To Enhance Multimedia Security in Cloud Computing Environment Using RSA and AES

P.V.NITHYABHARATHI, T.KOWSALYA, V.BASKAR

Abstract— **Cloud computing is raising field because of its performance, high availability, cost efficiency and many others. In this the data will be stored in storage which is provided by service providers. Due to lack of proper security control policy and weakness, which lead to many vulnerability in cloud computing so still many business companies are not willing to adopt these cloud computing technology. This exclusive pattern brings many new security challenges, which have not been well implicit. The major issues in the cloud computing are data integrity, data theft, privacy issues, infected application, data loss, data location, security on vendor level, security on user level. In previous section combination of RSA and DES which is represented as an crossbreed algorithm. It is mainly adopted for the optimization of multimedia data security in cloud computing. Their usage is limited to convey of keys for symmetric key encryption and in signature schemes where data size is usually small. To overcome this, the replacement of AES instead of DES with the combination of RSA was done in multimedia data due to the inbuilt weaknesses in DES that allows the encryption to be broken using certain methods of attack. Some of the applications of AES are still inflexible to various type of cracking techniques, which makes it a better choice even for top secret information. AES data encryption is more scientifically capable and graceful cryptographic algorithm, but its main force rests in the key length. The time necessary to break an encryption algorithm is straightly related to the length of the key used to secure the communication. AES allows you to choose a various type of bits like 128-bit, 192-bit or 256-bit key, making it exponentially stronger than the 56-bit key of DES.**

Index Terms— **AES, Could computing, DES and RSA.**

I. INTRODUCTION

The new data storage in "Cloud" brings about many challenging design issues which have deep influence on the security and performance of the overall system. One of the biggest concerns with data storage in cloud is data integrity proof at un trusted servers. For example, the storage service provider may decide to hide the data errors from the clients for the benefit of their own by using the Byzantine failures occasionally, what is more serious is that for saving money and storage space the service provider might neglect to keep or intentionally delete rarely accessed data files which belong to an ordinary client. Consider the large amount of the outsourced electronic data and the client's constrained resource capability, the heart of the problem can exist generalized as how can the client find an efficient way to perform review integrity verifications without the local copy of data files. Although scheme with private auditability can achieve higher scheme good organization, public auditability allows anyone, not just the client to brave the cloud server for truth of data storage while keeping no private information.

In Cloud computing, the remotely stored electronic data might not only be accessed but also updated by the clients, e.g., through modification of block, deletion, insertions are all performed. Unfortunately, the state of the art in the context of remote data storage mainly focus on fixed data files and the importance of this active data updates has received limited attention so far. But still many business companies are not willing to approve multimedia data security in cloud computing technology due to lack of proper security control policies. RSA and AES cryptographic algorithms are adopted here for the optimization of multimedia data security in cloud computing.

II. RELATED WORK

Cloud services as a utility service and begin to use them almost instantly. These features that make cloud computing so flexible with the fact that services are accessible anywhere any time lead to several potential risks. The key intent of this research work is to investigate the existing security schemes and to ensure data confidentiality, integrity and authentication. In model RSA algorithm and DES algorithm cryptographic algorithms are adopted for the optimization of data security in cloud computing. These days encryption techniques which use large keys are seldom used for data encryption due to computational overhead. Their usage is restricted to transport of keys for symmetric key encryption and in signature schemes where data size is generally small.

A novel highly decentralized information accountability framework to keep track of the actual usage of the users' data in the cloud. An object-centered approach that enables enclosing our logging mechanism together with users' data and policies [7]. The JAR programmable capabilities to both create a dynamic and traveling object, and to ensure that any access to users' data will trigger authentication and automated logging local to the JARs.It mainly focuses on security, scalability, and efficiency ABE-based framework for patient-centric secure sharing of PHRs in cloud computing environments, under the multi-owner settings. To address the key management challenges, conceptually divide

Manuscript received Jan, 2014.

P.V.Nithyabhararthi, *Computer Science and Engineering, United Institute of Technology, Coimbatore, India.*

T.Kowsalya*, Computer Science and Engineering, United Institute of Technology, Coimbatore, India,.*

V.Baskar*, Computer Science and Engineering, A.S.L Pauls College of Engineering and Technology, Coimbatore, India.*

ISSN: 2278 – 7798

the users in the system into two types of domains, namely public and personal domains (PSDs). In particular, the majority professional users are managed distributive by attribute authorities in the former, while each owner only needs to manage the keys of a small number of users in her personal domain. In this way, this framework can simultaneously handle different types of PHR sharing applications' requirements, while incurring minimal key management overhead for both owners and users in the system. In addition, the framework enforces write access control, handles dynamic policy updates, and provides break-glass access to PHRs under emergence scenarios.

III. SYSTEM MODEL

Data integrity and privacy are the main issues in cloud storage environment. The requested multimedia data is transferred securely from cloud server to client. Here the Security is provided with combinations of cryptographic algorithms.

1).RSA (Riverst, Shamir, Adleman)

2). AES (Advanced Encryption Standard)

In an encryption method, the message is encrypted using an encryption algorithm, rotating it into an unreadable cipher text this is usually done with the use of an encryption key, which denotes how the message is to be encoded. An authorized party can decode the cipher text by using a decryption algorithm, which regularly requires a secret decryption key, that challengers do not have access to it. For practical reasons, an encryption scheme usually needs a key-generation algorithm to arbitrarily produce keys.

A. Encryption of image

Original image is divided into a random number of blocks. And it creates the random number for each block and rotates the each pixel value by using the random number.

These random numbers are stored in the file and encrypted and then send to the receiver. The main purpose of the receiver is to decrypt the encrypted random file. The decrypted file is stored in the text file. This random file is used for the image decryption.

B. Encryption Image using Pixel Rotation

Input: Original Image
Output: Encrypted Image, and Random Number File
Steps:
1. It will read Image file in the beginning stage.
2. Then the image files divide into number blocks.
3. And it generate random number for each block
4. Now rotate each pixel by using the random number.

   (val>>n) | (val<<(8-n)) Where val is the actual value of the image pixel, and n represent the number bit rotation.
5. Encrypt the random number file using RSA algorithm.

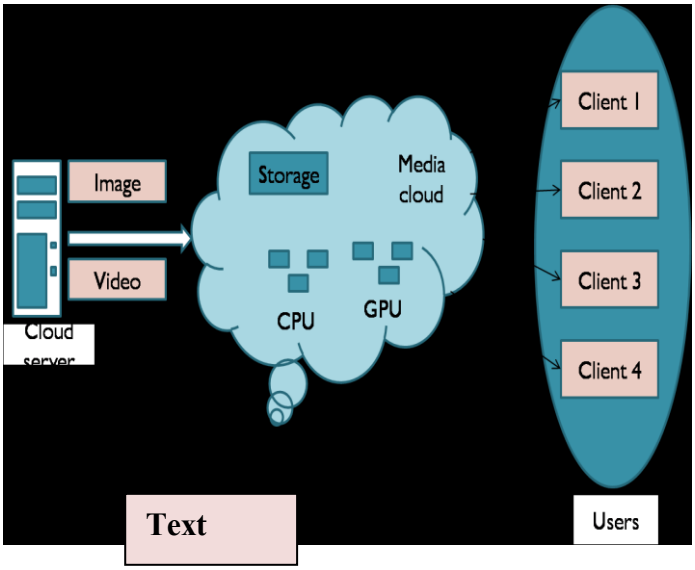


Fig Architecture diagram for proposed system

C. Storing and Retrieving of Data from Cloud

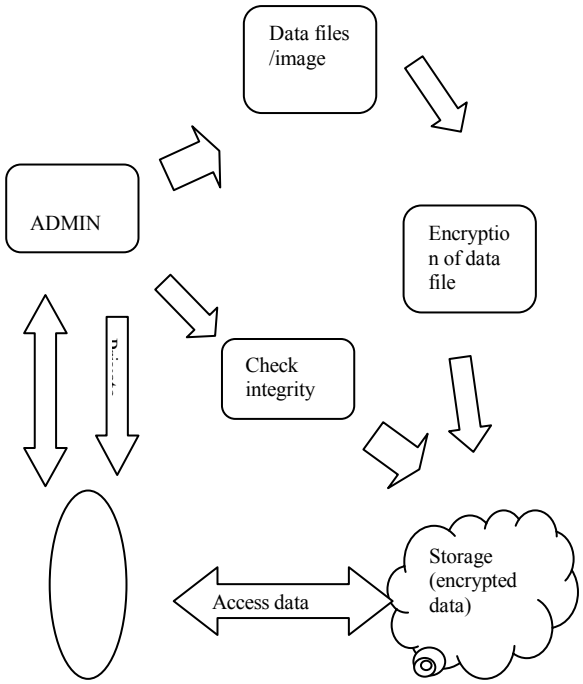


Fig Storing and retrieving data from cloud

- In the First step, pick any text file, image and then it will be uploaded in the cloud computing work.
- It will check the integrity of data using data integrity process.
- The data files text file, images are encrypted for a secured storage.
- To encrypt text file, images the cryptography RSA and AES algorithms to be used.
- In this the authorized user can easily access the data's from the cloud storage by private.

ISSN: 2278 – 7798

IV. MODULE DESCRIPTION

A. Cloud setup and data transformation

College consists of various department like information technology, computer, mechanical, electronic etc. Each department has different computer labs. Each branch requires different software, platforms which are purchased by the college which needs to be installed on every computer of different labs according to the requirement. Thus by setting up the cloud there will be no need of doing so. All the software and form need to be installed only once which will be stored on cloud server. The designed cloud storage is used within Intranet by using LAN connection and also by using Wi-Fi. Principal of the college will be admin. So that all activities performed by staff members and students will be known to him. Each student and staff member will be assigned a unique-id for login purpose which will help in maintaining security.

Here it denotes that whenever a student request for a particular software or platform he has to login using his/her id Allocated to him/her. If he/her is a valid user then the request is forwarded to the Cloud server. The cloud server with the help of database server validates the user and provides services**.**

The users of the drive are as follows:

a) Staff
- Have rights to upload data.
- Have rights to upload Software's.
- Have rights to download data.
- Have rights to add platform, software etc.
- User name as Employee ID.
- Password will be user defined.

b) Examination-cell authorities
- Can upload notices about Examination.
- Can upload various Examination Results.

c) Principal
- Can upload notices regarding student and teachers.
- Can give suggestion to teachers and students.

d) Student
- User name as Student ID and password-user defined.
- Have only access to read and download data.
- They can give feedback to teachers.

B. Encryption and decryption in RSA

RSA scheme is a block cipher in which the plain text and cipher text are integer between 0 and n-1 for some n. A typical size for n is 1024 bits or 309 decimal digits. That is n is less than 2^{1024}. RSA scheme has since that time reigned supreme as the most widely accepted and implemented general purpose approach to public key encryption. The RSA algorithm without digital signature is not secured. A user of RSA creates and then publishes the product of two large prime numbers along with an auxiliary value, as their public key. The prime factors must be kept secret. Anyone can use the public key to encrypt a message, but with currently published methods, if the public key is large enough, only someone with knowledge of the prime factors can feasibly decode the message.

In RSA, encryption keys are public, while the decryption keys are not, so only the person with the correct decryption key can decipher an encrypted message. Everyone has their own encryption and decryption keys.

The keys must be made in such a way that the decryption key may not be easily deduced from the public encryption key. Security of RSA Brute force attack.

Key generate in RSA algorithm

Select two prime numbers randomly p and q

For example p = 3 and q = 11

Compute n = p * q

(i.e.) n = 3 * 11 = 33

Compute Φ (n) = (p - 1) * (q - 1)

Φ(n) = (3 - 1) * (11 - 1)

Φ (n) = 2 * 10

Φ (n) = 20

Choose e such that 1 < e <Φ (n) and e and n are co-prime.

Let e = 7

1< 7 <20

Compute a value for d such that (d * e) % Φ (n) = 1

Check the value d[(d*e)% Φ (n)=1]

One solution is d = 3 [(3 * 7) % 20 = 1]

Public key is (e, n) => (7, 33)

Private Key is (d, n) => (3, 33)

The encryption for message $m = 2$ is $c = 2^7 \% 33 = 29$

The decryption of $c = 29$ is $m = 29^3 \% 33 = 2$

C. Encryption and Decryption in AES

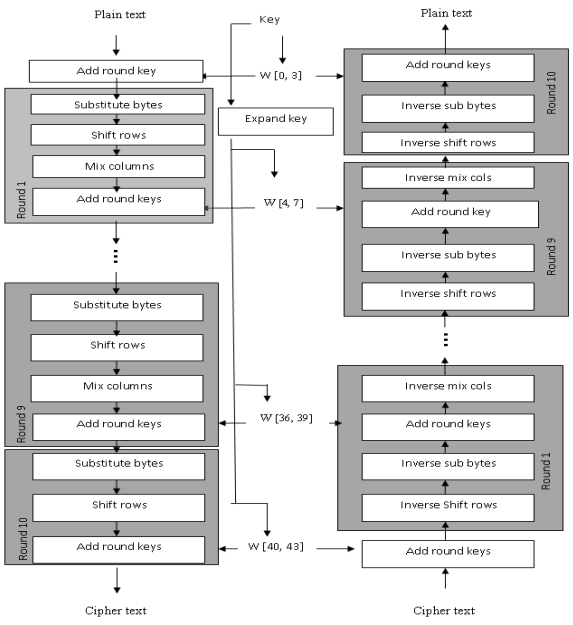


Fig Data encryption and decryption in AES

The AES Encryption process works as follows:

Processor writes the key data to AES Key register. Now the key setup operation has to be performed. The key setup

ISSN: 2278 – 7798

operation is requested by writing the KEY_SETUP command to the AES Control register. The completion of the key setup operation is flagged by the interrupt signal and the busy bit in the AES Status register.

Processor writes plain data to AES Data register. The 128 bit input data block is delivered by four subsequent write commands to the AES Data register. Finally the encoding operation is started by writing the command AES_ENCRYPT to the AES Control register. The completion of the encoding operation is flagged by the interrupt signal and the busy bit in the AES status register. Now the encrypted data may be read from the AES Data register by four subsequent read commands. The key remains in the module until a new key is written or a reset command is performed.

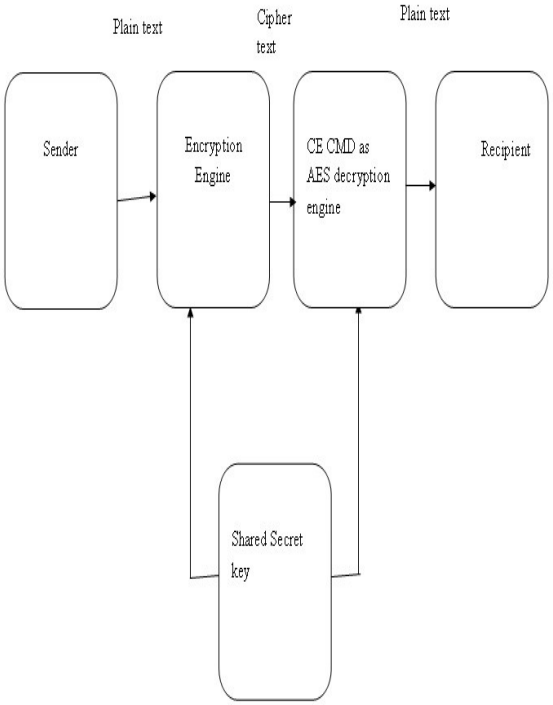


Fig Data encryption and decryption in AES using secret key

In this the sender creates a cipher text message by encrypting the plain text message with the iCE40 AES Encryption Engine and a shared secret key. The sender writes the key data to AES Key register. Then the key setup operation is performed.

Then the sender writes original data. The 128 bit input data block is delivered by four following write commands to the AES Data register. This is followed by the encoding operation. Now the encrypted data may be read from the AES Data register by four following read commands. The sender sends the cipher text message to the receiver.

An approach for encryption and decryption In this it consist of various process.

- Substitute bytes
- Shift rows
- Mix column
- Add round key

Substitute bytes:

It uses s-boxes to perform a byte by byte substitution of the block

Shift rows:

A simple permutation are performed here

Mix columns:

A substitution that makes use of arithmetic over GF(2^8)

Add round key:

A simple bitwise XOR of the current block with a portion of the expanded key. Cipher begins with an add round key followed by 9 rounds that each includes all 4 stages followed by a 10^{th} round of stages.

V. PERFORMANCE EVLUVAION

One of the methods used for encryption and decryption is RSA algorithm.

Representation of RSA algorithm

Two prime numbers randomly

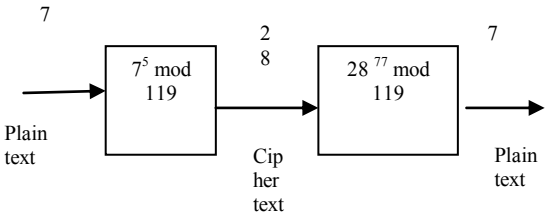
- P=7, q=17
- Φ (n)=(p-1)(q-1)
- Φ (n)=(6)(16)
- Φ (n)=96
- n=p*q 7*17
- Assume e=5(i.e.) e value should not be factor of Φ (n)
- D=d*e Mod Φ (n)=1
- D=d*5 Mod 96=1,so D=77

Now encrypting and decrypting the message HELLO

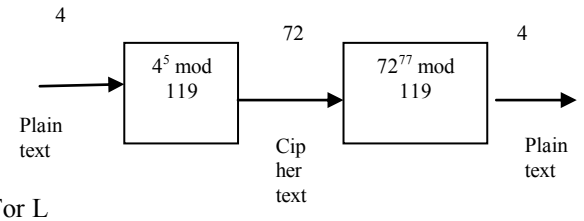
H E L L O

7 4 11 11 12

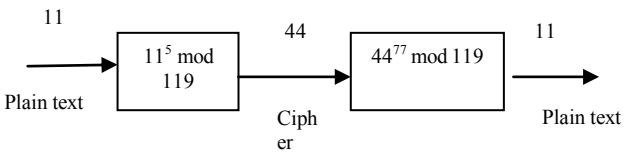
For H



For E

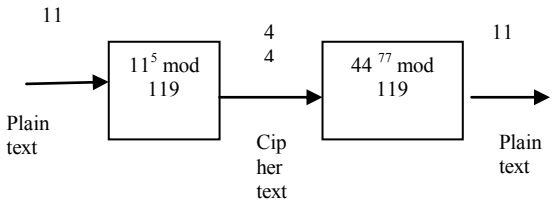


For L

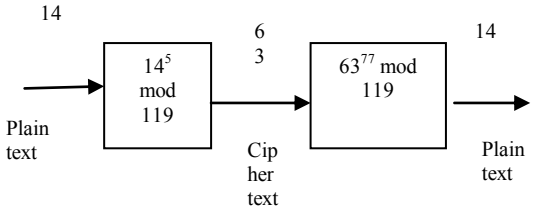


ISSN: 2278 – 7798

For L



For O



VI. CONCLUSION

The investigation of the data security in cloud storage for multimedia data, which is essentially distributed storage system for more effective and flexible distributed verification schema, to address the data storage security issue in cloud computing, as it relay on the cryptographic algorithm RSA and AES to be used. These algorithm are used for protecting user data include encryption prior to storage user authentication procedures prior to storage or retrieval and building secure channel for data transmission. This method maintains the availability reliability integrity to ensure coded data and at the same time identifies mischievous servers. The proposed system significantly improves the security in cloud computing for multimedia data. The future work of proposed system concentrates on text and image.

REFERENCES

[1] D.DanielM.Sona, , S.Vanitha"A Survey on Efficient Video Sharing and Streaming in Cloud Environment Using Video cloud"Vol. 1, Issue 8, October 2013.

[2] Douglas Selent, "Advanced Encryption Standard", Rivier Academic Journal, Volume 6, Number 2, 2010.

[3] Anna C.Squicciarini Dan Lin,Smitha Sundareswaran, "Ensuring Distributed Accountability for Data Sharing in the Cloud," IEEE 2012.

[4] Boyang Wang, Jingbo Yan, Xuefeng Liu, YuqingZhang,"Mona: Secure Multi-Owner Data Sharin for Dynamic Groups in the Cloud,"IEEE 2013.

[5] Larry A. Dunning and Ray Kresman," Privacy Preserving Data Sharing With Anonymous ID Assignment," IEEE 2013.

[6] KuiRen ,Ming Li, Shucheng Yu ,Yao ZhengWenjing Lou, , "Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption," IEEE 2013.

[7] Sonal Guleria1, Dr. Sonia Vatta, "To Enhance Multimedia Security in Cloud Computing Environment Using Crossbreed Algorithm", International Journal of Application or Innovation in Engineering and Management (IJAIEM), Volume 2, 2013.

[8] Cong Wang, KuiRen, Ning Cao,Qian Wang,Wenjing Lou, "Toward Secure and Dependable Storage Services in Cloud Computing," IEEE 2012.

P.V. NITHYABHARATHI, revised the BE degree in Computer Science and Engineering from Anna University, Chennai, India, 2012. He is currently pursuing Master of Engineering in Computer Science and Engineering, United Institute and Technology, Coimbatore, Tamil Nadu, India. Research interests include Cloud Computing, Network Security.

T.KOWSALYA, revised the BE degree in Computer Science and Engineering from Anna University, Chennai, India, 2012. He is currently pursuing Master of Engineering in Computer Science and Engineering, United Institute and Technology, Coimbatore, Tamil Nadu, India. Research interests include Cloud Computing, Network Security.

V. BASKAR, revised the BE degree in Computer Science and Engineering from Anna University, Chennai, India, 2012. He is currently pursuing Master of Engineering in Computer Science and Engineering, A.S.L Pauls College of Engineering and Technology, Coimbatore, Tamil Nadu, India. Research interests include Mobile Computing, Cryptography and Network Security and Data Mining.

ISSN: 2278 – 7798