Advances in Computer Science and Information Technology (ACSIT)
p-ISSN: 2393-9907; e-ISSN: 2393-9915; Volume 3, Issue 1; January-March, 2016, pp. 42-46

http://www.krishisanskriti.org/Publication.html

Analysis on Security in Cloud and Sky Computing

Shilpa M. Satre[1] and Vaishali P. Jadhav[2]

[1,2]Saraswati College of Engineering, Kharghar, Navi-Mumbai, India
E-mail: [1]shilpa.m.shelar@gmail.com, [2]vaishalijadhav_2000@yahoo.com

Abstract—*Typically cloud computing is a combination of computing recourses accessible via internet. Historically the client or organizations store data in data centers with recall and other security techniques used to protect data against intrudes to access the data. However in cloud computing, since the data is stored anywhere across the globe, the client organization has less control over the stored data. To build the trust for the growth of cloud computing the cloud providers must protect the user data from unauthorized access and disclosure. A trusted 3rd party cloud provider is used to provide security services, while the other cloud provider would be data storage provider. The trusted 3rd party security service provider would not store any data at its end, and it's only connected to providing security service. The application or software will provide data integrity verification by using hashing algorithm like SHA-1, provide encryption/decryption using symmetric algorithm like AES, and defining band of people who can access the shared data securely can be achieved by defining access list. In this security aspect we discussed security on cloud and sky computing environment. Sky computing is related to multi-cloud security and addresses possible solutions. It is found that the research into the use of multi-cloud providers to maintain security has received less attention from the research community than has the use of single clouds. This work aims to promote the use of multi-clouds due to its ability to reduce security risks that affect the cloud computing user.*

1. INTRODUCTION

With evolution of computers the life of people became more and more easily. They are able to keep the data on their devices, and started finding ways to make them accessible to others, for example say by using floppy, writable disks, which was followed by portable hard-disk, all these where expensive in the own way during time. As the world of computing got more advanced the ways for sharing data started to becoming cheaper. In recent years a new term has evolved call "Cloud" which is provided by different providers, and which is nothing but facility or service of different resources or components like hard-ware, platform, storage's, software etc [1], and it is gaining importance because it frees the user from maintenance perspective on a investment of some money for the use of these services provided by cloud service providers. Now to provide such service to the client, naturally the provider's must have and rather can have access to resources which are used by the people/clients. Among the reasons these access are greatly required are for maintenance perspective. And definitely since billions of clients will be thinking about using such service, the infrastructure ought to be capable enough to support them, and these resources ought to be shared between billions of client's. Service availability, data synchronization between different devices, availability of data via any devices which includes browser facility makes cloud more attractive [2]. Now since the info gets shared or stored in provider's area, the client gets worried about privacy of its data, although there are certain agreements and SLA which are agreed by cloud provider and client. Now although client has a platform to generally share the info, the expense of securing his/her data or in a nutshell making its data private gets costlier.

The cloud term is of interest not just to the patient clients but to organizations as well. With organization as a consumer the concern of data security becomes multirole. Consider a typical example of small scale business that has different departments like HR, Finance, etc. We will focus on maintenance department since maintenance details of any business, company, or organizations which are considered to be very sensitive and must be confidential. Therefore if the little scales company thinks of using the cloud services like storage. Storing all account maintenance related information in cloud stored makes it prone to leakage of sensitive information tells un-authorized users. Therefore securing this maintenance data is vital before it gets uploaded to the storage cloud, and just in case the data stored in cloud storage gets tampered there should be a method to verify the integrity of the data, moving further specific band of people should have access to this data which may be folks from maintenance department of client company or special auditors. Simply speaking the client must have the ability to store the data securely, verify the integrity of the data, and share the data securely with specific band of people [3-4].

2. PROBLEM STATEMENT

The clients concern about data security, data integrity, and sharing data with specific band of men and women must be addressed. You can need multiple means of achieving this, example encrypting data on client machine and then storing the information to cloud storage server, computing hash of the information on client machine and storing hash of data in client machine, client trying out the responsibility of sharing the trick key about encryption with specific band of people.

Therefore it becomes more tedious for client to keep these information and share such information, more over in the event the device which stores such information is lost or stolen it pose a threat to the total data. Another way could be same storage cloud provider providing the service for secured sharing, hashing, encryption/decryption, but since administrative can have use of both services for maintenance; the security service provided by the cloud storage provider, the information might be compromised. The aforementioned approaches burdens the client by which makes it additionally accountable for securing it data before storing it to the cloud storage.

3. OBJECTIVES

Our objective is to build a security service which will be provided with a trusted 3rd party, and would lead to providing only security services and wouldn't store any data in its system.

1. To construct Web service system which would provide data integrity verification, provide encryption and decryption of the consumer data.
2. Defining access list for sharing data securely with specific band of individuals.
3. To construct thin client application which would call this web service before uploading downloading the data to and from cloud.
4. Migration of cloud computing from single to multi-clouds to ensure the Security of the user's data in sky environment.

4. LITERATURE SURVEY

The an1alysis behind this topic could be subdivided into 4 different sub fields:

1. Study of cloud computing and various cloud computing models IaaS, PaaS, SaaS etc, study of different business models, and study of service level agreements.
2. Study of security issues in cloud.
3. Study of Cryptography [5].
4. Study of single to multi-cloud (sky computing) environment [6].

4.1 Overview of cloud

Cloud computing describes the combination of logical entities like data, software which are accessible via internet. Client data is generally stored in banks of servers spread across the globe. The client machine would demand a browser to get into this server functionality, and would use client CPU and memory for processing.

Cloud computing will vary from traditional client-server model by providing applications from the server which are executed and managed by a client's internet browser, with no installed client version of a credit card application require. Cloud providers free the client from software license management etc, since the services are accessible via internet. Software as a Service (SaaS), given by cloud company, require browser enabled devices like personal computers, laptops, and latest devices like smart-phone, tablets etc, to access these services once an individual is registered in cloud [7]. For instance, in case an individual opts for storage service from the cloud provider, then she or he can upload personal information, code, music, movies, songs, photographs, which are stored anywhere across the planet in the server bank under Cloud Company, the geographic storage location is generally kept unknown to the user. Since only browser enabled device are sufficient to access these les, different devices could be kept in synchronization.

4.1.1 Working of cloud

Generally the cloud services are browser based, therefore any browser enabled device such as for instance laptop, desktop, Smartphone, tablets can used to gain access to these services, the services at providers end may be hosted on any platform, from windows, Linux, etc, which are accessible via internet. As an example consider a regular income and expenditure application which gives different analysis on expenditure by a person, this application could be executing on cloud providers server, whilst the client browser will allow client to feed in the inputs and visualize the analysis prepared for the inputs provided, these analysis computation is completed at server side. Suppose this application can further create documentation on monthly bases which often can be stored in cloud storage once again relieving the client from storing or processing the le on its side. Because the cloud services are provided via internet, significant factors which play an important role in performance are speed of internet, processing power of the individual [8].

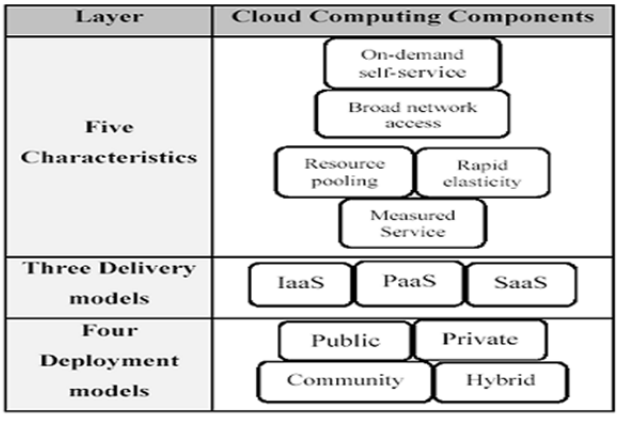

Fig. 1: Cloud Environment Architecture

This Cloud Environment Architecture provides how cloud divides and works on the basis of user requirement. While the cloud providers have server banks, to boost the processing

power, multiple server are often used internally by the cloud service providers. This pooling is invisible to the client. On another hand if these heavy tasks were to be executed on client side, it would require investment in hardware, time. Due to cloud, it frees the client from buying expensive hardware and investing his valuable time, since time is money. Having studied the overview of working cloud, let's now understand some of the essential characteristics.

- **On-the- y service**

A consumer can require more capabilities at any movement of time, example processing power for huge task, and this requirement must have fulfilled without Human intervention and be invisible to client.

- **Wide Accessibility**

Generally the cloud service are available via standard network protocols, it promotes different types of clients platforms (like, smart phones, laptops etc) for accessing these services.

- **Pooling Of Resources**

The pooling of the resources at cloud providers end is invisible to the end client, and resource assignment is done dynamically depending the need of the client.

- **Measured service**

Cloud has enough resources, and amount used by each client is measured by metering capability, and controlled at some level, for optimized resource usage, (like storage) [8-9].

4.1.2 Cloud Layers

At high level, cloud computing architecture can be partitioned into

1. Client or front end platform (thin or thick client).
2. Back-end platform (storage server etc).
3. The network (Internet etc)

These client platforms communicate with the cloud data storage via an application (hosted on middleware), accessible via a browser.

4.1.3 Cloud Service Models

In this section let's understand different service models of cloud.

- **SaaS**

Software as a Service (SaaS) also known as \on-demand software", as it name says allows client to use software services supplied by cloud provider via web browser. The management of server, internal cloud network, operating system, application configuration on middleware is responsibilities of cloud provider. Sales Force is among SaaS Company which supplies different software services.

- **PaaS**

Platform as a Service (PaaS) as the names suggests, cloud provider provides platform for deployment of user application, but doesn't give control of underlying hardware or infrastructure (storage, network).

- **IaaS**

Infrastructure as a Service (IaaS) is the limited accessibility for group of infrastructure is provided to the client for storage, network, processing etc. The client can deploy and execute is application using these infrastructure, the key advantage is frees the client on buys or purchasing top end servers, software's, data centre space, network infrastructure etc. The clients are charged on per-use basis [10].

4.1.4 Cryptography

Cryptography is a field of computer science & mathematics which deals with information security and related issues, in particular encryption and authentication. In Greek the word krypton mean "hidden" while the word graphein mean "to write". During encryption a plain-text is converted into cipher text, while the reverse process termed as decryption converts the cipher text into plain-text. The cipher is in unreadable format.

- **AES**

The Advanced Encryption Standard (AES) is a symmetric key encryption/decryption algorithm for converting plain-text to cipher text and vice-versa. Since the same key or master key is used, the must be kept secret or with trusted 3rd party, because compromise of this key would mean compromise to the data.

- **De e Hellman**

De e Hellman key exchange is a technique to exchange cryptographic keys between 2 parties with no prior knowledge of each other. It allows the 2 parties to establish a secret key which can be used for further secured communication.

- **SHA-1**

SHA stands for "Secure Hash Algorithm", SHA-1 is a cryptographic hash function technique where hash of data is computed. As compared to SHA-0, SHA-1 is widely used because it corrects errors in SHA hash specification, which led to weakness [11].

4.2 Sky Computing Environment (Single to Multi-clouds systems)

The Sky Computing term is "multi-clouds" which is similar to the terms "inter-clouds" or "cloud-of-clouds". These terms suggest that cloud computing should not end with a single cloud. Using their illustration, a cloudy sky incorporates different colors and shapes of clouds which lead to different implementations and administrative domains.

4.2.1 DepSky System: Multi-Clouds Model

The DepSky architecture consists of four clouds and each cloud uses its own particular interface. The DepSky algorithm exists in the clients' machines as a software library to communicate with each cloud. These four clouds are storage clouds, so there are no codes to be executed. The DepSky library permits reading and writing operations with the storage Clouds.

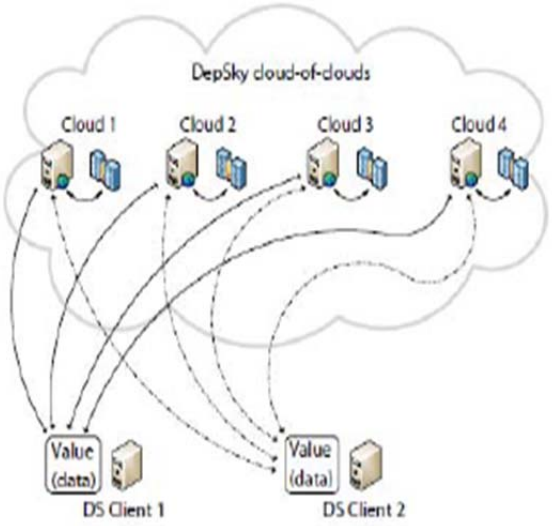

Fig. 2: Dep-Sky Architecture

DepSky Data model: It include three abstraction levels which are Conceptual data unit Generic data unit and Implementation data unit.

DepSky system model: It contains three parts: readers, writers, and four cloud storage providers, where readers and writers are the client's tasks. Readers can fail arbitrarily (for example, they can fail by crashing, they can fail from time to time and then display any behavior) whereas, writers only fail by crashing.

HAIL (High Availability and Integrity Layer): is another example of a protocol that controls multiple clouds. HAIL is a distributed cryptographic system that permits a set of servers to ensure that the client's stored data is retrievable and integral. HAIL provides a software layer to address availability and integrity of the stored data in an inter-cloud.

4.3 Security Risks in Sky Computing

In different cloud service models, the security responsibility between users and providers is different. The impact of security issues in the public cloud is greater than the impact in the private cloud. For instance, any damage which occurs to the security of the physical infrastructure or any failure in relation to the management of the security of the infrastructure will cause many problems. In the cloud environment, the physical infrastructure that is responsible for data processing and data storage can be affected by a security risk. Hence security is very important factor in sky environment because one virtual machine security directly depends on other model which are connected internally each other.

4.3.1 Security Risks in Sky Computing

1. Data Integrity: the data stored in the cloud may suffer from damage during transition operations from or to the cloud storage provider.

2. Data Intrusion: The stolen password allows the hacker to erase all the information inside any virtual machine instance for the stolen user account, modify it or even disable its services.

3. Service Availability: The user's web service may terminate for any reason at any time if any users files break the cloud storage policy.

4.3.2 Solutions of Security Risks

In order to reduce the risk in cloud storage, customers can use cryptographic methods to protect the stored data in the cloud. Using a hash function is a good solution for data integrity by keeping a short hash in local memory. In this way, authentication of the server responses is done by recalculating the hash of the received data which is compared with the local stored data. If the amount of data is large, then a hash tree is the solution. Many storage system prototypes have implemented hash tree functions, such as SiRiUS. The literature survey helped us gain a better insight with reference to cloud computing, Different models of cloud computing, current security issue. Understanding different encryption/decryption algorithms like AES, SHA-1, De e Hellman. During the survey it is noted that lot of research is going on in cloud computing security issues and how to overcome the security issues and to gain cloud users confidence.

5. CONCLUSION

We have seen how delegation of responsibility trusted 3rd party which provides security services secures user data. It reliefs the client from maintaining any kind of key information and allowing the client for using any browser enabled device to access the cloud services. It allows the client to verify the integrity of the data stored on download or retrieval of its own stored data in cloud. The client can share the data securely with specific band of people without any overhead of key distribution.

It is clear that although the use of cloud computing has rapidly increased; cloud computing security is still considered the major issue in the cloud computing environment. Customers do not want to lose their private information as a result of malicious insiders in the cloud. In addition, the loss of service availability has caused many problems for a large number of customers recently. Furthermore, data intrusion leads to many problems for the users of cloud computing.

The purpose of this work is to survey on single clouds computing and multi-clouds (sky) computing to address the security risks and solutions. We have found that much research has been done to ensure the security of the single cloud and cloud storage whereas multi-clouds have received less attention in the area of security. We support the migration to multi-clouds due to its ability to decrease security risks that affect the cloud computing user.

6. FUTURE WORK

We aim to provide a framework to supply a secure cloud database that will guarantee to prevent security risks facing the cloud computing community. This framework will apply multi-clouds and the secret sharing algorithm to reduce the risk of data intrusion and the loss of service availability in the cloud and ensure data integrity. In relation to data intrusion and data integrity, assume we want to distribute the data into three different cloud providers, and we apply the secret sharing algorithm on the stored data in the cloud provider. An intruder needs to retrieve at least three values to be able to find out the real value that we want to hide from the intruder.

1. To enhance the security more, a mechanism to secure the keys in security cloud can be area of research.
2. To reduce the overhead of network track can be another area of research.

REFERENCES

[1] Jing-Jang Hwang, Hung-Kai Chuang,Yi-Chang Hsu, Chien-Hsing Wu, "A Business Model for Cloud Computing Based on a Separate Encryption and Decryption Ser-vice," Proceedings of the 2011 International Conference on Information Science and Application, April 2011.

[2] Qian Wang ,Cong Wang ,Kui Ren ,Wenjing Lou ,Jin Li, "Enabling Public Au-ditability and Data Dynamics for Storage Security in Cloud Computing", *IEEE Transactions on parallel and distributed systems*, VOL. 22, NO. 5, MAY 2011.

[3] Balachandra Reddy Kandukuri, Ramakrishna Paturi V, Dr. Atanu Rakshit, "Cloud Security Issues", *IEEE International Conference on Services Computing*, pp. 517-520, September 2009.

[4] Peter Mell, Timothy Grance, "The NIST De nition of Cloud Computing", *NIST Special Publication 800-145*.

[5] Ling Li, Lin Xu, Jing Li, Changchun Zhang,"Study on the Third-party Audit in Cloud Storage Service", 2011 *International Conference on Cloud and Service Computing* .

[6] L. M. Vaquero,L. Rodero-Merino,J. Caceres, and M. Lindner, "A break in the clouds: towards a cloud de nition", *ACM SIGCOMM Computer Communication Review*, vol. 39, no. 1, pp. 50-55, January 2009.

[7] A. Parakh and S. Kak, "Online data storage using implicit security", *Information Sciences*, vol. 179, issue 19, pp. 3323-3333 ,September 2009.

[8] C. Weinhardt, A. Anandasivam, B. Blau, N. Borissov, T. Meinl, W.Michalk, and J. Stober, "Cloud computing ? a classi cation, business models, and research directions", *Business & Information Systems Engineering (BISE)*, vol. 1, no. 5, pp.391-399, 2009.

[9] L. Lamport, "Password authentication with insecure communication", *Communi-cations of the ACM*, vol. 24, no. 11, pp. 770-772, 1981.

[10] "Announcing the ADVANCED ENCRYPTION STANDARD (AES)", Federal In-formation Processing Standards Publication 197. *United States National Institute of Standards and Technology (NIST).* November 26, 2001. Retrieved October 2, 2012.

[11] William Stallings, "Cryptography and Network Security", 2009.