International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 04 | Apr 2019 www.irjet.net p-ISSN: 2395-0072

CLOUD COMPUTING WITH ENCRYPTION

Vishu aggarwal[1], Vaibhav kumar[2],Nitin rawat[3],Ashwani saini[4],Sanjeev dhewa[5],

Asst prof Ms.ashu jain[6]

[1,2,3,4]B.Tech Student, Dept. of Information Technology, Dr. Akilesh Das Gupta Institute of Technology and Management Delhi
[5]Mentor: Assistant Professor Ms. Ashu jain, Dept. of Information Technology, Dr. Akhilesh Das Gupta Institute of Technology and Management, Delhi-110053

Abstract - *The aim of this project is provide some services provided by cloud computing to store data at a local level. Cloud computing has become one of the most widely used technologies these days but there are many security issues involved with cloud computing. There are also many privacy issues involved with cloud computing. These security issues and privacy issues are handled by encrypting the data to be stored on the cloud using advanced encryption standard algorithm. Advanced encryption standard is a very strong encryption algorithm and no practical cryptanalysis attack against advanced encryption standard algorithm has not been discovered yet which makes it suitable to encrypt the data to be stored on the cloud.*

Key Words: Encryption,Decryption,AES,Cloud,Cryptanalysis

1.INTRODUCTION

Cloud computing is the on demand availability of computer resources, especially data storage and computing power. The term Cloud refers to a Network or Internet. The concept of Cloud Computing came into existence in the year 1950.

Cloud Computing is highly cost effective and offers on-demand self-service. Cloud Computing offers online development and deployment tools. cloud-computing providers offer their "services" according to different models of cloud computing. Theses three different models are Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). Cloud computing does not require to install a software to access or manipulate cloud. IaaS provides access to fundamental resources, PaaS provides the runtime environment for applications, SaaS allows to use software applications as a service to end-users. Cloud Computing also offers load balancing. The public cloud allows systems and services to be accessible to the general public. Security in cloud computing is one of the major concern. Data has to be first encrypted before storing it to server. Cloud Security Alliance (CSA) stack model defines the boundaries between each service model.

2. ENCRYPTION AND CLOUD COMPUTING

In our project we have planned to implement the idea of storing data on a server securely. Data is first encrypted and then stored on a server. When a person wants to download the data from the server he first has to decrypt the data and then download it. A password is used to decrypt and encrypt a data. In this project we have created a website.
Our project has two main modules one is user module and other one is admin module. The user module has options for registering a user , login, view profile ,upload file , download file , calculation module for data file , upload data using aes encryption. The admin module has options for view user , view file and modify user.
Using AES encryption makes data storage on server very secure hence the name given to the project is secure data storage on cloud. using this software storage on cloud becomes very secure and less prone to attackers.
The objective of the project is to create a technology that can make storage on cloud secure and for that we have used aes encryption for storing data on cloud. The website will be very simple to use and will be created using html. Coding for encryption will be done using java. When user downloads a file he has to provide a key which is used for decrypting the file . Cloud computing posses many security and privacy concerns that can be handled only by using some appropriate encryption technique. The service provider can access the data in the cloud at any time and he can also accidently alter the data thus an ggod encryption is necessary in cloud computing. Many issues involved in cloud computing easily gets solved by encrypting the data using a good encryption technique. Also all the data is transferred using Internet, data security is a major concern in the cloud and only a good and strong encryption technique can provide data security.

3. AES ENCRYPTION

The encryption used in this software is AES encryption. No Practical cryptanalysis attack against AES encryption has not been discovered yet. As no practical cryptanalysis attack against AES has not been discovered yet attacker cannot decrypt a file encoded using aes. There is a very huge need of security in storing data on cloud as the data stored on cloud gets out of control of user and aes easily secures the data

before it gets stored on cloud. AES is a very popular and widely adopted encryption algorithm. AES is faster than triple des algorithm and more secure than des algorithm. AES is based on substitution-permutation network and is a Iterative cipher. Unlike DES, the number of rounds in AES is variable and it has 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each round has four sub-processes. AES has built-in flexibility of key length. The AES security is assured only if it is correctly implemented. AES is a subset of the Rijndael block cipher developed by two Belgian cryptographers, Vincent Rijmen and Joan Daemen. In Advanced encryption standard algorithm the same key is used for both encryption and decryption. Advanced encryption standard algorithm has Software implementable in C and Java. AES performs all its computations on bytes rather than bits. AES treats the 128 bits of a plaintext block as 16 bytes. The sub-processes in the rounds of advanced encryption standard algorithm are Byte Substitution, Shiftrows , MixColumns and Addroundkey. The process of decryption of an AES ciphertext is similar to the encryption process in the reverse order.

4. CONCLUSIONS

This project works on the concept of cloud computing and data security using AES encryption technique. This project aims to feature the basic services provided by cloud computing and to encourage users to use this growing technology. Using aes encryption storage of data on cloud is made extremely secure. No practical cryptanalysis attack against AES encryption has not been discovered yet which makes AES encryption extremely secure.
Cloud computing poses privacy concerns and these privacy concerns are easily handled using advanced encryption standard algorithm.

REFERENCES

[1] http://www.thoughtsoncloud.com/2014/03/a-brief-history-of-cloud-computing/.
[2] http://www.thoughtsoncloud.com/2014/03/a-brief-history-of-cloud-computing/.
[3] http://www.thoughtsoncloud.com/2014/03/a-brief-history-of-cloud-computing/.