www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 4 Issue 7 July 2015, Page No. 13284-13288

Cloud Database Storage Model by Using Key-as-a-Service (KaaS)

J.Sivaiah[1], Dr.K.Venkataramana[2]
[1]M.Tech scholar, Dept of Computer science and Engineering,
KMM Institute of Technology and Science, Tirupathi
Jmssivaji99@gmail.com

[2]Associate Professor, Dept of Computer Science and Engineering,
KMM Institute of Technology and Science, Tirupathi
Ramanakv4@gmail.com

Abstract: - In this paper we have studied about issues related to authenticity, integrity and security of data storage in cloud data centres. Security in cloud is under scanner due to which its adoption by IT sector is in slow stride. Using Cloud Storage, users can remotely store their data at less cost per byte and access services with high quality from a shared pool of configurable computing resources, without Operational Expenditure and Capital Expenditure. In cloud environment client's data is stored outside the organization premises which make client insecure regarding his data at cloud storage facility as it may be accessed and modified by unauthorized users. So in this paper we have proposed a model Securing Cloud Data using Key as a Service (SCDKS) which will provide authenticity for accessing data at storage by providing keys to access file/data. CSP will authenticate every user by generating keys by Key as a Service (KaaS), KaaS will generate a unique key for every session dynamically when user wants to access data at cloud. Since key is generated for each session it cannot be used by other users or data cannot be accessed by them which ensure security, integrity to data. A sophisticated and threshold key generation algorithm is used in KaaS for generating keys for users after authenticated by Cloud Service provider.

Key words: - Cloud storage, Key as a Service, securing cloud, Session, data authenticity and Integrity.

1. Introduction

The cloud is a storage area and deliveries of service that are programmed are share in hard ware devices and different sizes and different speeds and whenever it needed to pay services. This is also maintaining centralized server and cloud computing is internet based computing.

The cloud computing is a self service storage device and cloud will provide services authorized users so it can contain self storage device is provide data integrity, storage security, sharing at multiple authenticators. Cloud server maintains data centralized server, low cost, reducing time complexity of cloud database storage. It is a self replica [1].

1.1. Service models

Once a cloud is established, how its cloud computing services are deployed in terms of business models can differ depending on requirements. The primary service models being deployed.

- ✓ Saas
- ✓ Paas
- ✓ Iaas

1.1.1 Software as a service :(saas)

Saas is a purchases the ability to access and use an application or service that is hosted in the cloud. Sequence for communication where indispensable in between the purchaser and the service is hosted as a part of the service in the cloud [2].

1.1.2. Platform as a service :(paas)

Consumer purchases access to the platform, enabling them to deploy their own software and applications in the cloud.

The os and access are not managed by the consumer and there might be constraints as to which application can be deployed.

1.1.3 Infrastructure as a service :(Iaas)

Consumers control and manage the systems in terms of the operating systems, application, storage, and network connectivity, but do not they control the infrastructure.

Microsoft:

Has micro soft share point online services that allows for content and business intelligence tools to be moved into the cloud, and micro soft currently makes office application available in a cloud.

Sales force .com:

Runs its applications set for its customers in a cloud, and , its force.com and vm force.com products provide developers with plat form to be build customized cloud services.

Characteristics:

- ✓ Shared infrastructure
- ✓ Dynamic provisioning
- ✓ Network accessing
- ✓ Managed metering

Shared infrastructure:

Users a virtualized software models, enabling the sharing of physical service, storage, and networking capabilities.

Dynamic provisioning:

Allows for the provision of services based on current demand requirements this is done automatically using software automation, enabling the expansion and constriction of service capabilities, as needed.

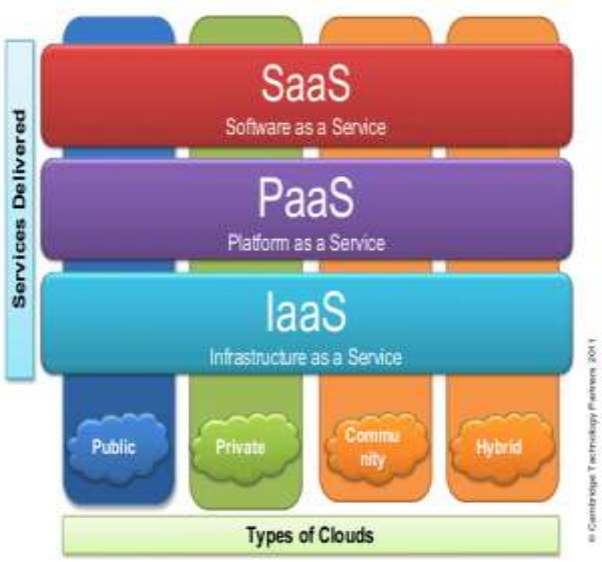
Network access:

Internet from needs to be accessed across the broad range of devices such as pcs, laptops, and mobile devices, using standard based API [2].

Managed metering*:*

Users metering cloud storage service for managing and optimizing cloud service and to make available treatment and information.

Layered cloud architecture:



End user application is delivered as a service platform and infrastructure is abstracted and managed. Application platform onto which custom application and services can be deployed, services need to be supported and managed. Physical infrastructure is abstracted to provide computing, storage, and networking as a service [3].

Deployment models:

- ✓ Private cloud
- ✓ Community cloud
- ✓ Public cloud
- ✓ Hybrid cloud

Private cloud:

The cloud infrastructure has been deployed, and is maintained and operated for a specific organization. The operation may be in-house or with a third party on the premises.

Community cloud:

The cloud infrastructure is shared a among a no. of organization with similar internets and requirements. This may help limit the capital expenditure costs for its establishments as the costs are shared among the organization. The operations may be in-house or with a third party on the premises.

Public cloud:

The cloud infrastructure is available to the public on a commercial basis by a cloud service provider. This is very little financial outlay compared to the capital expenditure requirements normally associated with other deployment options [4].

Hybrid cloud:

The cloud infrastructure consists of a no. of cloud of any type, but the clouds have the ability through their interfaces to allow and or applications to be moved from one cloud to another cloud. This can be a combination of private and public cloud that support the requirements to retain some data in an organization, and also the need to offer services in the cloud.

Benefits:

- ✓ Cost saving
- ✓ Scalability/flexibility
- ✓ Reliability
- ✓ Maintenance
- ✓ Mobile accessible

Cost saving:

Companies can reduce their capital expenditure and use operational expenditure for increasing their computing capabilities. This is a lower barrier to entry and also require fewer in-house it resources to provide system support.

Scalability/flexibility:

Companies can start with a small deployment and grow to a large deployment fairly rapidly, and they scale back if necessary. Also the flexibility of cloud computing allows companies to use extra resources at peak times enabling them to satisfy consumer demands.

Reliability:

Services using multiple redundant sites can support business continuity and disaster recovery.

Maintenance:

Cloud services providers do the system maintenance, and access is through API that does not require application installation into pcs, thus further reducing maintenance requirements.

Mobile accessible:

Cloud infrastructure available from Systems accessible mobile workers having storage service increased mobile productivity due to anywhere.

2. literature survey:

2.1. Issues of security:

Perhaps two of the more "hot buttons" issues surrounding cloud computing relates to storing and security data, and monitoring the use of the cloud by the service providers. These issues are generally attributed to slowing the deployment of cloud service. These challenges can be addressed, for example, by storing the information internal to the organization, but allowing to be used in the cloud. For to occurs, though, the security mechanisms between organizations and the cloud need to be robust and a hybrid cloud essential support such a deployment. . Present survey on the paper is security issues in cloud computing the security was feasible to technically, economically, and business oriented [5] [6]**.**

2.2. Techniques for protecting data in the cloud:

Traditional model of data protection have often focused on the network-centric and perimeter security, frequently with devices such as firewalls and intrusion detection system. But this approach does not provide sufficient protection against APTs privileged users or other insidious types of security attacks.

It's critical that CISO implements a data security strategy that provides a variable firewall around the data itself for comprehensive protection. Advanced data security solutions provide CISO with an early warning system about attacks, render the content unusable and leverage automation and big data analytics to continuously analyze logs and other information about their environment such as security events and data flow. While many organizations have implemented encryption for data security, they often overlook inherent weaknesses in key management, access control, and monitoring of data access, if encryption keys are not sufficiently protected, they are vulnerable to theft by malicious hackers. Vulnerability also lies in the access control model, thus, if keys are appropriately protected but access is not sufficiently controlled or robust, malicious or compromised personnel can attempt to access sensitive data by assuming the identity of an authorized user. The encryption implementation must incorporate robust key management solutions to provide assurance that the keys are sufficiently protects [5] [6]. It's critical to audit the entire encryption and key management solutions. Encryption works in concern with other core data security technologies, gleaning increased security intelligence, to provide a comprehensive multilayered approach to protecting sensitive data and mitigate risk in or out of the cloud. Therefore any data-centric approach must incorporate encryption, key management, strong access controls, and security intelligence to protect data in the cloud and provide the requisite level of security. By implementing a layered that includes these critical elements, organization can improve their security posture more effectively and efficiently then by focusing exclusively on traditional network-centric security methods. The strategy should incorporate a blue print approaches that addresses compliance requirements and actual security threads. Best practices should include securing sensitive data, establishing appropriate separations and IT security, ensuring that the use of cloud data confirms to existing enterprise policies as well as strong key management and strict access policies. It is important to

utilize security controls that protect sensitive data no matter where it lives, as point solutions by their very nature provide only limited visibility they are [6].

- ✓ Data lock down
- ✓ Access policies
- ✓ Security intelligence

First, make sure that data is not readable and that the solutions offer s strongly key management. Second, implement access policies that ensure only authorized users can gain access to sensitive information. Third, incorporate security intelligence that generates login information, which can be used for behavioral analysis to provide alerts that trigger when user are performing actions outside of the norm.

Cloud computing utilizes three delivery models by which different types of services are delivered to the end user. The three delivery models are the SaaS, PaaS and IaaS which provide infrastructure resources, application platform and software as services to the consumer. These service models also place a different level of security requirement in the cloud environment. IaaS is the foundation of all cloud services, with PaaS built upon it and SaaS in turn built upon it. Just as capabilities are inherited, so are the information security issues and risks. There are significant trade-offs to each model in the terms of integrated features, complexity vs. extensibility and security. If the cloud service provider takes care of only the security at the lower part of the security architecture, the consumers become more responsible for implementing and managing the security capabilities [6].

3. Proposed model

In the proposed Model Securing Cloud Data using Key as a Service (SCDKS) shown in figure-1 which allows user to authenticate with CSP which in turn allow user to use keys generated by Key as a Service for accessing requested data.

1. Client requesting data from cloud will send request to CSP by sending his A_{id} and information about data it want to access in cloud (Di).

2. CSP will send KSA_{id} to client which allows client to connect to Key-as-a-Service for obtaining keys to access data Di at Cloud data server.

4. Client will send request for Data key D_{ki} to Key-as-a-Service (KaaS) by sending KSA_{id} which in turn checks authenticity of client.

5. After authenticating by server (KaaS), it will send D_{ki} to client to accessing data at data server in cloud.

6. Finally client will send key D_{ki} along with Di to data server at cloud to access data, which in turn data server initializes a session after successful verification and sends requested data until session expires.

Thus above proposed model provides a three layered security approach to provide authenticity and integrity to data at cloud.

Security provide key as a service layer of cloud in this model to be implemented in securing cloud database storage (SCDBS). Mainly security is drawback of cloud service provider (CSP) so that have to overcome and implement key as a service in cloud storage device

The SCDKS contains three modules such as Authentication module, Key management module, Key verification and session establishment model.

3.1. Authentication module:

In SCDKS Authentication of client is done by CSP by verifying A_{id} and file/data permissions to access in cloud data server. After verification by CSP an authentication-Id (KSA_{id}) is sent to client for accessing KaaS server for keys to access file at data centre . Client will sent (KSA_{id}) to KaaS centre for requesting keys to access file/data in data centre. At KaaS center clients authenticity is verified again for key generation.

3.2. Key Generation module:

At the key generation centre KaaS will authenticate clients id (KSA_{id}) and executes key generation algorithm based on clients information for generating keys D_{ki} to access file/data that he want to access.

3.3 Data access module:

Cloud storage provides data storage where the digital data is stored in logical pools, the physical storage spans multiple servers (and often locations), and physical environment is typically owned and managed by a hosting company. These cloud storage providers should ensure security and integrity for client's data. So in our SCDKS before accessing data clients authenticity is verified twice and data is decrypted by using keys D_{ki} generated by KaaS. Any unintended changes to data as the result of a storage, retrieval or processing operation, is not possible since only an authorized user can access data by providing keys. If the changes are the result of unauthorized access, it may also be a failure of data security.

Conclusion

In this paper, we have studied about various issues relating to data storage security in cloud and proposed a model Securing Cloud Data using Key as a Service (SCDKS) which proposes new mechanism for authenticating and accessing data at data centre by using keys generated by KaaS. In SCDKS model client is authenticated multiple times to ensure his authenticity so unauthorized person may not access or modify at cloud data centre. In future works a new threshold key generation algorithm will be given.

References

[1] Cloud Security Alliance, "Top Threats to Cloud Computing, "http://www.cloudsecurityalliance.org, 2010.

[2] Q. Wang, C. Wang, K. Ren, W. Lou, and J. i,"Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing, IEEE Transactions on Parallel and Distributed Systems, vol. 22, no. 5,
pp. 847–859, 2011.

[3] Y. Zhu, G.-J. Ahn, H. Hu, S. S. Yau, H. G. An, and S. Chen, "Dynamic Audit Services for Outsourced Storage in Clouds," IEEE Transactions on Services Computing, vol. 6, no. 2, pp. 227–238, 2013.

[4] B. Wang, B. Li, and H. Li,: Public Auditing for Shared Data with Efficient User Revocation in the Cloud," IEEE Transactions on Services Computing, doi: 10.1109/TSC.2013.2295611, 2013.

[5] G. Ateniese, and S. Hohenberger, "Proxy Re-Signatures: New Definitions, Algorithms, and Applications," in: Proceedings of the 12th ACM
Conference on Computer and Communications Security (CCS 2005),2005, pp. 310–319.

[6] H. Wang, "Proxy Provable Data Possession in Public Clouds," *IEEE Transactions on Services Computing*, [online] ieeexplore. ieee.org/stamp/stamp.jsp?tp=&arnumber=6357181, 2012.

[7] K. Yang and X. Jia, "An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing," *IEEETransactions on Parallel and Distributed Systems*, [online] ieeexplore.
ieee.org/stamp/stamp.jsp?tp=&arnumber=6311398, 2012.