RESEARCHERID
THOMSON REUTERS

[ICRTCET-2018]

ISSN 2348 – 8034
Impact Factor- 5.070

GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

SECURE CLOUD DATA STORAGE WITH CRYPTOGRAPHIC INTERVENTION FOR PREMIER ENTERPRISE DATA

Anitha K L[*1] & T.R. Gopalakrishnan Nair[2]

[*1]Research Scholar, Bharathiar University, Coimbatore, India
Networks and Security Research Group, Advanced Research Centre, Rajarajeshwari Group of Institutions, Bangalore, India

[2]Networks and Security Research Group, Advanced Research Centre, Rajarajeshwari Group of Institutions,Bangalore, India. Visiting Professor, NIAS, Bangalore, India

ABSTRACT

Cloud computing provides access to a vast set of resources like networking, processing, and services through the Internet. The data which is usually stored in computing environment at user end can be deployed on to the provider's server at any location. It has brought issues and challenges in security for the consumers and service providers. Mitigating security risks is crucial to construct a comfort level among the consumer and the provider, to realize a transition of applications and data on to the cloud. In this paper, we propose a workflow of the user accessing cloud service for secure data storage and for downloading the data.

Keywords: *- Deployment models; Data storage; Cloud service provider; Cryptography.*

I. INTRODUCTION

Cloud computing is a known model that is, widely used in any communication system. It is the new standard which provides a huge collection of computing resources with its dynamic scalability, computing power, storage, and platforms. With the advent of this technology, the sharing of resources can be increased. Based on the nature of data, the industries can choose private, public or hybrid clouds to deploy their applications. There are efforts from different parts of the world to have deeper level controls over the security of private data in various types of cloud architectures including public ones. Here we studied a deeper level interventional algorithm capable of providing user authenticity detection for access protocol over data kept at storage control and management levels of cloud governance. Cloud Architecture consists of applications that use computation and storage services on-demand to clients over the network and the supply of infrastructure which includes computational resources and storage resources. According to U.S. National Institute of Standards and Technology (NIST), “Cloud computing is defined as a model for enabling a convenient, on-demand network access to a shared collection of the configurable computing resources like, the networks, servers, storage, applications, and services that can be rapidly provisioned and released with minimal management effort or service provider interaction” [1].

ISSN 2348 – 8034
Impact Factor- 5.070

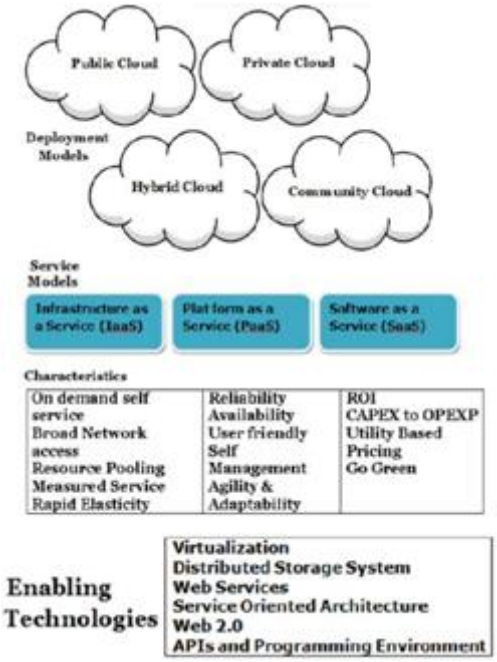

Fig. 1 Cloud computing representation

Fig 1 demonstrates the cloud computing representation, which can be mainly classified as deployment models and service models. The user can choose any deployment model like private, public or hybrid cloud to store their data. Instead of spending huge investments for the infrastructure, user can access the cloud service models like PaaS, SaaS and IaaS. A cloud data center is an infrastructure that supports Internet services from a variety of views, and the IaaS and PaaS categorize the most popular ones.

A. Deployment Models

The public cloud, community cloud, private cloud and hybrid cloud are the different deployment models of the cloud. According to the needs of the organization, they can select one among them.

TABLE I

Deployment Model	**User domain security issues**
Public cloud	High level
Private cloud	Medium level
Hybrid cloud	High level
Community cloud	High level

Table I shows user domain security issues of various deployment models.

Public Cloud: Public cloud offers a pool of computing services which is owned and functioned by a cloud provider. The public cloud is made available to the companies as payment basis. Security of the data is a key concern while using the public cloud.

Private Cloud: It is a cloud infrastructure which can be rented or owned and controlled solely by an enterprise. The users have to buy, deploy, manage and maintain them. It is more secure and more expensive if we compared it to the public cloud. Here in private cloud, there will be no extra protection guidelines, bandwidth limitations and the legal requirements as compared to the environment in public cloud. Eucalyptus Systems is an example of private cloud [2].

Hybrid Cloud: It is a combination of the more than one deployment models, connected in such a way that the transfer of data happens among them, without concerning each other. These clouds would normally be used by an organization, and the managerial tasks are divided, within a business organization and the cloud provider. Here an enterprise can summarize the objectives and requirements of the services [3].

The hybrid cloud is more secure compared to public cloud.
Community Cloud: It is shared by various companies designed for a shared reason and might be controlled via the company or a third party provider. It is usually based on conformity among the related enterprises such as educational institutions. A cloud environment can be hosted internally or externally.

B. Service Models
The three forms of services offered by the cloud provider: Platform as a Service (PaaS), Infrastructure as a Service (IaaS) and Software as a Service (SaaS). Cloud computing can be implemented exclusively for the enterprises to shift towards the IT solutions as they should pay for the resources which is used on utilization basis to improve business efficiency. Also, enterprises can effortlessly assemble the requirements of quickly varying markets in the corporate world to guarantee that they are forever on the foremost border for their users [4]. As with all cloud computing services it provides access to the computing resources in a virtualization environment.

IaaS delivers the computing resources in the form of virtualized hardware. In IaaS, provider assists the ability to the users for storage, processing, networks, and further the computing resources wherein, the customer can deploy and to interpret the software which consists of the applications and operating systems [5]. In this model, cloud providers have to offer a Virtual Machine Monitoring (VMM) environment and a trusted host for the consumers. Amazon Ec2 is an example of IaaS providers [6].

PaaS provides the computing platform and the runtime environment that enable developers to build customized applications and the services. The clients can be able to access the PaaS services hosted in cloud by a device which is internet enabled. PaaS allows the users to create any applications using the tools which are supplied by the provider. The features of PaaS consists of the Server-side scripting environment, devices for design and development, Database management system, Operating system, Storage, Network access, Hosting, Operating system.

SaaS can be depicted as a procedure through which the service provider hosts the applications and is made available to the customers with an internet connection. It eliminates a incredible amount of software maintenance; ongoing operation, protection and support [7]. It is compatible, and the applications can be accessed from anywhere if it is connected with the internet or from any internet enabled devices. Examples of SaaS include Google Apps, Salesforce.com.

SaaS is mainly suitable for companies wherein the processes are consistent. Even in plenty of companies, the users consider their methods are dissimilar and cannot be automated by the regulated application. If the enterprise people would take up consistent company processes and built-in SaaS applications which can automate those consistent processes wherein they would considerably pick up their production. Within the company's data center, the

ISSN 2348 – 8034
Impact Factor- 5.070

programs can be hosted and can be used by the client, and IT organizations should adopt internal or a private and public alternatives for the cloud computing, as their security necessities state [8].

II. CRYPTOGRAPHY

Cryptography is one of the special areas in the field of military and government services which can be extensively used for maintaining the privacy of data. It mainly offers the security credentials, such as confidentiality, integrity and availability of the data. Vernam one-time pad proposed by Gilbert Vernam, in 1917 is a well known symmetric algorithm

Here the secret key k is used once for enciphering a single message. For each and every message the key has to be renewed. One-time pads are completely secure wherein the encrypted message offers no information about the original message to a cryptanalyst. For sending each message Alice and Bob have to maintain a safe communication media to exchange the new secret key. In practice, this is not possible because they will be wasting partially of their communication time in exchanging the keys. However, the block cipher is used, which mainly rely on permutations. A block cipher is one in which a block of plain text is considered as a whole and is used to produce a cipher text block of equal length. We can use encryption algorithms for encrypting the data which is sensitive and then store on to cloud.

III. DATA STORAGE

Cloud data storage offers unlimited storage space for the consumer's data. The consumer can access data from anywhere with an internet enabled device at any time. We need to think regarding the security and privacy of the consumer's data which is stored on to the cloud. Users have no idea about what occurs within the cloud. Cloud data storage raises the risk of data leakage and unauthorized access. Transmitting the consumer's data on to cloud is risky due to the intruder's attacks. Data encryption acts a vital part in cloud computing environment to safeguard the end users data. Here we propose a workflow diagram for storing confidential data onto the cloud. The authorized user can avail the cloud services by means of pay-as-you-go model. Fig 2 shows the workflow of the consumer accessing cloud service for secure data storage.

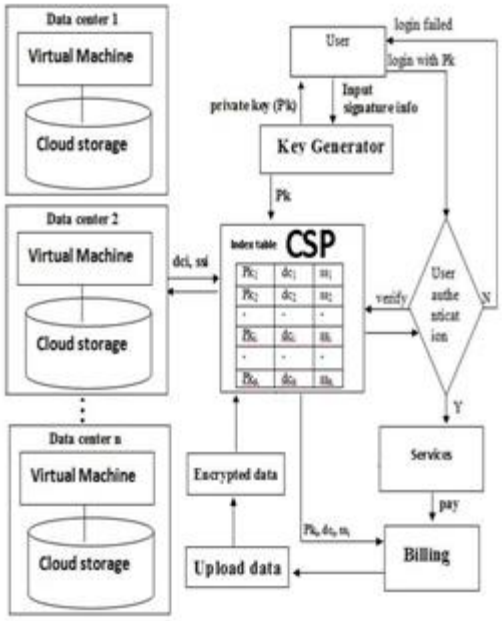

Fig. 2 Workflow of the consumer accessing cloud service for secure data storage.

ISSN 2348 – 8034
Impact Factor- 5.070

The user inputs the signature information to the key generator. The key generator generates a private key by taking signature information to numeric value and adds a random number by using a hash function and returns the private key (Pk) back to the user and also to the cloud service provider (CSP). The CSP maintains an index table which stores three attributes: the private key, data center id and storage space id. The private key is used to lock the storage space for a user called as logical locking maintained by using user encryption tags analysis. And the encrypted data will be managed by the logical manager. If the same user needs more storage space, later on, they can avail the storage space in the same data center if space is available. If not, the user gets additional space from any other data center which is recognized by the data center id. By maintaining the index table in CSP, fast retrieval of data is possible by identifying the data center located anywhere. Only the authorized user can access the storage space by using the private key. Moreover, the confidential data should be encrypted using various cryptographic standards.

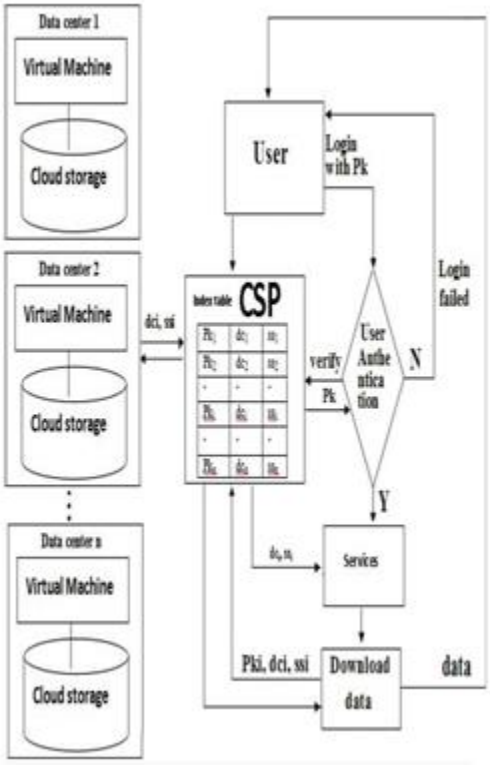

Fig. 3 Workflow of the consumer accessing cloud service for downloading the data

The users are concerned with the data security requirements like confidentiality, integrity and availability. To download the data, user has to login with his private key pk. The data center id and the storage space id will be identified by using this private key. The authenticated user can access the storage space and can download the data at anytime from anywhere. Fig 3 illustrates the workflow of user accessing cloud service for downloading the data.

ISSN 2348 – 8034
Impact Factor- 5.070

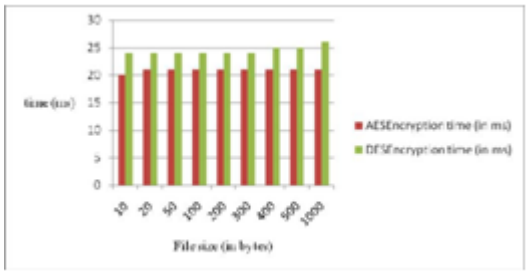

Fig. 4 AES and DES encryption time.

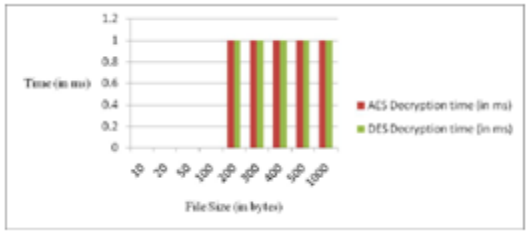

Fig. 5 AES and DES decryption time.

As per security concern the user is uploading the premier enterprise data only after encrypting it. Fig. 4 and Fig. 5 shows the encryption time and decryption time using various cryptographic algorithms like Advanced Encryption Standard (AES) [10] and Data Encryption Standard (DES) [11]. Less time is needed to encrypt the data using AES compared to DES. User can login using the private key and access the storage space and can download the encrypted data. Then the user can decrypt the data by using decryption algorithms.

IV. CONCLUSION

Cloud computing is a new standard in enterprise field wherein it contains the collection of resources which can be quickly provisioned through least management effort. In this paper, we presented issues in cloud computing such as security, service availability and authentication. User needs to concern about the data stored on to the cloud. Security of data is one of the most important issues when using cloud storage.

Workflow of the user accessing cloud service for secure data storage and for downloading the data has been discussed. The confidential data can be stored and retrieved from the cloud with proper authentication and encryption standards. We will make the actual design more practical and operational in the future. We propose to do so in the forthcoming endeavours.

REFERENCES

1. *NIST definition of cloud computing, http:// csrc.nist.gov/ publications/ PubsNISTIRs.html, 2007.*
2. *B. R. Kandukuri, R. Paturi V, A. Rakshit. "Cloud Security Issues", In Proceedings of IEEE International Conference on Services Computing, pp. 517-520, 2009.*
3. *Meiko Jensen, Jorg Schwenk, Nils Gruschka, Luigi Lo Iacon. On "Technical Security Issues in Cloud Computing", Proc. of IEEE International Conference on Cloud Computing (CLOUD-II, 2009), pp. 109-116, India, 2009.*
4. *A. Kundu, C. D. Banerjee, P. Saha. "Introducing New Services in Cloud Computing Environment", International Journal of Digital Content Technology and its Applications, AICIT, Vol. 4, No. 5, pp. 143-152, 2010.*
5. *Jianfeng Yang and Zhibin Chen. "Cloud Computing Research and Security Issues", in Computational Intelligence and Software Engineering (CiSE), 2010, pp. 1-3.*

6. *L. Savu. "Cloud Computing: Deployment Models, Delivery Models, Risks and Research Challenges", International Conference in Computer and Management (CAMAN), pp. 1-4., 2011.*
7. *R. L Grossman. "The Case for Cloud Computing", IT Professional, vol. 11(2), pp. 23-27, 2009, ISSN: 1520-9202.*
8. *Buyyaa, R., Chee Shin Yeo, Srikumar Venugopal, James Broberg, Ivona Brandic. "Cloud computing and emerging IT platforms: Vision, Hype, and Reality for Delivering Computing as the 5th utility", Future Generation Computer Systems (2009), doi:10.1016/j.future.2008.12.001.*
9. *https://en.wikipedia.org/wiki/One-time_pad.*
10. *N FIPS. 197: Announcing the advanced encryption standard (aes) Technology Laboratory, National Institute of Standards, 2009(12):8–12, 2001.*
11. *National Bureau Of Standards NIST. Data encryption standard (des). Technology,46-3(46):1–26, 1999..*