Advance Cloud Computing Security Evaluation Model based on Trust Management

Foram Chudasama[1], Nirav Shah[2]
[1]*M.E. Department of Computer Engineering, Silver Oak College of Engineering and Technology*
[2]*Department of Information Technology, Silver Oak College of Engineering and Technology*

***Abstract* - Cloud computing as a facilitator offers scalable resources and noteworthy economic assistance as the decreased operational expenditures. With the rapid development of cloud computing, public cloud as the main form, the attack value is higher, and security is more difficult. To maintain sensitive information and confidentiality in cloud computing is of great importance which means the need for more robust ways to keep it from the attackers. In this paper, several multi-coding levels were developed using more than one method to obtain more confidentiality through Modified Advanced Encryption Standard (MAES) with Trust Mechanism which is based on energy level. Then after we will check resulted parameters like Time Complexity, robustness, complexity, and security of data by using a Matlab program which has been used for implementing proposed scheme with several analyses.**

***Index Terms* - cloud computing, Trust Mechanism, security issue and challenge, robustness.**

1.INTRODUCTION

Cloud concept commitment to the principles to achieve a cost-effective utility computing, allowing users and providers easy access to the resources of self-service, pay-as-you go approach, thereby reducing the cost of system management and improve resource utilization and accounting. Cloud Computing is a gathering of coordinated network, hardware, software, and internet. Cloud Computing enables on-demand access to several computing resources in a pay-per-use manner. Cloud Platform provides on demand services which are always on anywhere, anytime, and anyplace. Cloud Computing is an information technology paradigm that provides ubiquitous access to shared, centralized pool of services which includes servers, computer networks, data storage, applications, and various other services over the internet It enables on- demand rationing, scalable and elastic computing, storage, and network resources.

In figure 1 also contains mobile's applications which are stored on database server, and you can used anywhere.

Deployment model, we will classify cloud as: public, private, hybrid, community cloud

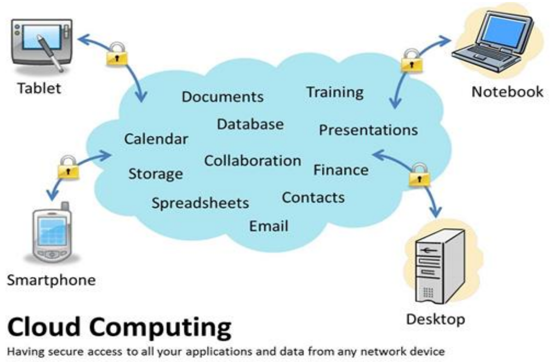

Fig. Cloud computing overview

1.1 Services in cloud computing

Cloud services are usually divided within the three main types, Software-as-a-Service (SaaS), Platform-as-a- Service (PaaS) and Infrastructure-as-a-Service (IaaS).

a. Software as a Service (SaaS)

SaaS is delivered applications over the internet as a service instead of installing and maintain software. The one big advantage of SaaS is that each one client is running an equivalent software version and new functionality are easily integrated by the provider and is available to all the clients. E.g., Salseforce.com.

b. Platform as a Service (PaaS)

Pass is type of cloud computing in which service provider delivers a platform to clients E.g., Google App Engine. This enables clients to use custom software using the tools and programming languages offered by the provider. The Clients have control over the deployed applications and environment-related settings. As with SaaS, the management of the underlying infrastructure lies within the responsibility of the provider.

c. Infrastructure as a Service (IaaS)

IaaS delivers hardware resources like CPU, network, or disc space components as a service. These resources are delivered as a virtualization platform by the Cloud provider and may be accessed across the web by the client. The clients have full control of the virtualized platform and are not responsible for managing the underlying infrastructure.

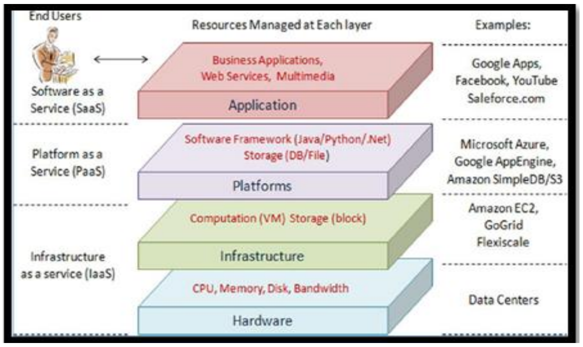
End Users
Resources Managed at Each layer
Examples:
Business Applications, Web Services, Multimedia
Application
Google Apps, Facebook, YouTube Saleforce.com
Software as a Service (SaaS)
Software Framework (Java/Python/.Net) Storage (DB/File)
Platforms
Microsoft Azure, Google AppEngine, Amazon SimpleDB/S3
Platform as a Service (PaaS)
Computation (VM) Storage (block)
Infrastructure
Amazon EC2, GoGrid Flexiscale
CPU, Memory, Disk, Bandwidth
Hardware
Data Centers
Infrastructure as a service (IaaS)

Fig. service of cloud computing

2.PROBLEM DEFINITION

As per survey found certain limitations in existing systems like Robustness, security, privacy of data, speed and also time complexity.

3.BACKGROUND

3.1 IDENTITY ACCESS MANAGEMENT

Identity and Access Management (IAM) is the security that enables the right person to access the right resources at the right times for the right reasons. IAM is identity management and access management. Identity management associates user rights with a given identity, giving users access to system resources. Mainly issuing a unique identity declaration for each subject, such as identity identification, user ID, password to authenticate identity.

3.2 MULTIFACTOR AUTHENTICATION

Multifactor authentication is an authentication method in which user have to successfully present two or more evidence only after that user granted access to a website or application. Multifactor authentication has been widely used by the network providers. One-time passwords and mobile code scanning are the most widely used multifactor authentication strategies. This will help in securing the data with the help of multifactor. In case unauthorized person would try to gain access to the data using password a wrong OTP will be sent, so that the unauthorized person will not be able to authenticate and gain access to the information. Multifactor authentication is regarded as high-level protection to the data in cloud.

3.3 DATA ENCRYPTION

Data encryption is security method where data encoded with key and only decrypt by the user who has right encryption key. Data encryption is the most used method for protecting data confidentiality. Data encryption makes it difficult for the cloud services to process the queries on the cloud. The two major methods that ensure data confidentiality are Encryption and querying encrypted data and trusted computing.

3.4 WRITTEN SECURITY POLICES

Written Security Policies Written data security policies are an important method of providing data security. The data security policies are useful for articulating the security needs which means the limitations of everybody are laid out and it is defined “who care perform what and on which set of data.

4. LITERATURE REVIEW

In this paper [9], Data Access It is important to ensure that the data can be accessed only by the administrator and not by the users. Providing access only to the administrator will enhance the security. The Information security and the information technology department of the organization is responsible for identifying such data access problems and ensure prevention from phishing and other malicious data attacks.

Backups In case of any such data theft and security issues, the cloud providers as well as organizations should ensure access to data backup. Also, loud backups of the data should be encrypted. As the data in the cloud is encrypted, the backup also should be encrypted.

Data Encryption Protecting data confidentiality is crucial. Data encryption is the most used method for protecting data confidentiality. Data encryption makes it difficult for the cloud services to process the queries on the cloud [7]. The two major methods that ensure data confidentiality are Encryption and querying encrypted data and trusted computing.

PIR (Private Information Retrieval) PIR is the technique that solves the problem of data privacy without even revealing to the server in which item is retrieved.

The PIR solutions can be used in both one as well as multiple servers. Earlier PIR solutions were criticized for incurring any expensive computation costs. PIR is an important technique that is most widely used for dealing with the query privacy problems. PIR is a procedure which lets any client to retrieve an item from any database without the owner of the database getting to know which item was chosen. Even though this issue has a small solution that is sending the whole of database to the client so that the client and query with complete confidentiality promise still there are methods of reducing the communication intricacy of this issue, which can be highly significant for huge data bases Oblivious RAM is considered as an important method for making PIR more practical in the way it is proposed for ensuring query privacy in the cloud server. Oblivious Ram follows the basic idea which is used in shuffling and restoring the data items in the RAM while accessing the data.

5 PROPOSED MODEL

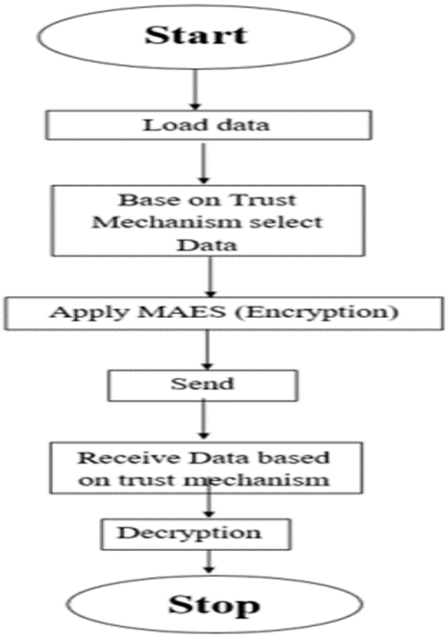
Start
Load data
Base on Trust Mechanism select Data
Apply MAES (Encryption)
Send
Receive Data based on trust mechanism
Decryption
Stop

Fig. Proposed model

Steps of the proposed system:

1. start
2. Load the data from different server
3. Select the data based on trust Mechanism
4. Apply MAES(Encryption) on it.
5. Send data to server
6. Receive data based on trust mechanism
7. Decrypt data.
8. Stop

AES Algorithm:

The AES algorithm is a symmetric key algorithm that was established as the standard for encrypting digital data by the US National Institute for Standard and Technology (NIST). It is an iterative round block cipher that works on 128bit plaintext using three different key lengths 128, 192, and 256 bits [9]. The key length determines the number of encryption and decryption rounds to be performed which could be 10, 12, and 14 rounds for 128, 192, and 256-bit key length, respectively. It is believed that the larger the key length, the higher the cryptographic strength [9]. The AES algorithm consists of four invertible transformations: SubBytes, ShiftRows MixColumns, and AddRoundKey, as shown in

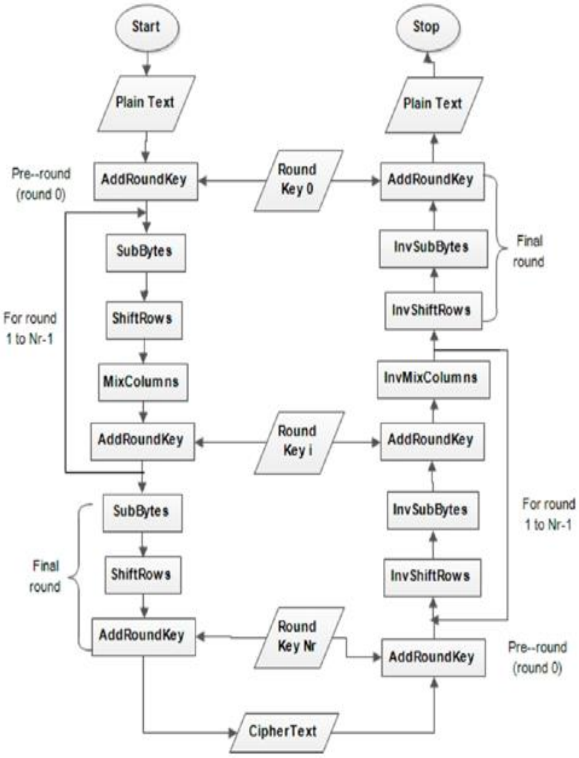

Fig. Structure of the Advance Encryption Standard (AES) Algorithm

Advanced Encryption Standard is the new encryption standard recommended by NIST to replace DES. Brute force attack is the only effective attack known against it, in which the attacker tries to test all the characters combinations to unlock the encryption. Both AES and DES are block ciphers. It has variable key length of 128, 192, or 256 bits; default 256. It encrypts data blocks of 128 bits in 10, 12 and 14 rounds depending on the key size. AES Encryption is fast and flexible; it can be implemented on various platforms especially in small devices. Also, AES has been carefully tested for many security applications.

Algorithm:

```
Cipher (byte [] output, byte [] input)
{byte [4,4] State.
copy input [] into State [] AddRndKey for (rnd = 1; rnd < Nr-1; ++rnd)
{
SubBytes ShiftRows MixColumns AddRndKey
}
SubBytes ShiftRows AddRndKey copy State [] to output []
}
```

AES consists of key expansion, initial and final round. Initial rounds consist of Add Round Key, Sub Bytes, Shift Rows, Mix Columns, Add Round Key, and final round also consists of similar function as initial round except mix columns. AES works fast on both software and hardware.

MAES algorithm:

A new modification for the AES algorithm (MAES) is done by replacing the MixColumns stage with random Generated IP vector for Permutation or Transposition stage at every session of encryption. This will increase the speed of the algorithm without a decrease in the security of the AES algorithm. In addition, the security of the MAES algorithm can be enhanced using the permutation stage that changes the IV vectors at every round of the encryption process.

The design of the MAES algorithm will ensure the following:

1. Speed up the encryption and decryption processes by replace MixColumns stage with simple xor operations.
2. The input state will be the first input for the xor operation. 3- Increase the decryption level of complexity by
   a. Using random number generator output as second input for xor operation.
   b. Key dependent random number generator.

Algorithm:

```
ShiftRows (byte state [4, Nb]) begin byte t[Nb]
if state [0][0] odd numbers for r = 1 step 1, 3
x = r mod 4
if x = 0 step 0 to x + 1 for c = 0 step 1 to Nb – 1
t[c] = state [r, (c + x) mod Nb] end for
for c = 0 step 1 to Nb – 1 state[r,c] = t[c]
end for end for else
for r = 2 step 2, 4
k = 0
x = r mod 4
if x = 0 step 0 to 3
for c = Nb - 1, c >= 0, c -1
t[c] = state [x, (c + x) mod Nb, k + 1 end for
for c = 0, c < Nb, c 1 + state[x,c] = t[c]
end for end for End
```

6.CONCLUSION

By using combination of AES and MAES we will get higher security in cloud computing. MAES is used for strongly secure transmission of data by using shift raw operation to modify encryption and decryption which will be quick than AES. we will get 15.8 second time complexity using Proposed Approach in MATLAB.

REFERENCES

[1] Sravan Kumar R, Ashutosh Saxena, “Data Integrity Proofs in Cloud

[2] Storage”, IEEE 2011 978-1-4244-8953-4/11/$26.00 c 2011 IEEE

[3] Nagababu Garigipati,Dr Krishna Reddy V Professor, “A Study on Data Security and Query privacy in Cloud” , 978-1-5386-9439-8/19/$31.00 ©2019 IEEE

[4] Rashmi Rao, Pawan Prakash, “Improving security for data migration in cloud computing using randomized encryption technique “, May-Jun. 2013 IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-

8727Volume 11, Issue 6, PP 39-42 www.iosrjournals.org

[5] Virendra Singh Kushwah, Aradhana Saxena, "A Security Approach for Data Migration in Cloud Computing", MAY 2013 International Journal of Scientific and Research Publications, Volume 3, Issue

[6] R.Vinodha, Mr.R.Suresh, "Secure Migration of Various Database over A Cross Platform Environment", 2013 International Journal of Engineering And Computer Science ISSN:2319-7242 Volume 2 Issue 4 April, 2013 Page No. 1072 -1076, www.ijecs.in

[7] Deyan Chen, Hong Zhao," Data Security and Privacy Protection Issues in Cloud Computing", 2012 IEEE International Conference on Computer Science and Electronics Engineering, 978-0-7695-4647-6/12 $26.00 © 2012 IEEE DOI 10.1109/ICCSEE.2012.193

[8] Solomn Guadie worku, Zhong Ting, Qin Zhi-Guang, "Survey on Cloud Data Integrity Proof Techniques", 2012 IEEE Seventh Asia Joint Conference on Information Security, 978-0- 7695 4776-3/12 $26.00 © 2012 IEEE DOI 10.1109/AsiaJCIS.2012.22

[9] Ashalatha R, "A survey on Security as A Challenge in Cloud Computing", July 2012 International Journal of Advanced Technology & Engineering Research (IJATER)

[10] Quingni Shen, Lizhe Zhang, Xin Yang, Ying Zhang," SecDM: Secure Data Migration Between Cloud storage Systems IEEE 2011 Ninth International Conference on Dependable, Autonomic and Secure Computing

[11] Sravan Kumar R, Ashutosh Saxena, "Data Integrity Proofs in Cloud Storage", IEEE 2011 978-1-4244-8953-4/11/$26.00 c 2011 IEEE

[12] Xiaojun Yu, Qiaoyan Wen, "A VIEW ABOUT CLOUD DATA SECURITY FROM DATA LIFE CYCLE", 2010 IEEE National Natural Science Foundation of China (Grant Nos. 60873191, 60903152, 60821001), Beijing Natural Science Foundation (Grant No. 4072020), 978-1-4244-5392-4/10/$26.00

[13] Wei Hao, I-Ling Yen, Bhavani Thraisingham, "Dynamic Service and Data Migration in Clouds", 2009 IEEE International Conference on Computer Software