ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 2, February 2017

Security Issues, Research and Challenges in Cloud Computing

[1] NehaTyagi [2] Kishan Agarwal [3]NishantUpadhyay [4]Mukesh Kumar [5]Brij Bhushan Gupta [6] Deepak Kumar
[1] Assistant Professor [2][3][4][5][6]Student of B.Tech
[1][2][3][4][5][6] Department of Computer Science and Engineering
GL Bajaj Institute of Technology and Management, Greater Noida (India)

***Abstract:* -- Cloud was used in network diagrams wherever we need to represent connection between internet and computer system until 2008, many services were introduced to access the computer over the internet which was termed as cloud computing. Cloud computing involves various activities such as the use of social networking sites and other forms of interpersonal computing; but however, the term cloud computing was always concerned with the access of online software applications, data storage and processing power. Cloud computing could easily help in increasing the capability of a computer system or a network without expending a single penny in infrastructure, training a new individual or licensing new software. In this way it helps to extend the existing capabilities of Information Technology. In the last few years, cloud computing has got a rapid growth because of the facility it provides to its client. It is the fastest growing segment of the software industry. As we know that everything has its.**

I. INTRODUCTION

Cloud was used in network diagrams wherever we need to represent connection between internet and computer system until 2008, many services were introduced to access the computer over the internet which was termed as cloud computing. Cloud computing involves various activities such as the use of social networking sites and other forms of interpersonal computing; but however, the term cloud computing was always concerned with the access of online software applications, data storage and processing power. Cloud computing could easily help in increasing the capability of a computer system or a network without expending a single penny in infrastructure, training a new individual or licensing new software. In this way it helps to extend the existing capabilities of Information Technology. In the last few years, cloud computing has got a rapid growth because of the facility it provides to its client. It is the fastest growing segment of the software industry. As we know that everything has its good and as well as bad aspects, so, as more and more information of an individual or a company is placed in the cloud, concern regarding how secure the information is also gets into scope . Despite all these security issues in cloud, customers are still reluctant to deploy their business in the cloud. Security issues in cloud computing has played a vital role in slowing down its acceptance, in fact security ranked first as the greatest challenge issue of cloud computing.

II. SERVICES PROVIDED BY CLOUD[1]

2.1 SaaS(Software As A Service)

SaaS can be described as a process by which Application Service Provider (ASP) provide different software applications over the Internet. This makes the customer to get rid of installing and operating the application on own computer and also eliminates the tremendous load of software maintenance; continuing operation, safeguarding and support [3]. SaaS vendor advertently takes responsibility for deploying and managing the IT infrastructure (servers, operating system software, databases, data center space, network access, power and cooling, etc) and processes (infrastructure patches/upgrades, application patches/upgrades, backups, etc.) required to run and manage the full solution. SaaS features a complete application offered as a service on demand. Examples of SaaS includes: Salesforce.com, Google Apps.

2.2 PaaS(Platform As A Service)

"PaaS is the delivery of a computing platform and solution stack as a service without software downloads or installation for developers, IT managers or end-users. It provides an infrastructure with a high level of integration in order to implement and test cloud applications. The user does not manage the infrastructure (including network, servers, operating systems and storage), but he controls deployed applications and, possibly, their configurations. Examples of PaaS

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 2, February 2017

includes: Force.com, Google App Engine and Microsoft Azure.

2.3 IaaS(Infrastructure As A Service)

Infrastructure as a service (IaaS) refers to the sharing of hardware resources for executing services using Virtualization technology. Its main objective is to make resources such as servers, network and storage more readily accessible by applications and operating systems. Thus, it offers basic infrastructure on-demand services and using Application Programming Interface (API) for interactions with hosts, switches, and routers, and the capability of adding new equipment in a simple and transparent manner. In general, the user does not manage the underlying hardware in the cloud infrastructure, but he controls the operating systems, storage and deployed applications. The service provider owns the equipment and is responsible for housing, running and maintaining it. The client typically pays on a per-use basis. Examples of IaaS includes Amazon Elastic Cloud Computing (EC2), Amazon S3, GoGrid.

III. TYPES OF CLOUDS

3.1 Private Cloud

Private cloud belongs to the organisations itself or rented by a third party with the setup at on or off the premises. In terms of security it is more secure and expensive on the other hand. Since it is private so it does not have any legal issues or formalities like bandwidth regulations, infrastructure. Only client and the provider have the right to access the cloud and they have optimal control over their data in the cloud. One of the best examples of a private cloud is Eucalyptus Systems.

3.2 Public Cloud

As the name suggests the public cloud is available for more than one user and the whole setup is beyond the premise or beyond the firewall of the user or the client of the cloud service. Several enterprises work on the infrastructure provided, at the same time and users can dynamically provision resources. These clouds are in full control of the provider and the provider is also responsible for installation, management, provisioning, and maintenance. Customers are only charged and optimal amount of money by the provider so there are very less chances for the under-utilization of the cloud. Clients or consumers have very nominal or no control over the infrastructure, process etc. of the cloud hence they require very high security for their assets (data).Since it is available for public use hence neither any kind of authentication nor any authorisation could be applied on this model.Cloud services which are provided by giants like Amazon, Microsoft azure and Google have some restrictions over the user.

3.3 Hybrid Cloud

As the name suggests it is combinations of two more cloud models in such a way that data flow does not get affected even when any one cloud is used solitary. These clouds are typically created by the involvement of enterprise as well as management responsibilities aresplitted between the enterprise and the cloud provider. In this model, a company cancustomize the goals and services that it needs from the cloud. A meticulously developed hybrid cloud is able to provide better security services which are needed by the client such as payment-gateways, banking transactions regarding the payroll of the employees, enterprise etc. The major problematic issue that is faced by the hybrid cloud is the difficulty in effectively developing and managing such kind of solution. This kind of development requires developing such kind of services which are originating from different locations but the interaction between them must be so well established that they should appear as they are originating from a single source. This makes it difficult to develop a hybrid cloud.

IV. SECURITY ISSUES IN CLOUD COMPUTING

4.1 Data Security

A general user,can easily find a possible storage by those providers that give the cloud services.Hypertext Transfer Protocol (HTTP) is the most common communication protocol that is used utilize the services provided by the cloud service providers. For the security of the data onto the cloud Hypertext Transfer Protocol Secure (HTTPS) and Secure Shell (SSH) are used commonly. In a traditional on premise application deployment model, the sensitive data of each enterprise continues to reside within the enterprise boundary and is subject to its physical, logical and personnel security and access control policies [2]. But, in cloud computing, the organisation's data is stored outside itsboundary, i.e. at the Service provider end. So the service provider needs to perform more security checks to make confirm that the data of the client is secured by the different kinds of

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 2, February 2017

attacks for example an unauthorised access, biased employee etc. To protect this data from various kinds of security attacks or breaches strong encryption techniques for data security and very good authorization of data are needed. Cloud service providers such as Amazon, the Elastic Compute Cloud (EC2) administrators do not have access to customer instances and cannot log into the Guest OS. EC2 Administrators with a business need are required to use their individual cryptographically strong Secure Shell (SSH) keys to gain access to a host[2]. These kinds of access need a regular auditing an logging. When data is idle then it is not encrypted by any algorithm but users can encrypt it before uploading it to any cloud server like Google, Amazon etc. doing this makes it difficult for any unauthorised user to access the data.

4.2 Data Privacy

Privacy of data on the cloud is one of the major points which should be taken care of. Since data in could be accessed globally i.e. from any part of the world hence the data is also available globally which attracts our mind with respect to jurisdiction, privacy and exposure.There should be a separate committee which looks after whether the all the measures regarding the security of the data is taken or not by the client and the service provider as well. If any one of them is not fulfilling all those formalities then a strict actions must be taken against the one. Organisations have a risk of legal actions if they not comply with the government policy regarding the data kept on the cloud while as the provider will face a legal action if a client's data or any sensitive information is exposed. Virtual co-tenancy of sensitive and non-sensitive data on the same host also carries its own potential risks.[2]

4.3 Data Integrity

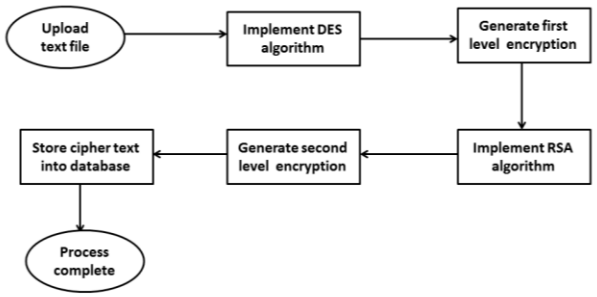
Data integrity means that it should be sent to the genuine receiver. Lack of data integrity may lead to data corruption so to overcome this problem data integrity monitor are setup in data centres to check whether integrity is maintained or not which is little cumbersome task. However if a system has a single database then its integrity could be maintained very easily. Integrity of data is maintained using some database constraints and ACID (Atomicity, Consistency, Isolation, and Durability) properties of any transactions. Most databases support ACID transactions and can preserve data integrity. Data generated by cloud computing services are kept in the clouds which mean the owner of the data loses some of the controls on one's own data and has to rely on the trust of the service provider for the security of the data who has all rights to access that data.

V. EXISTING SOLUTIONS

5.1 Encryption technique

As given in [3] the author is trying to implement multi-level encryption technique using DES (Data Encryption Standard) and RSA algorithm. After uploading the data onto the cloud storage first symmetric encryption technique DES is applied on the data followed by the RSA in second level.

STEP 1. Upload the plain text onto the cloud.
STEP 2. Apply DES to perform first level of encryption.
STEP 3. After applying the DES algorithm RSA algorithm is applied to achieve second level of encryption.
STEP 4. Cipher text which is generated after applying second and final level of encryption is stored into the database.
STEP 5. After storing the cipher text the process is finished. Now the data could be retrieved any time from the cloud by any authorised and authentic user of the data.
A block diagram (taken from [3]) of the encryption technique is given below:-



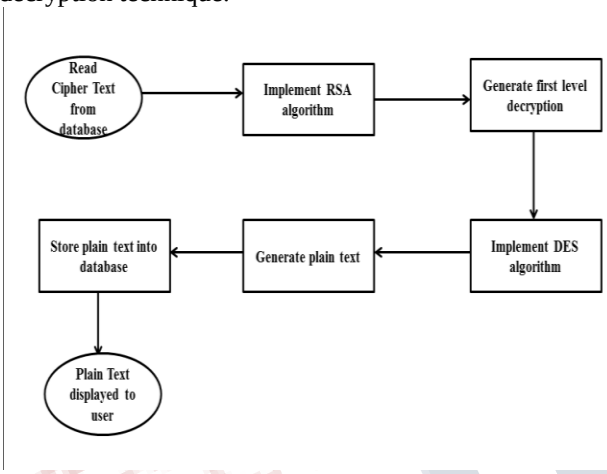
5.2 Decryption technique

The whole algorithm is reversed to get the original data from the cipher text following steps need to be taken:-

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 2, February 2017

STEP 1. Fetch the cipher text from the database which is needed to be translated.
STEP 2. To perform first level of decryption implement RSA algorithm to decrypt the second level of encryption.
STEP 3. After applying first level of encryption DES used to implement the second and final step of decryption and to translate the cipher text into the original data.
STEP 4. Store the plain text into the database.
The block diagram (taken from [3]) of the whole decryption technique:-



VI DRAWBACK IN THE PREVIOUS ALGORITHM

6.1 If somehow any attacker gets the key of the message then one would be able to attack on that message using the key.

6.2 Since all the encryption is being applied on the data therefore there are chances that if any unauthorised person gets the key of the message then one gets all the rights on the data that was intended for the receiver.

6.3 After getting the key the attacker can use various approaches to get the message. Brute force is of the example.

REFERENCES

[1] International Journal of Computer Networks (IJCN), Volume (3) : Issue (5) : 2011 Kuyoro S. O., Ibikunle F. &Awodele O.

[2] IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS) Vol. 1, No. 2, December 2011,Cloud Computing: Security Issues and Research Challenges,ISSN: 2249-9555.

[3] International Journal of Innovative Research in Computerand Communication Engineering(An ISO 3297: 2007 Certified Organization)Vol. 3, Issue 1, January 2015.

[4] Cloud computing security: The scientific challenge, and a survey of solutions-Mark D. Ryan (School of Computer Science, University of Birmingham, Birmingham B15 2TT, UK).

[5] A survey on security issues in service delivery models of cloud computing -S. Subashini N, V.Kavitha (Anna University Tirunelveli, Tirunelveli, TN627007,India).

[6] IJIRST –International Journal for Innovative Research in Science & Technology| Volume 2 | Issue 09 | February 2016 ISSN (online): 2349-6010 - Enhancement of Cloud Computing Security with Secure Data Storage using AES
Vishal R. Pancholi -Research Scholar (Pacific University Udaipur, Rajasthan)
Dr. Bhadresh P. Patel- I/C Principal (Matrushri L.J Gandhi (Bakorvala) BCA College Modasa, Gujarat)