ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

Designing Data Security Mechanism for Cloud Computing

Vinayak D. Shinde, Jyoti Vaibhav Jadhav, Pallavi Kamalakar Bhoir

H.O.D., Dept. of Computer Engineering, Shree L.R. Tiwari College of Engineering, Mira Road, Thane, India

M.E. Scholar (Computer Engineering), Shree L.R. Tiwari College of Engineering, Mira Road, Thane, India

ABSTRACT: Cloud computing is the collection of remote network servers which are hosted on the internet. They store, process, manage data remotely instead of storing it in local server or local computer. And **Data security** is securing data from unwanted uses or unwanted access. Data security in cloud computing is very important because data and program are not residing on enterprise's data center. It can be anywhere in the globe and can be managed by some other entity. This paper focuses on common security mechanisms like authentication, authorization, encryption and access control.

KEYWORDS: cloud computing, access control**,** encryption

I. INTRODUCTION

According to National Institute of Standards and Technology (NIST) [1] definition cloud computing enables ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. As per definition cloud computing gives access to pool of resources. Resources can be hardware, software or it can be infrastructure. Data security is major concern for users who want to use cloud computing. Most of the cloud services users are concern about their private data that may be used for other purpose.

Cloud computing is used for mainly for two purposes first is computing and second is data storage. In the computing scenario client just access the data and does computing over the internet without knowing where the data is located. In the second scenario client's data is stored on the cloud. So here the data protection and data security come into picture. Cloud computing provider has to provide security assurance to clients to gain their trust and make the cloud computing technology successful. This paper focuses on common security mechanism.

II. RELATED WORK

TYPES OF CLOUD SERVICES:

1. IaaS (Infrastructure as a Service)

This service provides storage, network and hardware to users to deploy their own application. Security provisions (except infrastructure) are provided by cloud subscriber.

2. PaaS (Platform as a Service)

This service provides development platform for the clients. It can be development language or application server technology. Cloud subscriber has control over application. Security is split into provider and subscriber.

3. SaaS (Software as a Service):

This is highest level of service. SaaS deliver application or software to user and users can access it with the help of web browser. The software is generally sold to users via subscription. Security is carried out solely by provider.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

III.PROPOSED ALGORITHM

DEPLOYMENT TYPES

1. Private cloud
Private Clouds are owned by particular enterprise. This enables the enterprise to use cloud computing in centralizing access from different locations, departments. Example: eBay.
2. Public cloud
Public cloud is owned by third party service provider. It provide service to users. Its resources are rented to users. Particular organization may use the cloud functionality from other providers reducing cost of its own infrastructure. Example: Amazon, Google Apps.
3. Hybrid cloud
Hybrid clouds consist of a mixed deployment of *private* and *public cloud* infrastructures to access the infrastructure. Client can deploy sensitive data on private cloud and less sensitive data on public cloud.

IV.PSEUDO CODE

DATA SECURITY AND STORAGE

Data security is important at all levels of cloud computing environment. The customers must ensure that any sensitive or regulated data is not placed into a public cloud or only encrypted data is placed into the cloud for simple storage only. Customers should also be concerned about what data the provider collects and how it is protected; like how metadata is secured, what access customers have to that metadata, what security controls provided are implemented at the network level and so on. The major areas where data security might be at risk are as follows :

1. Cloud data–in-transit: The protocol used to transfer data across clouds provides confidentiality and integrity (SSL,TLS) that is the data transfer happens in encrypted channel
2. Cloud data-at-rest: It is strongly recommended to encrypt the data-at-rest. The goal is to prevent unauthorized users to read the data.
3. Processing of data: Data must be encrypted when it is processed in the cloud, which means that it allows the data to be processed without decryption.
4. Data lineage: Following the path data (mapping application data flows) is known as data lineage that is exactly when and where the data was specifically located within the cloud, and maintained for auditor's assurance.
5. Data provenance: Data Provenance means that not only data has integrity, but it is computationally accurate also.
6. Data remanence: Data remanence is the residual representation of data that has been in some way nominally erased or removed, the risk posed by this in cloud is that an organisation's data can be inadvertently exposed to an unauthorized party.

V.SIMULATION RESULTS

DATA SECURITY ISSUES IN CLOUD

Security is one of the main issue in storing and processing data in the cloud. Following are the threats provided by CSA[2] against data in cloud computing:

1. Data Breaches – Organization's internal data (sensitive) is captured by competitors. If the cloud service database is not properly designed then attacker can access client data.
2. Data Loss – Data stored on the cloud is lost due to other reasons other than attackers. It could be accidental deletion or natural disaster.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

3. Account Hijack – If attacker gains access to credentials then he can manipulate data, transaction, redirect clients to other sites.
4. Denial of service – Attackers prevent the clients or users to access their data or their applications.
5. Malicious insiders – CERN [3] defines the insider threat as "A malicious insider threat to an organization is a current or former employee, contractor, or other business partner who has or had authorized access to an organization's network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems."
6. Abuse of cloud services – Small company can use large cloud computing power. Person can use this large computing power to get encryption key and with the help of this he can distribute the pirated software.

Some of the security measures adopted by the cloud in securing its data include authentication, authorization, access control and encryption.

VI. CONCLUSION AND FUTURE WORK

Authentication in Cloud

Cloud authentication makes sure that the user who is accessing the data is the authorized user. This is very crucial because cloud has sensitive data, files and other information which should be accessed by authorized user. We can protect the cloud data by authenticating the user who is accessing the cloud. This can be done by single identity verification, two factors or multiple factors authentication, Certificate based authentication.

1. Single identity Authentication: It will require username and password.
2. Two factor Authentication: Here authentication requires two steps. First is password verification and second can be knowledge factor or possession factor. One example can be OTP sent to mobile.
3. Multi factor Authentication: Here third factor is added which is a inherent factor (unique to user). This includes biometric verification like fingerprints, eye, facial etc.
4. Certificate based authentication: User has to provide digital certificate which crosschecked with trusted authority who has issued it.

Authentication in Cloud

After successful authentication, Authorization comes into picture. Authorization controls access rights of user for accessing the resources. One example is someone has logged in to a cloud computing system then the system may want to identify what resources the user can be given during this session. Authorization can see as both the preliminary setting & permissions given by a system administrator. E.g Oracle [4]provides Oracle vault to secure administrative data.

Encryption

Cloud encryption is transforming the cloud data into ciphertext. Ciphertext [5]is encrypted text. Plain text is what we have before encryption and cipher is after encryption. Cipher is decrypted at the receiving side. The data which is stored in cloud is in encrypted format so that it could not be modified or read at the data center. Encryption provides data security and integrity. Encryption level is related to level of sensitivity of the data.

Access Control

Access control is providing security to resources and data. It is more than controlling the users. Access control manages users, files, other resources. It is a multi step process. Before accessing any resource, authentication and authorization is done. Various access control mechanisms such as firewall, Intrusion detection and segregation of duties are enabled at various layers of the network and cloud. . The firewall is deployed in the network to allow only the filtered contents to pass through which can be set up by the users based on a certain set of policies. On accessing certain sites, automatic email will be send to the monitoring team. In this method, a threshold value on the various IP addresses of certain sites is set. Once the value has exceeded beyond its limits ,an SMS or email will be send to the nominated group. A log is maintained on the various visited sites.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

VII. CONCLUSION AND FUTURE WORK

Cloud computing is emerging technology. Cloud computing is boon for information technology field, business and various other applications. Cloud offers benefits such as scalability, elasticity, multi-tenancy, cost effectiveness and reliability. Data security and privacy are the main obstacles in cloud computing. A number of techniques are provided for data protection and security. More work has to be done to make the techniques more effective. This paper present common mechanism for data security.

REFERENCES

[1] P. Mell and T. Grance, "The nist definition of cloud computing," National Institute of Standards and Technology, vol. 53, no. 6, article 50, 2009. View at Google Scholar
[2] Cloud Security Alliance (2010) Top Threats to Cloud Computing V1.0. Available: https://cloudsecurityalliance.org/research/top-threats
[3] http://www.cert.org/insider_threat
[4] J. B. Bernabe, J. M. Marin Perez, J. M.Alcaraz Calero, F. J.Garcia Clemente and G. M. Perez,"Semantic-Aware –multitenancy-authorization system for cloud architectures", Future Generation Computer Systems,(2014),vol.32, pp.154-167
[5] http://whatis.techtarget.com/definition/ciphertext#(*Contributor(s):* Ramesh B Kothamasu *last updated in* June 2007)

BIOGRAPHY

Vinayak D. Shinde is H.O.D. of Computer Engineering Department in Shree L.R. Tiwari College of Engineering, Mira Road, Thane-401107.

Jyoti V. Jadhav is M.E. Scholar Computer Engineering Department in Shree L.R. Tiwari College of Engineering, Mira Road, Thane-401107.

Pallavi K.Bhoir is M.E. Scholar Computer Engineering Department in Shree L.R. Tiwari College of Engineering, Mira Road, Thane-401107