ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 4, April 2019

Securing Cloud Using Various Techniques

Prof. Shubhangi R. Khade

Assistant Professor, Department of Computer Engineering, Modern Education Society's College of Engineering Pune, Maharashtra, India

ABSTRACT: As we see that many firms are adopting cloud technology to store their data remotely on cloud which is initially done on physical storage devices. The services of cloud are provided to user on the basis of cloud consumption i.e "Pay for what you use". Along with this it is the task of cloud service provider is to provide security to the user data on cloud. The main pillars of security are Confidentiality, Integrity and Availability, to achieve this core principals of security one has to provide high security to the data which we are storing on cloud. The cloud service provider is only responsible for the data which is once stored on the cloud by cloud users. While storing data on cloud many security issues arises which are leakage of data, data attacking, unauthorized access. When a user outsources the data to the cloud, there is possibility to attack the data at rest as well as data in transit. The main thing is how to secure the data and rely on the services in cloud. In order to protect the data from unauthorized access, data should be in either encrypted format or masked format. In this paper we have proposed the various techniques which can be used to secure the cloud data from attacker and unauthorized access. Along with this we had given some disaster recovery solutions to recover the loss of data as well as to prevent loss of data from disaster.

KEYWORDS: Cloud Security, Encryption, AES, Steganography.

I. INTRODUCTION

Cloud computing is the most emerging topic in this days. The services provided by cloud to the users over internet includes platform, storage, security,etc. Cloud Service Provider (Cloud Storage Provider) have responsibility to store and manage the user data as well as provide the data to user whenever they want. Cloud consist of large number of various resources such are memory, CPU, etc which are virtualized on cloud platform. Cloud storage may vary from company to company in terms of space, size and functionality. Cloud provides the service of storing data on remote cloud and share the virtual resources among them which increases the resource utilization and resource virtualization. Cloud computing provide storage for all types of data over cloud and provide high speed availability of those resources to the users. The high seed services of cloud computing are cost effective. Cloud computing creates new issues and challenging security threats. For security purpose there are different multiple existing method and techniques that are used in cloud computing environment. In cloud data storage users perform various operations such as insertion, deletion, updation, on data regularly[1]. Cloud computing has various features such as scalability, low cost services, reliability, maintenance, location independence. Cloud computing provides different services such as

(1). Software as a service
(2). Platform as a service
(iii). Infrastructure as a service

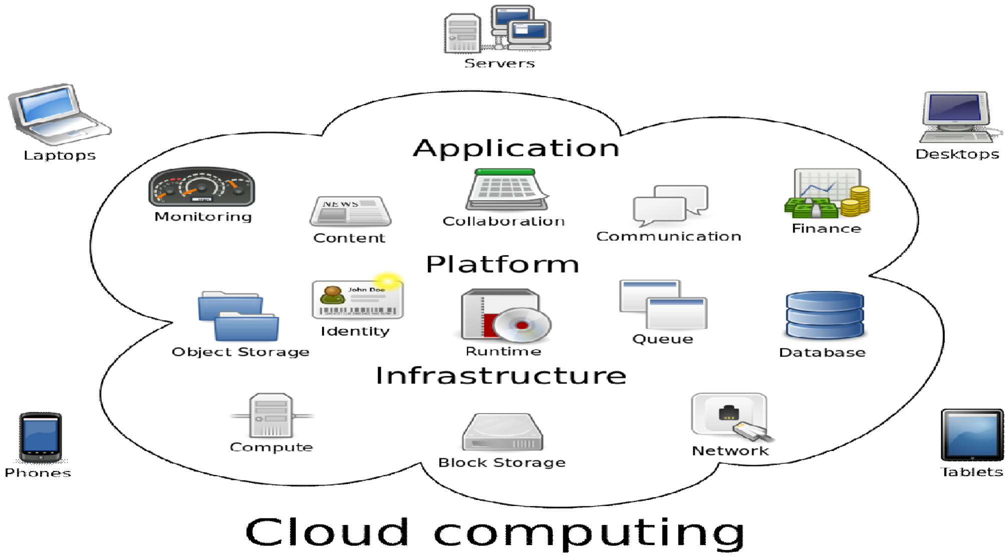


Fig 1. Cloud Computing and its services.

Cloud provides flexibility and reliability, the implementation of cloud-based solutions is still have restrictions deriving from potential security threats. As cloud computing implementation is connected over internet it suffers all the vulnerabilities of network. Along with this network vulnerabilities cloud applications need to cope up with the various potential threats[2]. To improve the security of cloud applications and data that gets stored on cloud we need to understand the dimensions of cloud security which are shown in Fig 2.

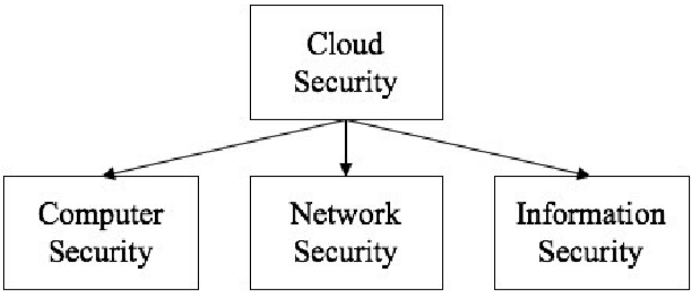


Fig 2. Dimensions of Cloud Security.

The rest of the paper is organized as follows: Section II presents Challenges to cloud security. Section III will describe about methodologies to secure cloud. Section IV describes conclusion.

II. CHALLENGES TO CLOUD SECURITY

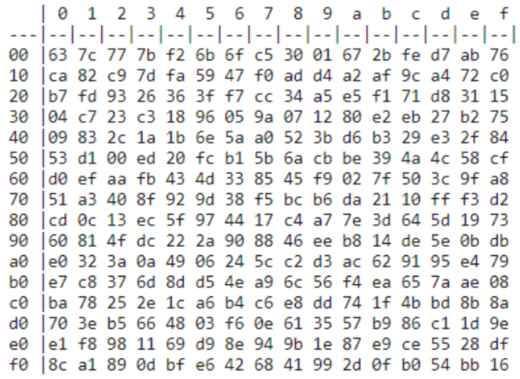
- **Elastic environment:** Due to the dynamic nature of environment the visibility of virtual instances of various resources is difficult. To protect this environment from unauthorized access or any kind of disaster we need to implement discovery, security assessment and taking actions on that circumstances[3].
- **Perimeter definitions:** Due to the fragmented nature of cloud workload across various geo locations it is difficult to control and manage the cloud assets centrally.

- **Loss of control on physical security:** As organizations lose control over physical security, the responsibility of protecting data and workloads at transit and rest falls into the dissatisfaction of the customers.
- **Data Breaches and Downtime:** The fact that generally speaking, enterprise-grade cloud services are more secure than legacy architecture, there is still a potential cost in the form of data breaches and downtime. With public and private cloud offerings, resolving these types of problems is in the hands of the third-party provider.

III. METHODOLOGIES TO SECURE CLOUD

- **Steganography:** Steganography is used to hide the data, messages, text, and information within another files, audio or images, etc. Various techniques are available to implement the steganography in cloud security. While storing the data on cloud we can apply steganographic algorithms to avoid the unauthorized access to the data. The primary goal of steganography is to hide data within some other data in such a way that hidden data cannot be detected. Only intended user can understand the meaning of the sent messages[4].
- **File splitting:** In file splitting, we are splitting the data file, image file or video file in small parts with some extension. After splitting we stored splitted file in our local system and after those files will be stored on the cloud. It is necessary at cloud side is that the algorithm must be implemented in such a way that it will merge all those files in correct order as they are originally.
- **Encryption:** The encryption technique will contains the transformation of readable text into some another unreadable format of data which will be difficult to crack by the attacker. To implement encryption there are two main categories of encryption which are public key encryption and private key encryption. The algorithms such as DES, AES, ECC, RSA can be used to achieve encryption of files. When the file is uploading to the cloud we can implement encryption algorithms and while downloading those files by authorized person decryption must be performed by the intended user with the help of dedicated key[5].
- **Compression:** Another technique to implement cloud security is implement compression and decompression of files. While uploading the files the file can be compressed that is irrelevant contents of files will get removed and stored on cloud same while downloading the files the decompression of the same file must be taken place by the intended user[6].
- **AES:** Advanced Encryption Standard (AES) algorithm has great speed. AES is the current standard for symmetric key encryption. AES is a symmetric key algorithm. It is having various chippers with different keys size and the message block size. In this technique plaintext is encrypted with the help of AES and then the ciphertext which we have got will again encrypt likewise there will be various round like the AES algorithm includes 10, 12 and 14 round with 128, 192, and 256 key bits. Due to the number of rounds the plaintext will be encrypted many times and it will make attacker difficult to decrypt the message[6]. AES is one the most efficient symmetric algorithm[7]. The Advantages It provides strong security from attackers. Disadvantages are a major drawback is that its clouds not withstand the attacks like Brute Force. AES algorithm has four steps:

  1. **Substitute Bytes** In this step, each byte of input data is replaced by another byte from the substitution table (S-box).



```
   | 0  1  2  3  4  5  6  7  8  9  a  b  c  d  e  f
---|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|
00 |63 7c 77 7b f2 6b 6f c5 30 01 67 2b fe d7 ab 76
10 |ca 82 c9 7d fa 59 47 f0 ad d4 a2 af 9c a4 72 c0
20 |b7 fd 93 26 36 3f f7 cc 34 a5 e5 f1 71 d8 31 15
30 |04 c7 23 c3 18 96 05 9a 07 12 80 e2 eb 27 b2 75
40 |09 83 2c 1a 1b 6e 5a a0 52 3b d6 b3 29 e3 2f 84
50 |53 d1 00 ed 20 fc b1 5b 6a cb be 39 4a 4c 58 cf
60 |d0 ef aa fb 43 4d 33 85 45 f9 02 7f 50 3c 9f a8
70 |51 a3 40 8f 92 9d 38 f5 bc b6 da 21 10 ff f3 d2
80 |cd 0c 13 ec 5f 97 44 17 c4 a7 7e 3d 64 5d 19 73
90 |60 81 4f dc 22 2a 90 88 46 ee b8 14 de 5e 0b db
a0 |e0 32 3a 0a 49 06 24 5c c2 d3 ac 62 91 95 e4 79
b0 |e7 c8 37 6d 8d d5 4e a9 6c 56 f4 ea 65 7a ae 08
c0 |ba 78 25 2e 1c a6 b4 c6 e8 dd 74 1f 4b bd 8b 8a
d0 |70 3e b5 66 48 03 f6 0e 61 35 57 b9 86 c1 1d 9e
e0 |e1 f8 98 11 69 d9 8e 94 9b 1e 87 e9 ce 55 28 df
f0 |8c a1 89 0d bf e6 42 68 41 99 2d 0f b0 54 bb 16
```

Fig 3. S-Box

In the SubByte step, each byte in the state is replaced with its entry in a fixed 8-bit lookup table,

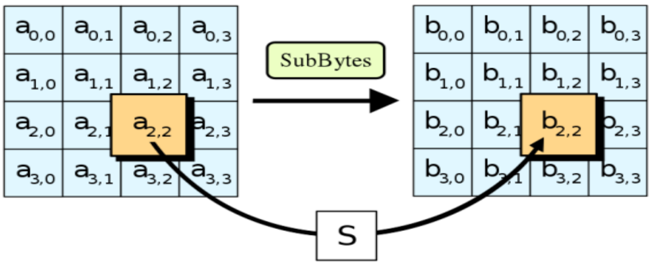

$a_{0,0}$ $a_{0,1}$ $a_{0,2}$ $a_{0,3}$
$a_{1,0}$ $a_{1,1}$ $a_{1,2}$ $a_{1,3}$
$a_{2,0}$ $a_{2,1}$ $a_{2,2}$ $a_{2,3}$
$a_{3,0}$ $a_{3,1}$ $a_{3,2}$ $a_{3,3}$
SubBytes
S
$b_{0,0}$ $b_{0,1}$ $b_{0,2}$ $b_{0,3}$
$b_{1,0}$ $b_{1,1}$ $b_{1,2}$ $b_{1,3}$
$b_{2,0}$ $b_{2,1}$ $b_{2,2}$ $b_{2,3}$
$b_{3,0}$ $b_{3,1}$ $b_{3,2}$ $b_{3,3}$

Fig 4. Sub Byte

2. **Shift Rows:** In the shiftRows, the byte in each row of the state is shifted cyclically to the left. The number of places each byte is shifted differs for each row.

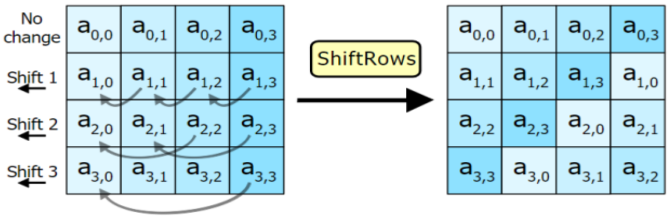

No change
Shift 1
Shift 2
Shift 3
$a_{0,0}$ $a_{0,1}$ $a_{0,2}$ $a_{0,3}$
$a_{1,0}$ $a_{1,1}$ $a_{1,2}$ $a_{1,3}$
$a_{2,0}$ $a_{2,1}$ $a_{2,2}$ $a_{2,3}$
$a_{3,0}$ $a_{3,1}$ $a_{3,2}$ $a_{3,3}$
ShiftRows
$a_{0,0}$ $a_{0,1}$ $a_{0,2}$ $a_{0,3}$
$a_{1,1}$ $a_{1,2}$ $a_{1,3}$ $a_{1,0}$
$a_{2,2}$ $a_{2,3}$ $a_{2,0}$ $a_{2,1}$
$a_{3,3}$ $a_{3,0}$ $a_{3,1}$ $a_{3,2}$

Fig 5. Shift Rows

3. **Mix Columns:** In the MixColumns step, each column of the state is multiplied by a fixed polynomial *C(x)* .

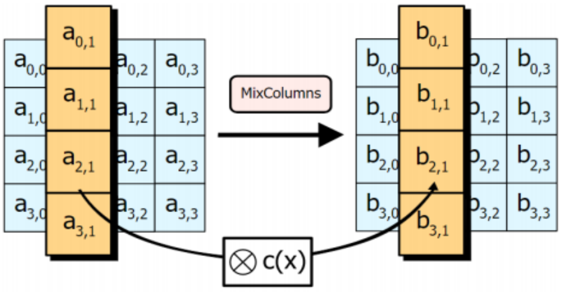

$a_{0,0}$ $a_{0,1}$ $a_{0,2}$ $a_{0,3}$
$a_{1,0}$ $a_{1,1}$ $a_{1,2}$ $a_{1,3}$
$a_{2,0}$ $a_{2,1}$ $a_{2,2}$ $a_{2,3}$
$a_{3,0}$ $a_{3,1}$ $a_{3,2}$ $a_{3,3}$
MixColumns
⊗ c(x)
$b_{0,0}$ $b_{0,1}$ $b_{0,2}$ $b_{0,3}$
$b_{1,0}$ $b_{1,1}$ $b_{1,2}$ $b_{1,3}$
$b_{2,0}$ $b_{2,1}$ $b_{2,2}$ $b_{2,3}$
$b_{3,0}$ $b_{3,1}$ $b_{3,2}$ $b_{3,3}$

Fig 6. Mix Columns

4. **AddRoundKey:** In the AddRoundKey step, each byte of the state is combined with a byte of the round subkey using XOR operation

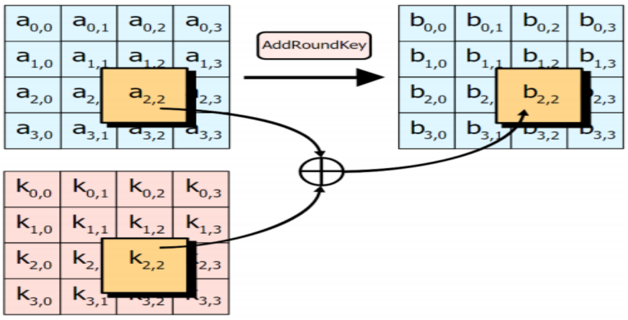

$a_{0,0}$ $a_{0,1}$ $a_{0,2}$ $a_{0,3}$
$a_{1,0}$ $a_{1,1}$ $a_{1,2}$ $a_{1,3}$
$a_{2,0}$ $a_{2,1}$ $a_{2,2}$ $a_{2,3}$
$a_{3,0}$ $a_{3,1}$ $a_{3,2}$ $a_{3,3}$
AddRoundKey
⊕
$b_{0,0}$ $b_{0,1}$ $b_{0,2}$ $b_{0,3}$
$b_{1,0}$ $b_{1,1}$ $b_{1,2}$ $b_{1,3}$
$b_{2,0}$ $b_{2,1}$ $b_{2,2}$ $b_{2,3}$
$b_{3,0}$ $b_{3,1}$ $b_{3,2}$ $b_{3,3}$
$k_{0,0}$ $k_{0,1}$ $k_{0,2}$ $k_{0,3}$
$k_{1,0}$ $k_{1,1}$ $k_{1,2}$ $k_{1,3}$
$k_{2,0}$ $k_{2,1}$ $k_{2,2}$ $k_{2,3}$
$k_{3,0}$ $k_{3,1}$ $k_{3,2}$ $k_{3,3}$

Fig 7. AddRoundKey

IV. CONCLUSION

Thus here in this paper we have discussed various techniques which can be used to secure the cloud which are AES algorithm, encryption, compression, steganography, etc. Along with this we have discussed various challenges and issues regarding cloud security.

REFERENCES

1. Kajal Rani , Raj Kumar Sagar,' Enhanced Data Storage Security in Cloud Environment using Encryption, Compression and Splitting technique', International International Conference on Telecommunication and Networks, 2017.
2. Xiaotong Sun ,' Critical Security Issues in Cloud Computing: A Survey', IEEE International Conference on Big Data Security on Cloud, 2018.
3. Deepak R Bharadwaj, Anamika Bhattacharya, Manivannan Chakkaravarthy, ' Cloud Threat Defense – a Threat Protection and Security Compliance Solution', IEEE International Conference on Cloud Computing in Emerging Markets, 2018.
4. Dr.D.I.George Amalarethinam, B.FathimaMary, ' Data Security Enhancement in Public Cloud Storage using Data Obfuscation and Steganography', World Congress on Computing and Communication Technologies (WCCCT), 2017.
5. DIAO Zhe, WANG Qinghong, SU Naizheng, ZHANG Yuhan, ' Study on Data Security Policy Based On Cloud Storage', IEEE 3rd International Conference on Big Data Security on Cloud, 2017.
6. Rizwana A.R. Shaikh, Masooda M. Modak, ' Measuring Data Security for a Cloud Computing Service', International Journal of Computer Networks (IJCN), 2017.
7. Bih-Hwang Lee, Ervin Kusuma Dewi, Muhammad Farid Wajdi,' Data Security in Cloud Computing Using AES Under HEROKU Cloud', 27th Wireless and Optical Communications Conference (WOCC2018), 2018.