International Journal of Current Trends in Engineering & Research (IJCTER)
e-ISSN 2455–1392 Volume 2 Issue 4, April 2016 pp. 84 - 92
Scientific Journal Impact Factor : 3.468
http://www.ijcter.com

DATA SECURITY IN CLOUD COMPUTING

Ch. Chakradhara Rao[1], A.V.Ramana[2]

[1]CSE Department, GMRIT, Rajam, India
[2]IT Department, GMRIT, Rajam, India

Abstract—Cloud Computing is current buzzword in the market Confidentiality, Integrity, Availability, Authenticity, and Privacy are essential concerns for both Cloud providers and consumers as well. Security in Cloud computing is an important and critical aspect, and has numerous issues and problem related to it. Cloud service provider and the cloud service consumer should make sure that the cloud is safe enough from all the external threats so that the customer does not face any problem such as loss of data or data theft. There is also a possibility where a malicious user can penetrate the cloud by impersonating a legitimate user, thus infecting the entire cloud and affects many customers who are sharing the infected cloud. In this we will discuss how to provide security for the data from the unauthorized users and provide integrity to the users.

Keywords—Cloud Computing, Data Integrity, Confidentiality, AES, Steganography

I. INTRODUCTION

Cloud computing is a model for convenient and on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort. In simple words, Cloud Computing is the combination of a technology, platform that provides hosting and storage service on the Internet. Main goal of the cloud computing is to provide scalable and inexpensive on-demand computing infrastructures with good quality of service levels. Many companies developing and offering cloud computing products and services but have not properly considered the implications of processing, storing and accessing data in a shared and virtualized environment. In fact, many developers of cloud-based applications struggle to include security. In other cases, developers simply cannot provide real security with currently affordable technological capabilities. Cloud computing is sharing of resources on a larger scale which is cost effective and location independent. Resources on the cloud can be used by the client and deployed by the vendor such as amazon, google, IBM, salesforce, zoho, rackspace, Microsoft. It also shares necessary software's and on-demand tools for various IT Industries. Benefits of Cloud computing are enormous. The most important one is that the customers don't need to buy the resource from a third party vendor, instead they can use the resource and pay for it as a service thus helping the customer to save time and money. Cloud is not only for Multinational companies but it's also being used by Small and medium enterprises.

The architecture of the Cloud Computing involves multiple cloud components interacting with each other about the various data they are holding on too, thus helping the user to get to the required data on a faster rate. When it comes to cloud it is more focused upon the frontend and the back end. The front end is the User who requires the data, whereas the backend is the numerous data storage device, server which makes the Cloud. There are three types of cloud according to their usage. They are private cloud, public cloud and hybrid cloud. The private cloud is owned by a single organization and public clouds are shared on a larger scale. Private cloud provides better control and more flexibility. Hybrid cloud is a combination of Private cloud and Public Cloud which is used by most of the industries. The advantages of cloud computing may be very appealing but nothing is perfect. Cloud got many issues when it comes to security especially on Data theft, Data loss and Privacy. The parameters that affect the security of the cloud and problems faced by cloud service provider and cloud service consumer such as data, privacy, infected application and security issues.

1.1 Parameters affecting cloud security

There are numerous security issues for cloud computing as it encompasses many technologies including networks, databases, operating systems, virtualization, resource scheduling, transaction management, load balancing, concurrency control and memory management.

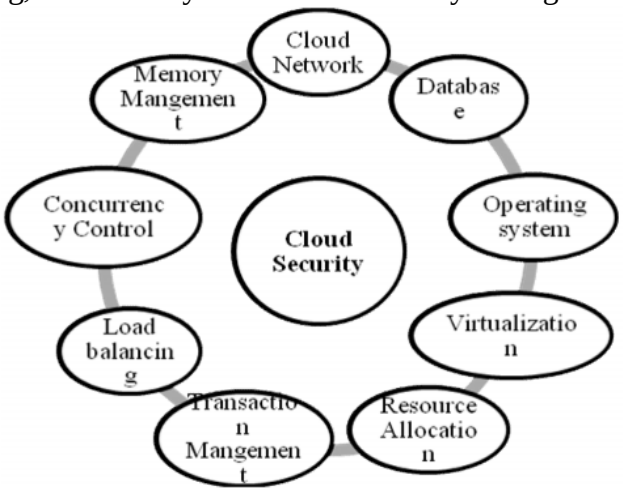


Fig:1.1

1.2 Security Issues faced by Cloud computing

Whenever a discussion about cloud security is taken place there will be very much to do for it. The cloud service provider for cloud makes sure that the customer does not face any problem such as loss of data or data theft. There is also a possibility where a malicious user can penetrate the cloud by impersonating a legitimate user, there by infecting the entire cloud. This leads to affects many customers who are sharing the infected cloud. There are four types of issues raise while discussing security of a cloud.

1. Data Issues
2. Privacy issues
3. Infected Application
4. Security issues

1.2.1 Data Issues

Sensitive data in a cloud computing environment emerge as major issues with regard to security in a cloud based system. Firstly, whenever a data is on a cloud, anyone from anywhere anytime can access data from the cloud since data may be common, private and sensitive data in a cloud. So at the same time, many cloud computing service consumer and provider accesses and modify data. Thus there is a need of some data integrity method in cloud computing. Secondly, data stealing is a one of serious issue in a cloud computing environment. Many cloud service provider do not provide their own server instead they acquire server from other service providers due to it is cost affective and flexible for operation and cloud provider. So there is a much probability of data can be stolen from the external server. Thirdly, Data loss is a common problem in cloud computing. If the cloud computing service provider shut down his services due some financial or legal problem then there will be a loss of data for the user. Moreover, data can be lost or damage or corrupted due to miss happening, natural disaster, and fire. Due to above condition, data may not be accesses able to users. Fourthly, data location is one of the issues what requires focus in a cloud computing environment. Physical location of data storage is very important and crucial. It should be transparent to user and customer. Vendor does not reveal where all the data's are stored.

1.2.2 Secrecy Issues

The cloud computing service provider must make sure that the customer personal information is well secured from other providers, customer and user. As most of the servers are external, the cloud service provider should make sure who is accessing the data and who is maintaining the server so that it enable the provider to protect the customer's personal information.

1.2.3 Infected Application

Cloud computing service provider should have the complete access to the server with all rights for the purpose of monitoring and maintenance of server. So this will prevent any malicious user from uploading any infected application onto the cloud which will severely affect the customer and cloud computing service.

1.2.4 Security issues

Cloud computing security must be done on two levels. One is on provider level and another is on user level. Cloud computing service provider should make sure that the server is well secured from all the external threats it may come across. Even though the cloud computing service provider has provided a good security layer for the customer and user, the user should make sure that there should not be any loss of data or stealing or tampering of data for other users who are using the same cloud due to its action. A cloud is good only when there is a good security provided by the service provider to the user.

II. EXISTING WORK

The barrier and hurdles toward the rapid growth of cloud computing are data security and privacy issues. No organizations will transfer their data or information to the cloud until the trust is built between the cloud service providers and consumers. This paper surveyed different techniques about data security and privacy, focusing on the data storage and use in the cloud, for data protection in the cloud computing environments to build trust between cloud service providers and consumers. For building that trust worthiness confidentiality, Integrity, Availability must be provided.
So in this paper we provided

Confidentiality:
Confidentiality by authenticating the user by generating OTP(Random number) ,checking the validity of the users.

Integrity:
Integrity by storing the encrypted data in cloud service provider(Drop box) the normal multimedia, and used steganography for hiding most sensitive data like passwords…..

Availability:
User can use these services where and when ever needed by connecting to internet

III. PRESENT WORK

Cloud computing and storage solutions provide users and enterprises with various capabilities to store and process their data in third-party data centers. Organizations use the Cloud in a variety of different service models (SaaS, PaaS, and IaaS) and deployment models (Private, Public, Hybrid, and Community). There are a number of security issues/concerns associated with cloud computing but these issues fall into two broad categories: security issues faced by cloud providers (organizations providing software- as-a-service , platform- as-a-service, or infrastructure-as-a-service via the cloud) and security issues faced by their customers (companies or organizations who host applications or

store data on the cloud). The responsibility goes both ways, however the provider must ensure that their infrastructure is secure and that their client's data and applications are protected while the user must take measures to fortify their application and use strong passwords and authentication measures.

In Cloud Computing there are three major potential threats namely

1. Security (for the stored data)
2. Privacy (from the Unauthorized Users)
3. Trust (Data Integrity)

3.1 Data Security and Privacy

Data is stored in the cloud shared by multiple tenants. The data location is mobile, that is, it can move from one location to another. The cloud users may not be aware of the data location or about the access log of their data. The confidential information is stored away from its owner, which increases its vulnerability. This raises serious questions about the security of user's data.

3.2 Identity and Access Management

Data in the cloud is stored at multiple locations, that is, the location of data in the cloud is mobile. The cloud user may or may not be aware of his data's location. The cloud being multi-tenant in nature, the cloud user may have to logon using different user credentials for different providers. This poses potential threat to data as any individual may fake as the original owner in case the credentials are lost/leaked outside the system. A cloud needs to have a strong and sturdy identity and access management system in place so as to attract more transfers to the cloud.

3.3 Proposed System

In this paper, we will review different security techniques and challenges for data storage security and privacy protection in the cloud computing environment. The techniques used in the cloud computing through data security aspects including data integrity, confidentiality, and availability.

3.3.1 Data Integrity

Data integrity is one of the most critical elements in any information system. Generally, data integrity means protecting data from unauthorized deletion, modification, or fabrication. Managing entity's admittance and rights to specific enterprise resources ensures that valuable data and services are not abused, misappropriated, or stolen.

Authorization is used to control the access of data. It is the mechanism by which a system determines what level of access a particular authenticated user should have to secure resources controlled by the system.

Data integrity in the cloud system means preserving information integrity. The data should not be lost or modified by unauthorized users. Data integrity is the basis to provide cloud computing service such as SaaS, PaaS, and IaaS. Besides data storage of large-scaled data, cloud computing environment usually provides data processing service.

3.3.2 Data Confidentiality

Data confidentiality is important for users to store their private or confidential data in the cloud. Authentication and access control strategies are used to ensure data confidentiality. The data confidentiality, authentication, and access control issues in cloud computing could be addressed by increasing the cloud reliability and trustworthiness.

Because the users do not trust the cloud providers and cloud storage service providers are virtually impossible to eliminate potential insider threat, it is very dangerous for users to store their

sensitive data in cloud storage directly. Simple encryption is faced with the key management problem and cannot support complex requirements such as query, parallel modification, and fine-grained authorization.

IV. DESCRIPTION

We are concentrating on Authentication and Data Integrity. Data Integrity means protecting data from unauthorized deletion, modification. Authentication means giving access only to the privileged users.

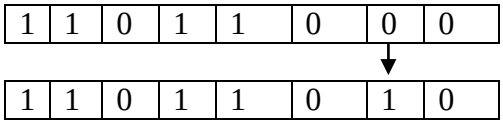
- To authorize the users we are generating random numbers (RN).
- The RN will be sended to the mobile number which was given during their Registration.
- When the user enters the code (RN) then they will we allowed to add data, modify the data and to access the data.
- If the User enters incorrect code then the user is an Unauthorized User then he/she cannot access the data.
- Users can store multimedia data into the cloud Service provider i.e drop box.
- The very sensitive data of the users can be stored in much secured way using steganography.
- The multimedia data will be encrypted and then uploaded to cloud service provider.
- While downloading the multimedia from drop box then it will be decrypted and given to the users.
- In this way the data will be very much secured and not revealed to other users

4.1 EXISTING TECHNOLOGIES

Hiding of data inside an image is simply called steganography. A lot of steganography techniques are used frequently to cover an information, is an image steganography technique and is a

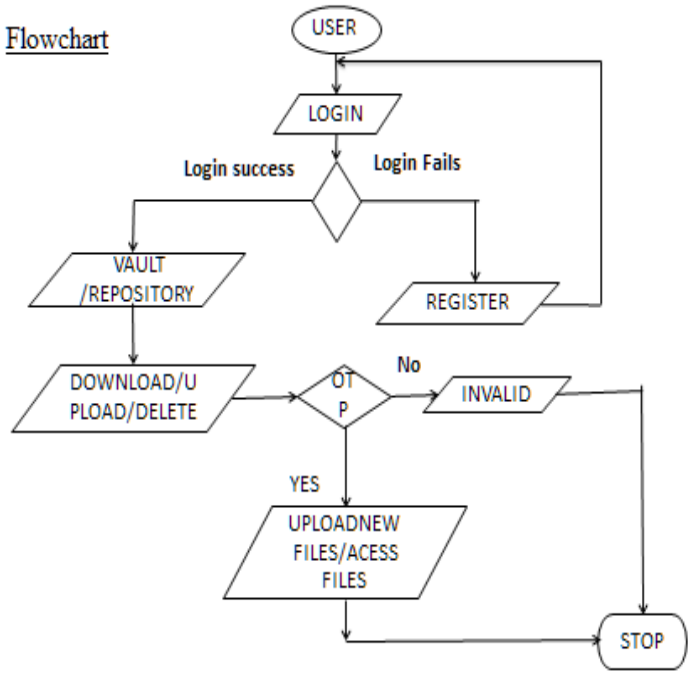
4.1.1 LSB –2 STEGANOGRAPHY

In LSB-2 Steganography the data embedding process is slightly different. It alters the 2nd bit from right for all pixels [7]. The algorithm is as follows:
Step1: Convert the data from decimal to binary.
Step 2: Read Cover image.
Step 3: Convert the Cover Image from decimal to binary.
Step 4: Break the byte to be hidden into bits.
Step 5: Take first 8 byte of original data from the Cover Image.
Step 6: Replace the least significant bit by one bit of the data to be hidden.
First byte of original information from the Cover Image:
E.g.:- 1 1 0 1 1 0 0 0
First bit of the data to be hidden: 1
Replace the least significant bit



Step 7: Continue the step 6 for all pixels.

4.1.2. FLOWCHART:



V. AES ALGORITHM

In this section, we propose a framework which involves securing of files through file encryption. The file present on the device will be encrypted using AES algorithm The user can also download any of the uploaded encrypted files and read it on the system.

A. AES Algorithm

The Advanced Encryption Standard (AES) is a symmetric-key block cipher published by the National Institute of Standards and Technology (NIST). The criteria defined by NIST for selecting AES fall into three areas:

1. Security
2. Cost
3. Implementation.

AES is a non-Feistel cipher that encrypts and decrypts a data block of 128 bits. It uses 10, 12, or 14 rounds. The key size, which can be 128, 192, or 256 bits, depends on the number of round.

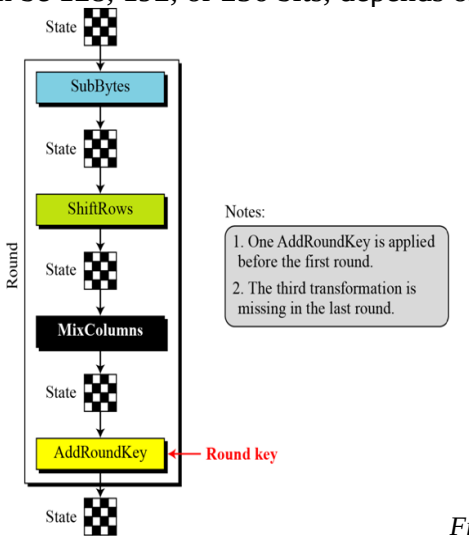


Fig 1.2

To provide security, AES uses four types of transformations: substitution, permutation, mixing, and key-adding**.**

Substitution

A non-linear substitution step where each byte is replaced with another according to a lookup table.

Permutation

A transposition step where each row of the state is shifted cyclically a certain number of steps.

Mixing

A mixing operation which operates on the columns of the state, combining the four bytes in each column.

Key-Adding

In the AddRoundKey step, the subkey is combined with the state. For each round, a subkey is derived from the main key using Rijndael's key schedule; each subkey is the same size as the state. The subkey is added by combining each byte of the state with the corresponding byte of the subkey using bitwise XOR.

5.1 AES Encryption & Decryption Algorithm

AES is an algorithm for performing encryption (and the reverse, decryption) which is a series of well-defined steps that can be followed as a procedure. The original information is known as plaintext, and the encrypted form as cipher text. The cipher text message contains all the information of the plaintext message, but is not in a format readable by a human or computer without the proper mechanism to decrypt it; it should resemble random gibberish to those not intended to read it. The encrypting procedure is varied depending on the key which changes the detailed operation of the algorithm. Without the key, the cipher cannot be used to encrypt or decrypt.

5.1.1 AES Encryption Algorithm

```
Cipher (byte in [4*Nb], byte out [4*Nb], word w [Nb*(Nr+1)]) begin
  byte state[4,Nb]
  state = in
  AddRoundKey(state, w[0, Nb-1])
  for round = 1 step 1 to Nr–1
      SubBytes(state)
      ShiftRows(state)
      MixColumns(state)
      AddRoundKey(state,w[round*Nb,(round+1)*Nb-1])
 end for
 SubBytes(state)
 ShiftRows(state)
 AddRoundKey(state, w[Nr*Nb, (Nr+1)*Nb-1])
  out = state
 end
```


5.1.2 AES Decryption Algorithm

```
InvCipher(bytein[4*Nb],byteout[4*Nb],word w[Nb*(Nr+1)])
Begin
  byte state[4,Nb]
  state = in
  AddRoundKey(state, w[Nr*Nb, (Nr+1)*Nb-1])
  for round = Nr-1 step -1 downto 1
      InvShiftRows(state)
      InvSubBytes(state)
      AddRoundKey(state,w[round*Nb,
       (round+1)*Nb-1])
      InvMixColumns(state)
  end for
  InvShiftRows(state)
  InvSubBytes(state)
 AddRoundKey(state, w[0, Nb-1]) out = state
End
```

VI. CONCLUSION

Cloud computing is a promising and emerging technology for the next generation of IT applications. The barrier and hurdles toward the rapid growth of cloud computing are data security and privacy issues. Reducing data storage and processing cost is a mandatory requirement of any organization, while analysis of data and information is always the most important tasks in all the organizations for decision making. So no organizations will transfer their data or information to the cloud until the trust is built between the cloud service providers and consumers. A number of techniques have been proposed by researchers for data protection and to attain highest level of data security in the cloud. However, there are still many gaps to be filled by making these techniques more effective. More work is required in the area of cloud computing to make it acceptable by the cloud service consumers. This paper surveyed different techniques about data security and privacy, focusing on the data storage and use in the cloud, for data protection in the cloud computing environments to build trust between cloud service providers and consumers

REFERENCES

[1] Harjit Singh Lamba and Gurdev Singh, “Cloud Computing-Future Framework for emanagement of NGO's”, IJoAT, ISSN 0976-4860, Vol 2, No 3, Department Of Computer Science, Eternal University, Baru Sahib, HP, India, July 2011.

[2] Dr. Gurdev Singh, Shanu Sood, Amit Sharma, “CM- Measurement Facets for Cloud Performance”, IJCA, Lecturer, Computer science & Engineering, Eternal University, Baru Sahib (India), Volume 23 No.3, June 2011.

[3] Rabi Prasad Padhy, Manas Ranjan Patra , Suresh Chandra Satapathy, “Cloud Computing: Security Issues and Research Challenges”, International Journal of Computer Science and Information Technology & Security (IJCSITS) Vol. 1, No. 2, December 2011.

[4] Prince Jain, “Security Issues and their Solution in Cloud Computing”, International Journal of Computing & Business Research, Proceedings of ‘I-Society 2012’ at GKU.

[5] Balachandra Reddy Kandukuri, Ramakrishna Paturi V, DR. Atanu Rakshit, “Cloud Security Issues”, 2009 IEEE International Conference on Services Computing.

[6] “Cloud computing Benefits, risks, recommendations for information security cloud computing”November-2009.

[7] Huiming Yu, Nakia Powell, Dexter Stembridge and Xiaohong Yuan, "Cloud Computing and Security Challenges", 2012 ACM Publication.

[8] Hassan Mathkourand, B. Al-Sadoon and Ameur Touir, "A New Image Steganography Technique", *IEEE 4th International Conference on Wireless Communications, Networking and Mobile Computing*, pp. 1-4, 2008.

[9] Qingzhong Liu, Andrew H. Sung, Zhongxue Chen and Xudong Huang, "A JPEG-Based Statistically Invisible .

[10] A. E. Mustafa, A. M. F. ElGamal, M. E. ElAlmi and B. D. Ahmed, "A Proposed Algorithm For Steganography In Digital Image Based on Least Significant Bit", *Research Journal Specific Education Faculty of Specific Education Mansoura University*, pp. 752-767, 2011.

