# Mechanism for Protecting Storage Data with Encryption Algorithm in Cloud Computing Environment

**Umesh Pratap Singh**
Assistant Professor
Department of Computer Science & Engineering
Shri Ramswaroop Memorial Group of Professional Colleges, Lucknow, India

*Abstract*— Cloud computing is the evolving technology for the several years. It allows user to store bulk amount of data in cloud storage and use as requirement from anywhere of the world through any display device. Since cloud computing is based on internet, privacy issues, data security, confidentiality, and authentication is encountered. In order to secure the data, a multiple encryption algorithms and mechanisms are used. I have selected to use of authentication technique with an encryption algorithm. “Two level of secure transfer of data mechanism” ensures all the three protection scheme of authentication, data security and verification, at the same time. AES encryption algorithm to make confidentiality of data stored in server. This proposed architecture of two way mechanism makes it tough for hackers to decipher data and hence the security system to secure data stored in cloud environment.

***Keywords:*** Cloud Environment, AES, Data, Security, Client, Server

## I. Introduction

Cloud computing is evolving and considered as next era architecture for computing. Customers are very focused about the risks of Cloud Computing if not properly secured. To maintain the protection of data and privacy in cloud computing infrastructure is a new challenge, as cloud services process users’ data on machines that the users do not operate this can lessen users’ control. Privacy issues are central to user concerns about adoption of cloud computing, this may prove fatal to many different types of cloud services. The client must have the ability to store the data securely, verify the integrity of the data, and share the data securely with specifies group of users.

Typically cloud computing is a combination of computing technologies accessible to internet. Historically the client’s or company’s data is stored data centers with firewall and other security techniques used to protect data against hackers who access these data. Since the data is stored in data centers in limits of companies, the control over the data was more and well defined via procedures that could be used for accessing its own data. However in cloud computing, since the data is stored anywhere across the world, the clients have less control over the stored data. To build the trust for the growth of cloud computing the cloud providers must protect the user data from un-authorized disclosure. One way could be encryption of data (Encryption done using AES) on client side before storing it in cloud storage and send the same to server where it will be stored in server and vice versa. Encryption/decryption service if provided by same cloud storage provider, the data compromise cannot be done since same provider has access to both storage and security service. The data from Storage Cloud is decrypted and stored in memory. On user request data is decrypted on server side and send the same data to the client side for user over the internet using security method which is then compared with AES techniques of original data stored in Security Cloud. Finally, this software/application provides the user with the ability to store the encrypted data in Storage cloud and encryption/decryption keys in security cloud service. Other benefit of AES method is that it reliefs the client from any kind of key management or over head is maintenance of any key information related to data on it device, because of which it allows the client to use any browser enabled devices to access such service.

### A. Keywords

Cloud computing; encryption and decryption service; data protection.

## II. Problem Statement

With cloud computing, organizations can use services and data is stored at any physical location outside the organization. This facility raised the different security questions like privacy, confidentiality, integrity etc and required a trusted computing environment wherein data security can be maintained. To need trusted computing environment, there is required of a system which performs authentication, verification and encryption/ decryption data transfer, so that environment can maintain data confidentiality.

## III. Related Works

### A. Selection of AES

The encryption/decryption techniques can be done via symmetric key or asymmetric key. In symmetric algorithms, both parties share the secret key for both encryption/decryption, and from privacy perceptive it is important that this key is not compromised, because cascading data will then be compromised. Symmetric encryption/decryption requires less power for computation. On the other hand asymmetric algorithms use pairs of keys, of which one key is used for encryption while other key is used for decryption.

Generally the private key is kept secret and generally held with the owner of data, while the public key can be distributed to others for encryption. The secret key can't be obtained from the public key. The AES algorithm work on the basis of following procedures:

1) 128--bit data iinput
2) 128 to 256--bit secret key
3) Round--based::
   SubByttes: Non--lliinear byte substitution
   Shift Row:: Word rotation
   MixColumn:: llinear wordttransfformation
   Add RoundKey:: modulus 2 addition with round key

 

4) Encryption and Key Schedule
   Use t same basic operations
   Decryption uses iinverse
   Operations of encryption [1]

### *B. Data encryption*

The threat of data compromise increases in the cloud and interactions between risks and challenges which are either unique to cloud, or more dangerous because of the architectural or operational characteristics of the cloud environment. For examples, insufficient authentication, authorization, and audit (AAA) controls; inconsistent use of encryption and software keys; operational failures; data center reliability; and disaster recovery. Contractually demand providers wipe persistent media before it is released into the pool and also provide backup and retention strategies. There is the utmost need to encrypt multi-use credentials, such as credit card numbers, passwords, and private keys, in transit over the Internet. Cloud provider networks may be more secure than the open Internet, they are by their very architecture made up of many unrelated components, and unrelated organizations share the cloud. Therefore it is important to protect this sensitive and regulated information in transit even within the cloud provider's network. Typically this can be implemented with equal ease in SaaS, PaaS, and IaaS environments. For long-term archival storage, some customers encrypt their own data and then send it as cipher text to a cloud data storage vendor. The customer then controls and holds the cryptographic keys and decrypts the data, if necessary, back on their own premises. Encrypting data at rest is common within IaaS environments, using a variety of provider and third party tools. Encrypting data at rest within PaaS environments is generally more complex, requiring instrumentation of provider offerings or special customization. Encrypting data at rest within SaaS environments is a feature cloud customers cannot implement directly, and need to request from their providers. Encrypting data on backup media can protect against misuse of lost or stolen media. However, as a customer and provider of data, it is your responsibility to verify that such encryption takes place. Cloud customers and providers need to guard against data loss and theft. Encryption of personal and enterprise data is strongly recommended by laws and regulations around the world. Cloud customers want their providers to encrypt their data to ensure that it is protected no matter where the data is physically located. Likewise, the cloud provider needs to protect its customers' sensitive data. Cloud environments are shared with many tenants, and service providers have privileged access to the data in those environments. Thus confidential data hosted in a cloud must be protected using a combination of access control, contractual liability, and encryption, which offers the benefits of minimum reliance on the cloud service provider and lack of dependence on detection of operational failures.

## IV. PROPOSED DIAGRAM

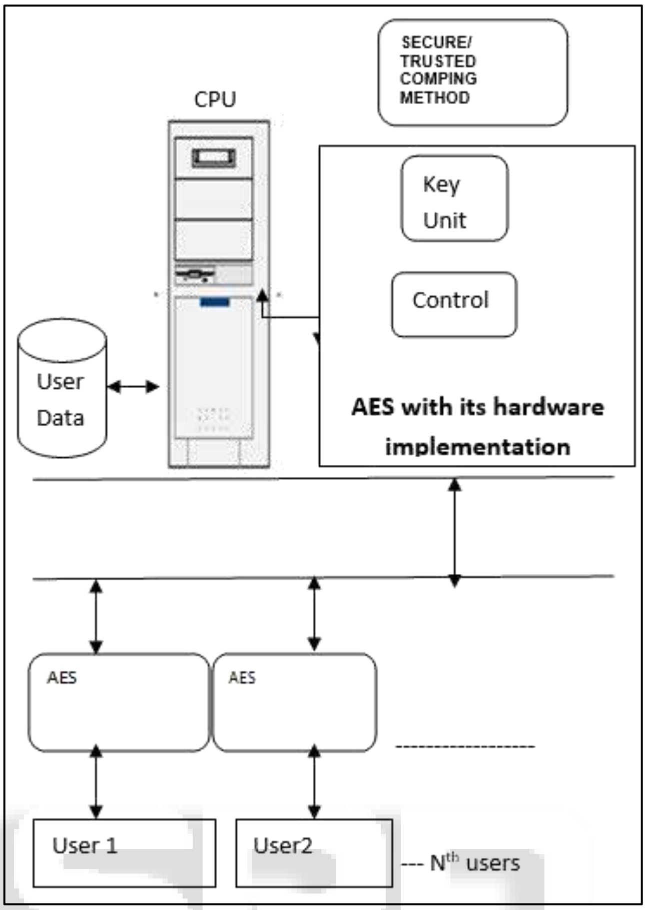


Fig. 1: Proposed Architecture

Steps to insure data security:

1) Sign up
2) Login with user ID & Key
3) Encryption of user data with 128 bit key AES architecture at client side
4) Uploading / Downloading Data Encryption- AES
5) Data is stored / retrieved from Storage server (User Data).
6) Logout.

## V. CONCLUSION

Cloud computing uses various technique to secure performance in an efficient manner depends on network, virtualization environment, hypervisors which sit on operating system to control the virtual plays. The growth of cloud depends on both safe and cost effective nature to make the institutions and individuals to adopt the cloud.

Our research is focusing on providing solution to security issues and develops a model to give security of cloud infrastructure.

## REFERENCES:

[1] "Announcing the ADVANCED ENCRYPTION STANDARD (AES)", Federal In-formation Processing Standards Publication 197. United States National Institute of Standards and Technology (NIST). November 26, 2001.

[2] Advanced Encryption Standard Secured Architecture and its Auto-Test Capabiilliittiies.pdf
[3] Cloud Computing and Intelligent Systems (CCIS), 2012 IEEE 2nd International Conference
[4] Deyan Chen and Hong Zhao “Data Security and Privacy, Protection Issues in Cloud Computing” 2012 IEEE International Conference on Computer Science and Electronics Engineering.
[5] Grid and Cooperative Computing (GCC), 2010 9th International Conference.
[6] Mohamed Al Morsy, John Grundy and Ingo Müller “An Analysis of The Cloud Computing Security Problem” Proceedings of APSEC 2010 Cloud Workshop, Sydney, Australia, 30th Nov2010.
[7] William Stallings, "Cryptography and Network Security", 2009.