International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume: 3 | Issue: 2 | Jan-Feb 2019 Available Online: www.ijtsrd.com e-ISSN: 2456 - 6470

# Cloud Cryptography

**Padmapriya I, Ragini H**

MOP Vaishnav College for Women, Nungambakkam, Chennai, Tamil Nadu, India

**ABSTRACT**
Cloud computing is the emerging trend in today's world. Cloud computing is not a separate technology, it is platform which provides platform as a service, Infrastructure as a service and Software as a service. The most important thing with cloud is that we hire everything from a third party or store our important data's in a third parties place .Here comes the major issue of how our data's are secured. In this paper, we discuss about how to protect our data's in the cloud with various cryptographic techniques.

***Keywords:*** *Public key, private key, encryption, decryption, cipher text*

## 1. INTRODUCTION

Cloud computing –an upcoming trend in computing world, when compared with traditional computing process has many advantages. In traditional computing, we need to have all our computing resources in the premises where we are going to work. But it is not the case with cloud computing. Similarly, setup an environment with all the needed resources will amount to a large pay and not all companies can offered for all the needed resources, not all the resources will be used all the time. But in cloud , we hire and use what we need and pay only for what we have used .Thus ,cloud has many advantages when compared to traditional computing techniques. Every good thing will have some defects associated with it. Likewise, the major issue cloud has is "Security issue". So, one way to secure the data on the clod environment is using cryptographic techniques. This includes the use of private and public keys, which plays an important role in encrypting the data from a plain text to cipher text. Public keys are given to those who are going to decrypt the data and use it ,where the private keys are used only by the own user of the data to encrypt it.

**Literature review:**
Survey paper on cloud storage security by
SUNITA SHARMA, AMIT CHUGH, helped us in understanding how to secure data on the cloud using Kerberos authentication service and cloud proof technique.

Strengthen Cloud Computing Security with Federal
Identity Management Using Hierarchical Identity-Based

Cryptography by
Liang Yan, Chunming Rong, and Gansen Zhao made us understand about securing the data's on the cloud through various identity based cryptographic techniques.

Secure User Data in Cloud Computing Using Encryption Algorithms by
Rachna Arora, Anshu Parashar gave us knowledge about the various algorithms used for cryptographic techniques.

Data Security in Cloud Computing with Elliptic Curve Cryptography by
Veerraju Gampala, Srilakshmi Inuganti, Satish Muppidi greatly helped us to know about a new technique for encrypting data on the cloud.

Enhancing Security in Cloud computing using Public Key Cryptography with Matrices by Birendra Goswami, Dr. S. N. Singh helped us know about a mathematical technique-matrices, for encrypting and decrypting cloud data's.

**Issues with Data's stored on cloud:** [1]
**Issue 1: (Data Breaches)**

In cloud all data's get stored in online rather than getting stored in a secured premises which makes it more unsecured.

**Issue 2: (Hijacking of accounts)**
Once attackers get one's username and password ,they get access to the data's on the cloud like a legal user.

**Issue 3: (Insider Threats)**
This attack is from the insider who has an authorized access, but uses it to perform unauthorized activities.

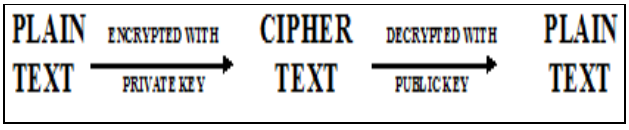
**Issue 4: (Malware injection)**
This attack is like injecting malware into our cloud service that becomes a serious threats to the cloud users.

**Issue 5: (DOS Attacks)**
DOS attacks could be putting more request than the cloud server could handle to crash the server.

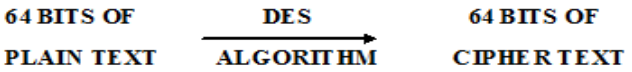
In addition to this there are many issues like, Insecure API's, Insufficient due diligence, Shared Vulnerabilities, Data loss etc. There are several algorithms Proposed to handle these issues.

**Algorithms:**
To handle these above threats,many algorithms were proposed,

**RSA Algorithm:**
Here, public and private keys are used. Private keys are used to encrypt the data by the own user of the data and stored on the cloud and the public keys are used to decrypt the data's when it is needed by other's to access it. The disadvantage that data is secured until Private key is unknown to others. once the private key is known by intrude, full privacy is lost.

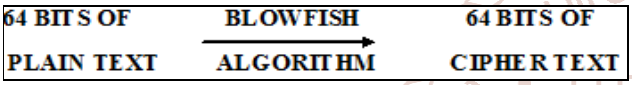


**DES Algorithm:**
In DES, a block of 64 bits of plain text is sent as an input to the DES algorithm which produces 64 bits of cipher text and the cipher is converted into plain text using the same key. The key length here is 56 bits, which is considered to be very small and this is considered to be its serious disadvantage.




**AES Algorithm:**
AES is alternative to DES, as DES key length used for encryption is very small. This algorithm uses a 128-bit length key to encrypt the data. The data to be stored on the cloud is encrypted using AES algorithm and is sent to the cloud service provider. Any request to access the data is satisfied by decrypting the data with the encrypted key and given to user for access as a plain text. No plain text is stored on the cloud environment.

**Blowfish:**
Blowfish takes 64 bits block of plain text and encrypts it into cipher text and stores the cipher text into the service providers place with a key having variable lengths from 32 bits to 448 bits.




**Homomorphic:**
Homomorphic is a encryption technique where encrypted cipher data is stored in the cloud Service providers place and When one needs access to the data can work on the cipher text as though it a real plain text.

**Drawbacks with these algorithms:**
All the above algorithms uses the concept of keys for encrypting the data .The major drawbacks of all the algorithms are ,once if the key used to encrypt the data is known ,an intruder can easily modify the data ,for Securing what these several actions are done.

**Solution to these Drawbacks:**
The drawbacks of the algorithms could be solved by using these proposed techniques like,

**Federal Identity Management:**
Here, each user is given a unique digital identity using which one can have access to the different cloud services and its data's. The digital identity are given in such a way that they cannot be guessed as easily as possible. [2]

**Identity based cryptography:**
In this method, public identifier of a user is his/her public key, that can be used for securing data on the cloud[2]

**Federal Identity Management:**
This method is a development from identity based cryptography, but it adds solutions to avoid the scalability problems. [2]

**Elliptic curve cryptography:**
This is a cryptographic technique based on elliptic curve theory to generate cryptographic keys rather using the traditional key generation techniques. It provides greater level security with 164 bit keys.[3]

**Securing data on the cloud by cryptography with matrices:**
This method mainly has two parts: One is Preprocessing, which includes data shuffling and traversing of the data. The second part deals with Key generation, Key agreement and encryption and decryption processes.[6]

**Diffie Hellmann Key Exchange:**
It has two keys-Private and public keys. The sender of the data encrypts the data with his Private key and receivers public key and send its to the receiver. The receiver decrypts the data using his Private key and senders public key, thus providing two ways of authentications.[4]

**Securing data on the cloud with cloud proof:**
With these techniques, one can detect the threats occurrence to the data and also report it to the CSP's with valid proof.

**Kerberos authentication services:**
Here Kerberos techniques were used to authenticate the valid user for securing data. This uses the complex Ticket granting algorithms for creating tickets and granting tickets for each users. [6]

**Conclusion:**
Cloud environment has benefitted people of different communities. At the same time it has its own drawbacks. Every great things have to face its own drawbacks. Taking the good part of it and providing safety measures for the flaws, one can use cloud technology and benefit at its fullest.

**References:**
[1] **Secure User Data in Cloud Computing Using Encryption Algorithms by** Rachna Arora(Research Scholar, HCTM, Kaithal, Haryana), Anshu Parashar (Associate Professor, HCTM, Kaithal, Haryana)

[2] **Strengthen Cloud Computing Security with Federal Identity Management Using Hierarchical Identity-Based Cryptography by** Liang Yan(University of Stavanger, Norway), Chunming Rong(University of Stavanger, Norway), and Gansen Zhao(South China Normal University, China)

[3] **Data Security in Cloud Computing with Elliptic Curve Cryptography by** Veerraju Gampala, Srilakshmi Inuganti, Satish Muppidi

[4] **Data Security in Cloud Architecture Based on Diffie Hellman and Elliptical Curve Cryptography by** Neha Tirthani, Ganesan R

[5] **Survey paper on cloud storage Security by** Sunita Sharma **(**M.Tech. Student, Dept. of CSE, Lingayas University Faridabad, Faridabad, India)**,** Amit chugh2 **(**Assistant Professor, Dept. of CSE, Lingayas University Faridabad, Faridabad, India)

[6] **Enhancing Security in Cloud computing using Public Key Cryptography with Matrices by** Birendra Goswami **(**Faculty Member, UMA, Ranchi), Dr. S. N. Singh (HOD, Deptt. Of IT, XISS, Ranchi)