Data Centric Security in Cloud Computing

Asif Husain
PhD Pursuing
Department of Computer Science
Shri Satya Sai University of Technology and Medical Sciences, Sehore, M.P., India

Abstract— As the Cloud Computing is growing day by day, It is a great deal to control and manage the data, escape from stealing and other security issues. Security is one of the critical issue in Cloud Computing. To make data very secure in clouds, a lot of work has been done in this area. Although Cloud Computing has a number of unique advantages but various issues like Integrity, Unauthorized access, Security attacks always come in picture. Security, Specifically data security, is one of the most essential and critical aspect of Cloud Computing. A lot of work has been done in this field and researchers are still working on it, but the existing security solutions are not sufficient. This paper emphasizes the requirement of adoption of new approach in data security which is known as data/information centric security. This paper presents a security framework and describes many tools of data centric security. Data Centric Security ensures data security in both in transit as well as in motion. In data centric security procedures /modules are embedded in data itself, instead of the data container.

Keywords: Cloud Computing, Data Centric Security, FPE

I. INTRODUCTION

Cloud Computing is the on-demand availability of computer resources especially storage and infrastructure without active management by the user. Cloud computing refers to anything that involves delivering hosted services over the Internet. In cloud computing, data or information is stored in centralized servers and fetched temporarily on demand on client's system. Cloud computing is very convenient but the data storage in other company's server increases the insecurity of data especially for sensitive data like government schemes data, Personal, financial data etc. Insecurity of data breaks the trust on Cloud Company. Data Centric Security is one of the best way to maintain the security of sensitive data. In this security solution security system in not supposed to retain in the organization, it moves with the data. Data security is provided through cryptography, the encrypted data is unusable to anyone who does not have decryption key. It does not matter whether the data is in motion or at rest, it will remain protected. The owner of the data who has decryption keys maintains the security and can decide to whom and which permission is to allow access to the data. But the major problem with the encryption is that during data processing on intermediate nodes, the data must be decrypted first, because processing cannot be done on encrypted data and the size of file may will also increase. Sharing of secret keys is also an issue.

II. PROCEDURE FOR PAPER SUBMISSION

A. Review Stage

The technologies available for content centric security. Are briefly described as:

1) Object Based Storage:

An Object Storage system provides facility to store files along with metadata added to them, which is called objects. In Object Storage, no file system hierarchy is used. In object storage all storage nodes are treated as a single pool where all objects have same level or priority rather than file sys-tem hierarchy. Object storage can be accessed through applications that use a REST API (Representational State Transfer). It is a software architecture that is used for distributed application environments, such as the internet. An API is used for an application (client) to talk to its environment (backend servers, storage, databases etc.) An identifier is created while storing objects. This identifier is used to locate these objects from the pool. Structure of an object is shown in Fig.1.

The Applications which needs to access objects can quickly retrieve the data through the object identifier or by using the associated metadata (information about the objects, like name). The object based approach is faster and easier as compared to a traditional file system. Labeling, indexing etc. procedures can be made an integral part of metadata to implement data centric security.

2) Tokenization:

It is a process where critical data such as Account number is re-placed by any other irrelevant information, which is known as token. In data centric security a token is provided in lieu of sensitive data. Token is an identifier that maps to the sensitive data through a tokenization system. The mapping from original data to a token uses methods which makes tokens infeasible to re-verse in the absence of the tokenization system. Tokens re-placement of data results is minimized exposure of sensitive data and reduction in risk of compromise to sensitive data.

3) Data Masking

In Data Masking the existing sensitive information is replaced with some information that looks real but is useless to anyone who might wish to misuse it. In data masking data is visible to unauthorized entity but it is useless. Shuffling, substitution, number and date variance are some of the well-known techniques of data masking.

4) Format Preserving Encryption:

In Encryption, once data is encrypted, the encrypted data can-not be processed until it is decrypted. Hence new advancements in this field of encryption made a data centrical solution viable which is known as Format-preserving encryption (FPE). FPE encrypts a plaintext of some specified format into a cipher-text(Secret Text) of the same format— for example, encrypting a mobile number into another mobile number. Now encryption can be applied to any type of data — such as first and last names stored in a file — and still be processes by the application without error. And encryption keys can be provided to select users, keeping data secret from those not entrusted with keys.

B. Proposed Framework

The proposed framework is shown in fig. 2. In the proposed framework in cloud, operating environment, object storage and services are presented as separate modules but these modules can be merged because object storage is a storage (infrastructure) module in real sense. The proposed model incorporates the feature of Oracle labelling security for labeling of data items and for security policy enforcement.

1) Commodity Hardware

This layer deals with the IaaS (Infrastructure as a Service) layer of cloud computing. All the hardware devices required for net-working and data storage comes under this layer.

a) Data Storage

In cloud environment, the data storage is broadly categorized into two categories i.e Storage Area Network (SAN) and Object based storage. In SAN dedicated storage nodes are organized in clusters, which are used to store data. It uses hierarchical storage structure but it has an issue of scalability. On the other hand, Object based storage share a pool of objects without any hierarchical relationship. Objects are identifiable entities, having a unique ID and associated metadata. In this proposed security framework Critical data is stored under object based scheme. Less critical data could be stored under block storage mechanism. Hence it comprises the advantages of both the mechanisms.

2) Data Management Layer

As we know that the sensitivity of all information stored at cloud provider site is not same, Some Information may be highly sensitive and some may be less sensitive; hence uniform level of security is not required to all the data. For this purpose data should be labeled based on its sensitivity. Oracle labelling security enables to control the display of individual data items using labels which are assigned to data items and application users. The Visibility of sensitive information can be easily restricted to authorized users only. Oracle label security enables classification of data at row level and provides out of the box access mediation based on the data classification and the user label authorization or security clearance. Anyone may get access to that particular row. Visibility labels provide an assurance that a particular set of data item will be allowed to access by authorized user only. Data whether in rest or in motion is also encrypted to add an additional level of protection.

3) Access Control Services and Key Management

This layer is dedicated to authenticate the authorized users. This layer also deals with the management of user credentials along with cryptographic keys.

4) Interfaces

This layes is responsible to grant access of any cloud service (i.e. IaaS, PaaS, Saas).It provides a GUI or API, through which user can interact with the application.

5) Auditing and Policy Specification

This layer is responsible to keep audit record of each and every request for data access. It not only maintains record for successful requests but also for failed requests. This layer also specifies the privileges to view data that has particular set of visibility labels after successful authentication of the entity involved. This layer works throughout all the layers of the proposed model.

C. Figures

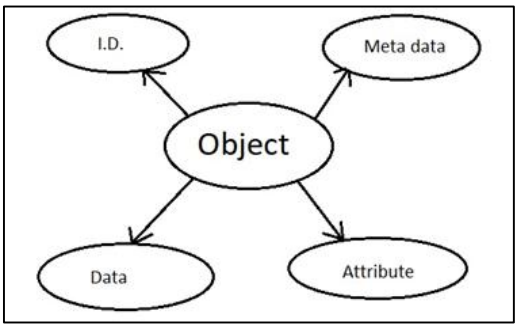

Fig. 1: Object Based Storage

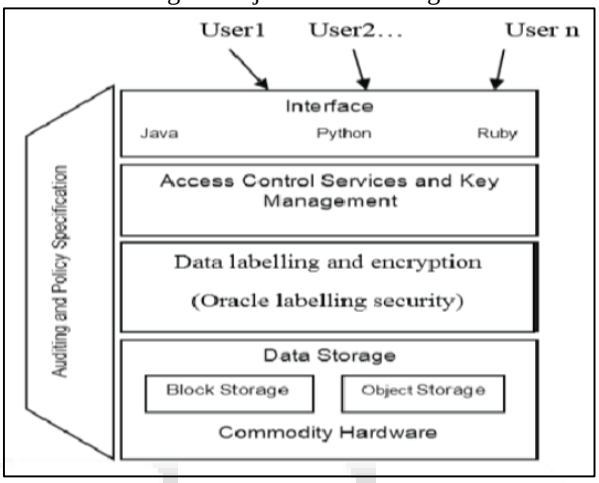

Fig. 2: Proposed Security framework for cloud computing

III. Conclusion

In spite of there are number of security enhancements in cloud computing but still there is no assurance of good level of security. In the proposed scheme, discussed in this paper, attempts to secure data in a cloud environment by adopting a data centric scheme. A data centric security framework is also proposed which can fit in cloud environment effectively. Content centric security is a paradigm shift from traditional network or host based security. This does not mean that traditional container based security schemes were totally overlooked. Cloud computing security can be benefited by utilizing both the mechanisms. Through data centric security it is possible that data reach only intended audience.

References

[1] Kelley Diana,"How Data-Centric Protection Increases Security in Cloud Computing and Virtualization", Security curve white paper, 2011.
[2] Gentry Craig,"A Fully Homomorphic Encryption Scheme", Dessertation of Ph.D, Sept. 2009.
[3] Leyden Tom,"A Beginner's Guide To Next Generation Object Storage", Data Directs Network White paper, 2013.
[4] B. Tarnauca et al., Netinf evaluation, EC FP7-ICT-4WARD Project, Deliverable D-6.3, June 2010 [Online] Available: http://www.4ward-project.eu).
[5] Jacobson V. et al.,"Networking named content", In Proc. Of CoNEXT'09 - 5th International Conference on Emerging Net-working Experiments and Technologies, Rome, Italy, Dec. 2009.

