ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 5, Issue 7, July 2016

Addressing Security Concerns in Cloud Computing

Sai Kumar Malve

Abstract— **Cloud Computing is a concept of internet based computing. In other words it is a shared pool of resources. It doesn't have a standard meaning to it. It is reliable, ubiquitous and remote. It has its own advantages and disadvantages. Pay as you use, reliable, manageable, reduced usage of software and hardware are some of the advantages of cloud computing. The main disadvantages of it are security, limited control, vendor lock-in.**
Security of data is the main concern of cloud computing during transmission of data and storage. Because of this concern many people are not ready to use it. One way to make it more secure is authenticating the user using CHAP(Challenge-Handshake Authentication Protocol). And second recommendation is encryption of data. This paper recommends the use of DES(Data Encryption Standard) and AES(Advanced Encryption Standard). This paper covers this possible solution.

***Index Terms*— Cloud Computing, Models, Security, Authentication, CHAP, Encryption, DE$, AES.**

I. INTRODUCTION

The term cloud computing doesn't have a standard definition. The term cloud is used as a metaphor for internet. So, cloud computing can be defined as a internet based computing that provides a shared pool of resources and data on demand. It is ubiquitous, remotely hosted and commodified(means it is similar to traditional commodities like electricity, gas. You pay for what you use).

Cloud computing has five characteristics :

- on demand self service
- broad network access
- resource pooling
- rapid elasticity
- measured service

Cloud computing and storage solutions are provided by third-party data centers with minimal management efforts on user's end. By using this technology the consumers can save cost of hardware for deployment, software licenses and maintenance of system. Users can use cloud services through web browsers or using applications.[3]

Manuscript received July, 2016.
***Sai Kumar Malve**, B.Tech(CSE), Sreenidhi Institute of Science and Technology, Hyderabad, India.*

II. CLOUD COMPUTING SERVICE MODELS

Based on service provided cloud computing can be divided into:

A. SaaS(Software as a Service)

In this model cloud services are provided through internet by means of applications.
Ex: Outlook, Facebook.

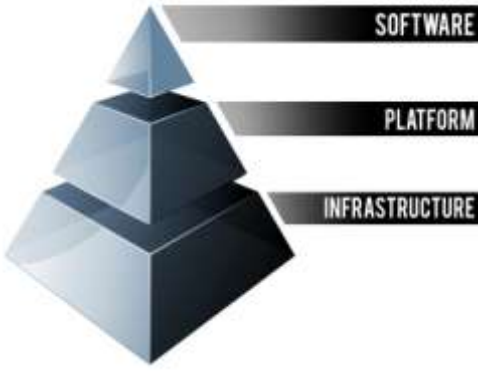

Figure 1. Cloud Computing Service Models

B. PaaS(Platformas a Service)

Cloud vendor provides basic infrastructure to users build an application and test it.
Ex: Google App Engine

C. IaaS(Infrastructure as a Service)

Admin or cloud vendor has major part in this model. Users are provided a platform and/or applications which act as an interface between the users and cloud.
Ex: Microsoft Azure, Amazon Web Services(AWS)[1]

III. CLOUD COMPUTING DEPLOYMENT MODELS

Based on deployment, administration power, and end users cloud computing can be classified as:

A. Public Cloud:

In public clouds, the cloud vendor allocates resources to the end user dynamically through web or mobile applications.
Ex: OneDrive, DropBox

B. *Private Cloud:*

The access of private clouds is limited to few users who are part of an organization. The power of access granting is with the organization's administrators.
Ex: In Educational Institutions, only students, staff, and Administrators can access data of the institution.

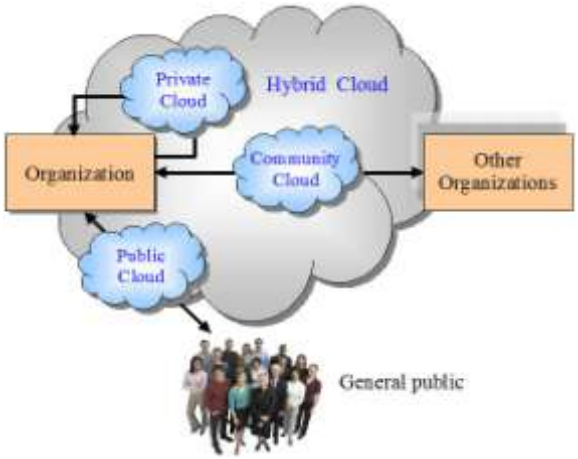

Figure 2. Cloud Computing Deployment Models

C. *Public Cloud:*

Two or more organizations come together to share a common cloud. But the management of cloud is vested with selected organizations which are using its service or third-party organization.

D. *Public Cloud:*

Combination of any two of the above cloud models can be called as Hybrid cloud.[6]

IV. SECURITY ISSUES IN CLOUDS

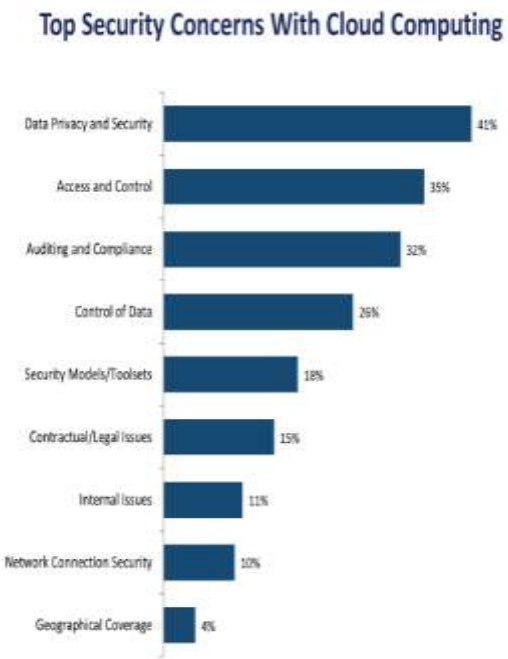

Figure 3. Top Security Concerns

Cloud computing has got many issues. Some of them are costs, vendor lock-in, performance , up-time. But the most troublesome issue which is seen very often in real world is *leakage of data*. So, data privacy and security is major concern of cloud computing.

Data can be stolen when it is being transmitted to cloud or when data is stored in clouds. That means *Data Integrity* must be taken care. For this purpose the data must be encrypted before transmitting it cloud. Even if an intruder gets hands on data, he'll not be able to know what it is unless he decrypts it. Decryptipon is impossible unless the intruder knows the key. *Encryption algorithms* like DES, AES must be used to maintain *data integrity.*

Next concern is *what if an unauthorized user tries to login?.* For *user authentication* methods like *CHAP* must be used.

V. DATA INTEGRITY

A. *DES*

Data Encryption Standard(DES) is a block cipher. The plain text is processed in blocks of 64bits. The length of the key is 56bits. It is a symmetric key encryption, that means it uses same key on sender side and receiver side. Number of rounds in DES is 16.

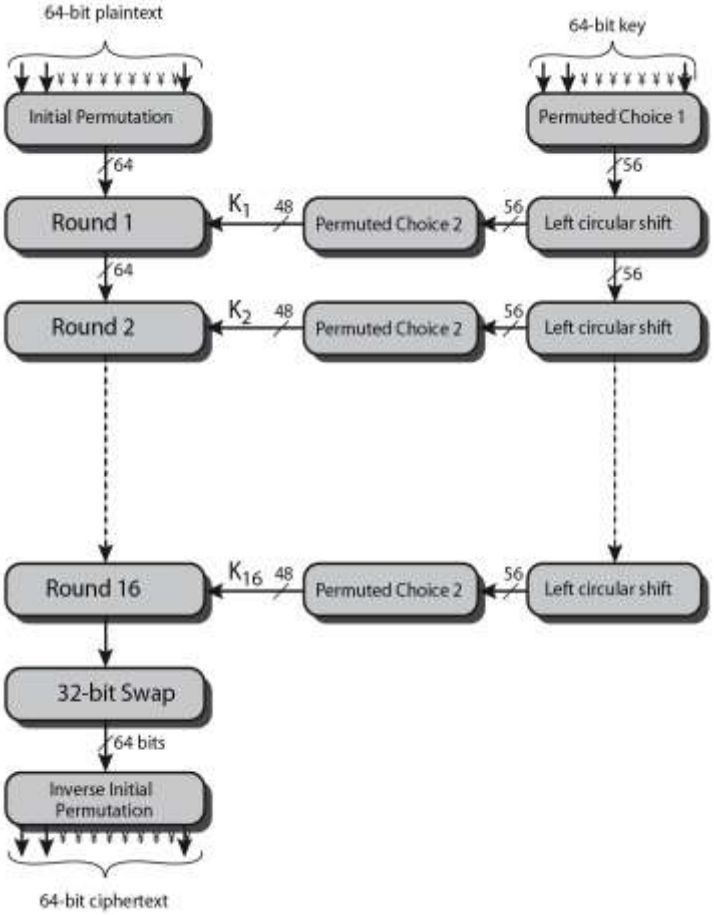

Figure 4. DES

The left side shows the basic process for enciphering a 64-bit data block which consists of:
- an initial permutation (IP) which shuffles the 64-bit input block

- 16 rounds of a complex key dependent round function involving substitutions & permutations
- a final permutation, being the inverse of IP

The right side shows the handling of the 56-bit key and consists of:
- an initial permutation of the key (PC1) which selects 56-bits out of the 64-bits input, in two 28-bit halves
- 16 stages to generate the 48-bit sub-keys using a left circular shift and a permutation of the two 28-bit halves.

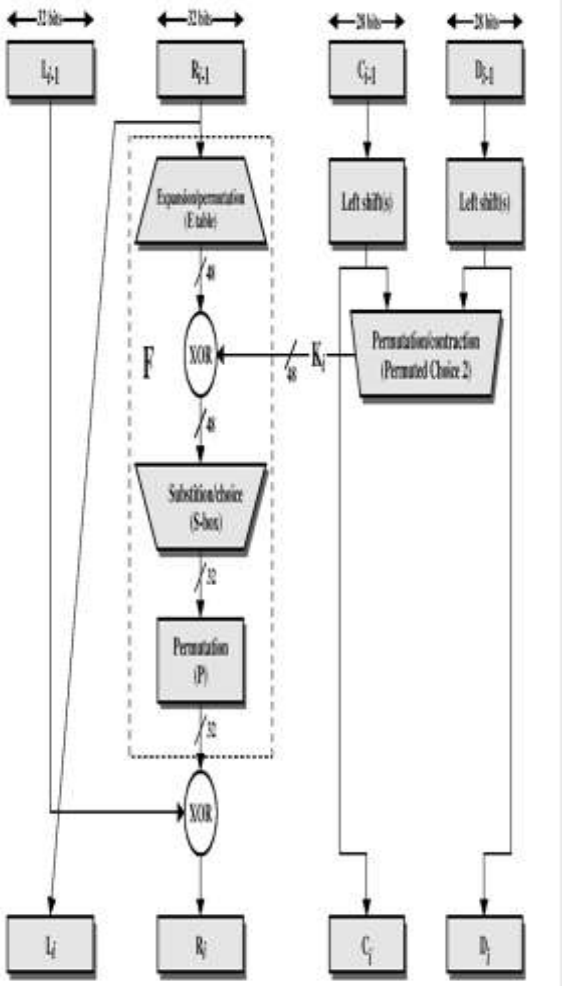

Figure 5. Round *i* of DES

Figure 5 shows the process in each round of DES. DES is not useful when size of plain text is huge because it encrypts 64bits only at each time.[5]

B. AES

Advanced Encryption Standard(AES) is the most widely used and secure encryption standard than DES. It was designed by Rijmen-Daemen in Belgium. Key length can be 128/192/256 bits and number of rounds are 9/11/13 respectively. Higher the key size greater is the security. Plain text size is 128 bits. It is processed as a block of 4 columns of 4 bytes. [2]

In each round the plain text goes through 4 transformations.

- Byte Substitution
- Shift Rows
- Mix Columns
- Add Round Key

But the last round has only 3 transformations. No Mix Columns transformation for last round. Only Add Round Key uses key.

1. Byte Substitution:

A 16X16 S-box is used in this transformation. Each byte is replaced by byte indexed by row(left 4 bits) and column(right 4 bits).

2.Shift Rows:

1st row is unchanged. 2nd row undergoes 1byte left circular shift. 3rd row undergoes 2 bytes left circular shift. 4th row undergoes 3 bytes left circular shift.

3. Mix Columns:

In this step each column is multiplied by a known matrix which has either 1 or 2 or 3 as elements.

Multiplication arithmetic is simple in AES. Multiplication by 1 means no change, by 2 means left shift, by 3 means left shift followed by initial unchanged value.

4. Add Round Key:

Key is used to generate sub-keys. Each column undergoes XOR with its respective sub-key.

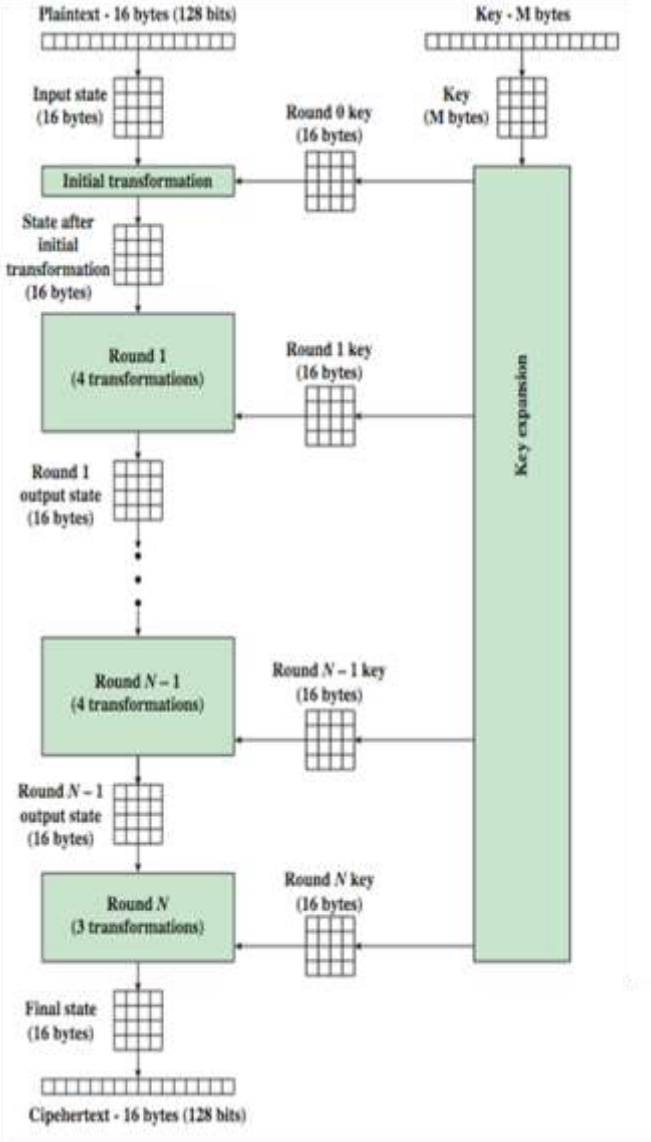

Figure 6. AES

VI. AUTHENTICATION

CHAP(Challenge-Handshake Authentication Protocol) is an authentication protocol used by Point-to-Point Protocol(PPP) to validate the clients of a remote server.
Following steps illustrate CHAP process:

1. Link establishment.
2. The authenticator sends a "challenge" message to the peer.
3. The peer responds with a value calculated using a one-way hash function on the challenge along with the secret.
4. The authenticator generates a hash value and compares with peer response. If both match, the peer is said to be authentic and the authenticator sends an acknowledgement. Otherwise, the connection is terminated.
5. At discrete intervals of time, the authenticator sends a "challenge" message to the peer and steps from 2 through 5 are repeated.[4]

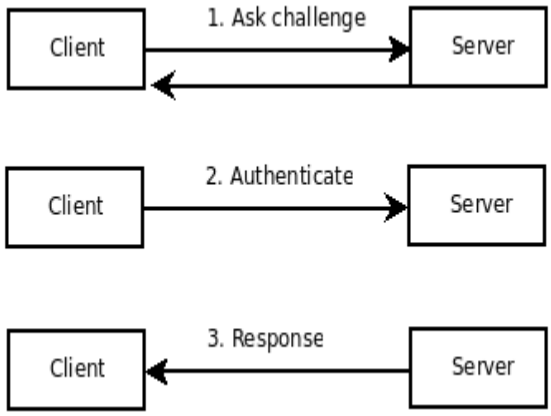

Figure 7. CHAP

VII. CONCLUSION

Cloud computing has got its advantages. But every coin has two sides. Cloud computing is no exception. It has its own vulnerabilities. Data security being the major concern among all others. As long as there is a solution one can keep using cloud computing. Such solutions like encryption of data and user authentication are discussed here. If people have methods to explore the vulnerability, we have got countermeasure for it.

REFERENCES

[1] Sanjoli Singla, Jasmeet Singh, "Cloud Data Security using Authentication and Encryption Technique" International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 7, July 2013
[2] Ritu Pahal, Vikas kumar, "Efficient Implementation of AES" International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE) Volume 3, Issue 7, July 2013
[3] http://www.nist.gov/itl/csd/cloud-102511.cfm
[4] https://en.wikipedia.org/wiki/Challenge-Handshake_Authentication_Protocol
[5] https://en.wikipedia.org/wiki/Data_Encryption_Standard
[6] http://whatiscloud.com/cloud_deployment_models/index