centers and ask them to provide you copies of their security policies. If their policies and protections are less stringent than your own, you may have a problem.

2.Understand where you are vulnerable and deploy solutions that address concerns, particularly in protecting data as it travels between cloud environments. Certain products can offer security protection as data moves between your enterprise and the public cloud. One example is Intel Expressway Tokenization Broker, which offers an in-line proxy solution that can be deployed at the edge of the enterprise and the public cloud provider. It protects the traffic and data going into, out of or flowing in between Platform as a Service application programming interfaces (APIs) and providers. The gateway applies format-preserving encryption, tokenization or message-level security to API and Web services messages that are flowing through enterprise systems to cloud provider environments.

3.Centralize governance and control of cloud deployments within the IT organization. This will allow IT to control security policies, ensure compliance and put in the proper technologies and procedures for backup, archiving and recovery. The last thing you need is for a line-of-business manager to put the organization at risk by not doing the proper homework or not putting in the proper procedures in selecting a public cloud partner. IT should ensure that security features and compliance policies are managed consistently across the entire cloud environment -- public and private

VII. CONCLUSION

This paper presents an approach for data privacy in hybrid cloud environment. In order to provide data privacy, a data privacy model for cloud computing is introduced here. However, this privacy model relies on the fact that sensitive data of an enterprise should be maintained by the enterprise itself. Moreover, the authentication algorithm is implemented in a very small setup cloud environment and experimental results are provided.

In future scope, the authentication algorithm can be tested in an established hybrid cloud computing environment. Moreover, encryption and authentication algorithms can be enhanced in order to provide more data privacy and security. Further, a new approach for data privacy, information security monitoring, can be implemented by inferring identity from user behavior in cloud environment.

REFERENCES

I. Wesam Dawoud, Ibrahim Takouna, Christoph Meinel, “Infrastructure as a Service Security: Challenges and Solutions”, Proceedings of the 7th International Conference on Informatics and Systems, March 2010, pp 1-8.

J. John Harauz, Lori M. Kaufman, Bruce Potter, “Data Security in the World of Cloud Computing”, Proceedings of the IEEE Conference on Security and Privacy, July/August 2009, pp 61-64.

K. Wassim Itani, Ayman Kayssi, Ali Chehab, “Privacy as a Service: Privacy-Aware Data Storage and Processing in Cloud Computing Architectures”, Proceedings of the 8th IEEE International Conference on Dependable, Autonomic and Secure Computing, 2009, pp 711-716.

L. Balachandra Reddy Kandukuri, Ramakrishna Paturi V, Atanu Rakshit, “Cloud Security Issues”, Proceeding of IEEE International Conference on Services Computing, 2009, pp 517-520.

M. Lijun Mei, W.K. Chan, T.H. Tse, “A Tale of Clouds: Paradigm Comparisons and Some Thoughts on Research Issues”, Proceedings of the IEEE Asia-Pacific Services Computing Conference, 2008, pp 464-469.

N. Siani Pearson, “Taking Account of Privacy when Designing Cloud Computing Services”, Proceedings of the Workshop ICSE 2009, May 2009, pp 44-52.

O. Manish Pokharel, YoungHyun Yoon, Jong Sou Park, “Cloud Computing in System Architecture”, Proceedings of the International Symposium on Computer Network and Multimedia Technology, January 2009, pp 1-5.

P. Ganguly Uttam, “An Approach to Data privacy in Cloud Computing: Keep Sensitive Data Private”, International Conference on Computing and Systems 2010, The University of Burdwan.

Q. Jian Wang, Yan Zhao, Shuo Jiang, Jiajin Le, “Providing Privacy Preserving in cloud computing”, Proceedings of International Conference on Test and Measurement, 2009, pp 213 - 216.

R. Zhimin Yang, Lixiang Qiao, Chang Liu, Chi Yang, Guangming Wan, “A Collaborative Trust Model of Firewall-through based on Cloud Computing”, Proceedings of the 14th IEEE International Conference on Computer Supported Cooperative Work in Design, 2010, pp 329-334.

S. Shucheng Yu, Cong Wang, Kui Ren, Wenjing Lou, “Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing”, Proceedings of the IEEE INFOCOM, March 2010, pp 1-9.

T. HMAC, Federal Information Processing Standards, *PUB 198* 2002.

BIOGRAPHY

Falguni M Panchal born in Mumbai, Maharashtra India. She is pursuing MCA final year in ASM's Institute of Management & Computer Studies ,IMCOST, Thane

Manali V. Mulik born in Mumbai, Maharashtra India. She is pursuing MCA final year in ASM's Institute of Management & Computer Studies, IMCOST, Thane