Protection and Security of Data in Cloud Computing

[1.] E. Poonguzhali
Department of CSE
AMCEC, Bengaluru

[2.] Suhas Rao M V
Department of CSE
AMCEC, Bengaluru

[3.] Shanth GK
Department of CSE
AMCEC, Bengaluru

[4.] Mujasem Khanum
Department of CSE
AMCEC, Bengaluru

Abstract- **Cloud Computing is the current trend in the modern technology. Data Security and Data Privacy plays an important role in Cloud Computing. Data Protection is concerned with all the aspects of security of data present in the cloud. There are many data protection methods which are approachable by people to make sure there is less threats and risks. The data present in the cloud is sharable and can be accessed by many applications, but at times it might be risky to expose the data for those applications which have security loopholes in them. The concepts of Data at Rest and Data in Transit are discussed briefly. Different levels of services such as Software as a Service(SaaS), Platform as a Service(PaaS) and Infrastructure as a Service(IaaS) are highlighted.**

Keywords— Data Security, Cloud Computing, Data Protection, Privacy, Risks and threats

I. INTRODUCTION

Cloud computing is a type ofInternetbased computing that provides shared computer processing resources and data to computers and other devices on demand. Cloud computing is when data is stored in a central server, rather than being distributed locally. For instance, you may log into your iCloud account on all of your devices, and your data appears to be stored on each device. In actuality, your data is kept on Apple's server, and pulled to each device when it is needed. Computation in Cloud is service oriented concept and not application based concept. Thus, being service oriented infrastructure overhead and the cost ownership is reduced. It ensures maximum flexibility and the end user gets improved performance [2, 3].

Privacy and security are the major concerns in usage of cloud for data [4]. Features of Data such asprivacy, integrity and protection must be upheld. Different mechanisms and policies are used by different service providersdepending on the type of data, size of data and nature of data. In Cloud Computing, the main advantage is that various organizations can share the data.But, the advantage causes data to be at risk. Therefore, risk to the data needs to be overcome and thus data protection is very much required.

For clouds to be used for the data storage purpose, the doubt which arises is that if we could make use of the third party service providers of cloud or if we could create a organizational internal cloud. When the sensitiveness of the data is too high to store on a public cloud, we use internal organizational cloud. National security data and other highly confidential data are the examples of data which are not to be stored in public cloud. In public cloud, Data exposure could lead to problem which might turn serious. Thus, storing data in cloud which is internally organized is highly recommended.

There are various techniques that are used in the world to protect and secure the data. This paper discussesthe threats caused to the data in the cloud and also tells about the various solutions given by the service providers.

II. LITERATURE REVIEW

In "Cloud Computing Basics," there are information about the different applications which can be made and developed by using the cloud computing concept. It might be very helpful for the developing world.

Large Enterprises still would not prefer cloud because of the security concerns and the issues faced in the cloud environment. To find an optimal solution to all of these issues faced, there are many surveys going on and many service models have been suggested to overcome the issues.

Based on Cloud structure there are many proposed models on data security and the issues faced in securing the data. Many software has been developed to enrich the data security models.

III. SECURITY RISKS, SECURITY THREATS AND CONCERNS IN CLOUD ENVIRONMENT

A. *Loss of Data or Data Leakage*

An example that can be given for data loss is modifying or deleting a certain set of data present in the cloud without taking the backup of the older version of data. This can lead to data loss or any other harmful consequences. Other ways through which problems may arise is by forgetting the encryption keys which may lead to unauthorized access to people. Stealing Data is also one of the major threats in the computing world.

B. *Virtualization*

Virtualization software allows you to run other Operating Systems completely inside your installed OS. Allocation and de-allocation of resources is the main risk in virtualization. Problems may arise if the OS doesn't clear the memory before performing every new task. Memory needs to cleared just after that particular task is finished. If not, Data will be exposed which is very big problem.

C. *Public Cloud Data Storage*

In Public Cloud, Data storage is very much risky. Hackers try and target public cloud which has less privacy. Thus we are recommended to use private clouds.

C. *Multitenancy*

Resources such as memory, storage, CPU etc. could be used by multiple users and this will lead to multitenancy which is a major risk in the cloud computing world. Private clouds also sometimes lead to accidental leakage of data to other users if multiple users access the same resources at a time. One system failure may cause other systems failures and access to private systems become easier.

IV. CLOUD DATA SECURITY

In cloud computation, data security is not only concerned with encryption but also many other processes. Data security requirements is related by and totally depends on these three level of service models, i.e. IaaS, PaaS, and SaaS.

Data is said to be at risk if it is in one of the forms, Data in Rest and Data at Transit. Data in Rest refers to the stored data in the cloud which is at rest and Data at Transit means the data which is moving in/out of the cloud.

A. *Data in Rest*

By the means of Internet, if we are able to access the data present in the cloud, then that data is referred to as Data in rest. It also includes live data and backup data as well.

B. *Data at Transit*

The data which moves out/in to the cloud is referred to as Data at Transit. The data here could be of the form of a database or a file stored in the cloud. This data can be used at any other location points throughout the world.

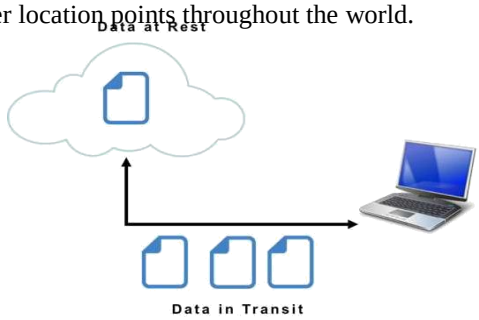
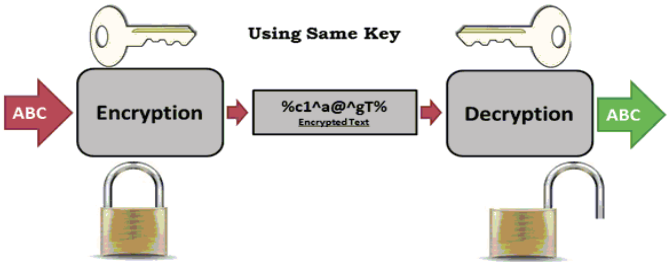


Fig a : Data at Rest and in Transit.

The best way to protect Data at Transit is by Encryption technology. The proposed solution is to add a program to encrypt the data before being fragmented and duplicated on the different storage devices and integrate the decryption functionality in restitution program so that the encrypted data will then be decrypted by the restitution program to present them to the user. Since the size of data to store is generally big, we should use the symmetric encrypting algorithm with the same cryptographic key to both decrypt and encrypt the data.



V. MAJOR SECURITY CHALLENGES

The major challenges involved are:

- *Isolation failure*
- *Malicious attacks from management internally*
- *Insecure or incomplete data deletion*
- *Data interception*
- *Compromise of management interface*

VI. ENCRYPTION PROCESS

There might be different techniques to Data in rest and Data at Transit. The keys used to encrypt data in data at transit is for a lesser period of time but the keys used for encryption for data in rest can be of longer time. Thus, it shows the difference of usage of keys.

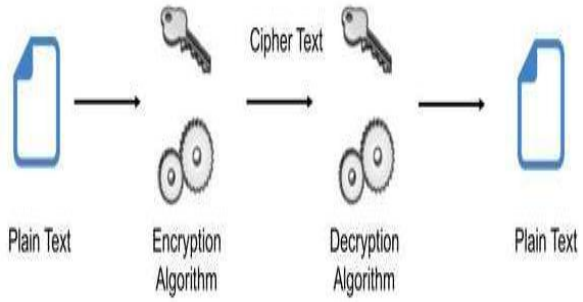


Fig b: Basic Cryptography Process

In the cryptographic process, the plain text is converted to cipher text by usage of a key called as encryption key. The cipher text which is resulted after the encryption process is next decrypted by usage of a key known as decryption key.
The types of cryptography process are:

A. Block Ciphers

In data Encryption, an algorithm and a cryptographic key is applied for a block of data rather than applying it for each bit at a given time.

At the end of this mechanism, cipher text is formed which again needs to be decrypted in order to bring it back to the human understandable form.

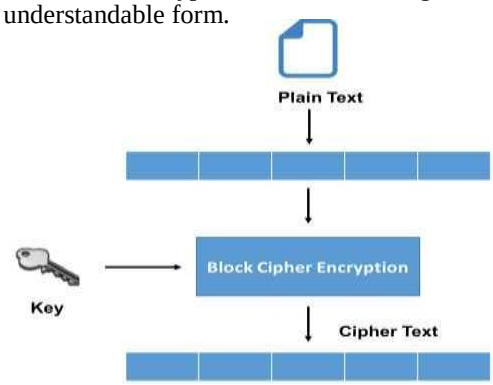


Fig c: Block Cipher Mechanism

B. Stream Cipher

The mechanism depends on the current state of cipher and thus its called state cipher. The encryption process is performed on each bit rather than block of data at a time.

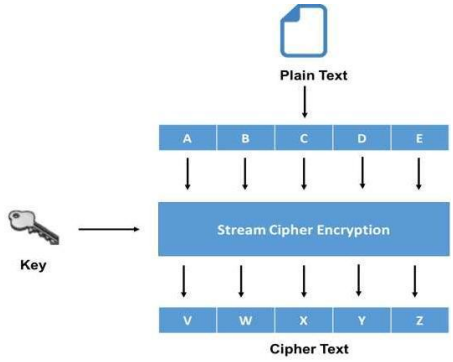


Fig d: Stream Cipher Mechanism

The data is now in stream of encrypted bits which later again needs to be decrypted by using a key of decryption and an algorithm of it which produces back the plain text from the cipher text.

C. Using AES as an encryption algorithm to crypt data

AES is abbreviated as Advanced Encryption Standard which is a symmetric encryption algorithm. The Encryption and Decryption algorithm is stated below.

```
Inp : table T1 , key K1
Out : table T1 altered
FuncAES (T1, K1)
Start
KeyExpansionFunc (K1, TK1);
AddKeyRoundFunc (T1, TK1 [0];
for (j = 1; j<NR; j + +)
Round (T1, TK1 [j]);
FinalRoundFunc(T1, TK1 [NR]);
End
```

Encryption algorithm

```
Decryption(T1, K1)
{
KeyExpansionFunc(K1, RK);
AddRoundKeyFunc(State, RK[NR]);
for (j=NR-1; j>0; j--)
 {
InvShiftRowsFunc(T1);
InvSubBytesFunc(T1);
AddRoundKeyFunc(T1, RK[j]);
InvMixColumnFunc(T1);
}
InvShiftRowsFunc(Outp);
InvSubBytesFunc(Outp);
AddRoundKeyFunc(Outp,RK[0]);
}
```

Decryption Algorithm

VII. CONCLUSION

Several security issues were highlighted and appropriate measures were suggested to be followed. All the concepts namely Virtualization, Public cloud data storage, Multitenancy were briefed. The encryption process was explained and the different mechanisms of encryption were discussed. The different states of data are shown. An AES model was displayed which could be followed by people around the world. Block Cipher and Stream Cipher mechanisms were shown with the diagrams in detail.

REFERENCES

[1] J. Srinivas, K. Reddy, and A. Qyser, "Cloud Computing Basics," *Build. Infrastruct. Cloud Secur.*, vol. 1, no. September 2011, pp. 3–22, 2014.

[2] M. A. Vouk, "Cloud computing - Issues, research and implementations," *Proc. Int. Conf. Inf. Technol.Interfaces, ITI*, pp. 31–40, 2008.

[3] P. S. Wooley, "Identifying Cloud Computing Security Risks," *Contin. Educ.*, vol. 1277, no. February, 2011.

[4] A. Alharthi, F. Yahya, R. J. Walters, and G. B. Wills, "An Overview of Cloud Services Adoption Challenges in Higher Education Institutions," 2015.

[5] MostaphaDerfouf, "Vulnerabilities and storage security in cloud computing", 2015.

[6] Dr.K.B.PriyaIyer, "Analysis of cloud security", 2016