INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X

Impact factor: 4.295

(Volume 4, Issue 2)

Available online at: www.ijariit.com

Encryption Algorithm for Enhanced Data Security in Cloud Computing

Anila Ashrafiwala
anila.ashrafiwala1@gmail.com
Matoshri Pratishthan Group of Institutions, Nanded, Maharashtra

Amol Patil
amol321p@gmail.com
Matoshri Pratishthan Group of Institutions, Nanded, Maharashtra

ABSTRACT

Cloud storage is a model of a networked storage system where data is stored in pools of storage which are generally hosted by third parties. In this paper, we present another fine-grained two-variable validation (2fa) access control framework for electronics distributed computing administration. In particular, in our proposed 2fa access control framework, a property based access control system is executed with the need of both a client secret key and it lightweight security device. The sender sends the data that is stored on the cloud. Only two factors authenticated the user is able to access the data if he has the device and secret key. Data stored on the cloud is store by fragments.

Keywords: *Encryption, Cloud Computing, Fine-grained, Two Factor and Access Control.*

1. INTRODUCTION

Cloud computing has emerged as a long-dreamt vision of the utility computing paradigm that provides reliable and resilient infrastructure for users to remotely store data and use on-demand applications and services. Currently, many individuals and organizations mitigate the burden of local data storage and reduce the maintenance cost by outsourcing data to the cloud. However, the outsourced data is not always trustworthy due to the loss of physical control and possession over the data. As a result, many scholars have concentrated on relieving the security threats of the outsourced data by designing the Remote Data Auditing technique as a new concept to enable public auditability for the stored data in the cloud. The Auditing is a useful technique to check the reliability and integrity of data outsourced to single or distributed servers.

2. PROBLEM DEFINITION

The problem definition revolves around resolving the critical issue in cloud domain- data security and data correctness over the network.

- Authorization and Authentication: Data user should be permitted by data owner for data access.
- Key Management: For effective key management, separate key distribution center is used for providing keys to authorized users.
- Encryption/Decryption on the Client side- To enable confidentiality, encryption and decryption technique used .for more security, AES and RSA combined approach used.
- Data Integrity-To check data correctness, a standard unique hash of data checked by Trusted Third Party Auditor (TPA) externally.
- Privacy-Preserving – Without knowing data, external auditor should able to check the data correctness.

2.1 Cloud Auditing Types

- Public Auditing (Third Party Auditing)
  In this approach TPA, instead of the data owner, verifies the integrity of the data stored in the cloud server. The system model consists of three entities: the data owner, the cloud server, and the TPA.

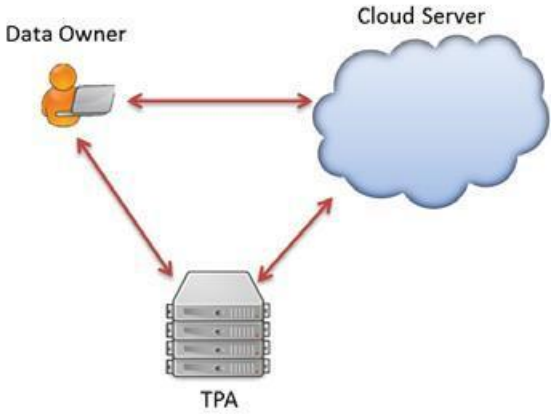


Figure 2.2: Public Auditing [17]

- Private Auditing (Data Owner Auditing)
  It's also known as Private Verifiability/Auditing when the data owner verifies the integrity of the data stored on the cloud server. The system model consists of two entities: the data owner and the cloud server

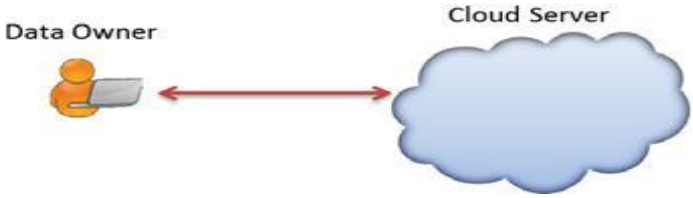


Figure 2.3: Private Auditing [17]

3. SELECTION OF AES ALGORITHM

The AES cipher is part of a family known as block ciphers, which are algorithms that encrypt data on a per-block basis.These "blocks" which are measured in bits determine the input of plaintext and output of ciphertext. So for example, since AES is 128 bits long, for every 128 bits of plaintext, 128 bits of ciphertext are produced.Like nearly all encryption algorithms, AES relies on the use of keys during the encryption and decryption process. Since the AES algorithm is symmetric, the same key is used for both encryption and decryption. AES operates on what is known as a 4 x 4 column major order matrix of bytes. Here is how the cycles break down. A) 10 rounds are required for a 128-bit key. B) 12 Rounds are required for a 192-bit key. C) 14 Rounds are required for a 256-bit key.

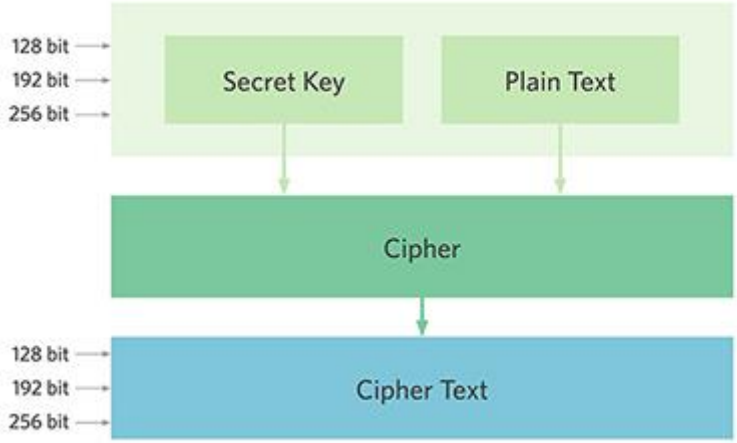


Figure -1: AES Design

Broadly speaking the encryption/decryption 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 another

key is used for decryption. Generally, the private key is kept secret and generally held by the owner of data or trusted 3rd party for the data, while the public key can be distributed to others for encryption. The secret key can't be obtained from the public key

4. KEY GENERATION ALGORITHM

```
Cipher(byte in[16], byte out[16], key_array round_key[Nr+1])
Begin
        byte state[16]; state = in;
        AddRoundKey(state, round_key[0]);
        for i = 1 to Nr-1 stepsize 1 do SubBytes(state);
        ShiftRows(state);
        MixColumns(state);
        AddRoundKey(state, round_key[i]);
        end for SubBytes(state);
        ShiftRows(state);
        AddRoundKey(state, round_key[Nr]);
End
```

4.1 High-level description of the algorithm

- **KeyExpansions**—round keys are derived from the cipher key using Rijndael's key schedule. AES requires a separate 128-bit round key block for each round plus one more.
- **initial round**

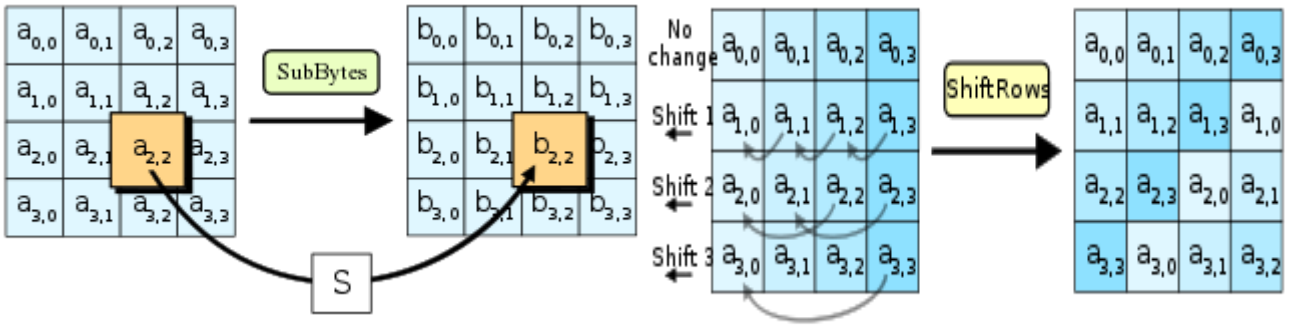
    1. **AddRoundKey**—each byte of the state is combined with a block of the round key using bitwise xor.

- **Rounds**

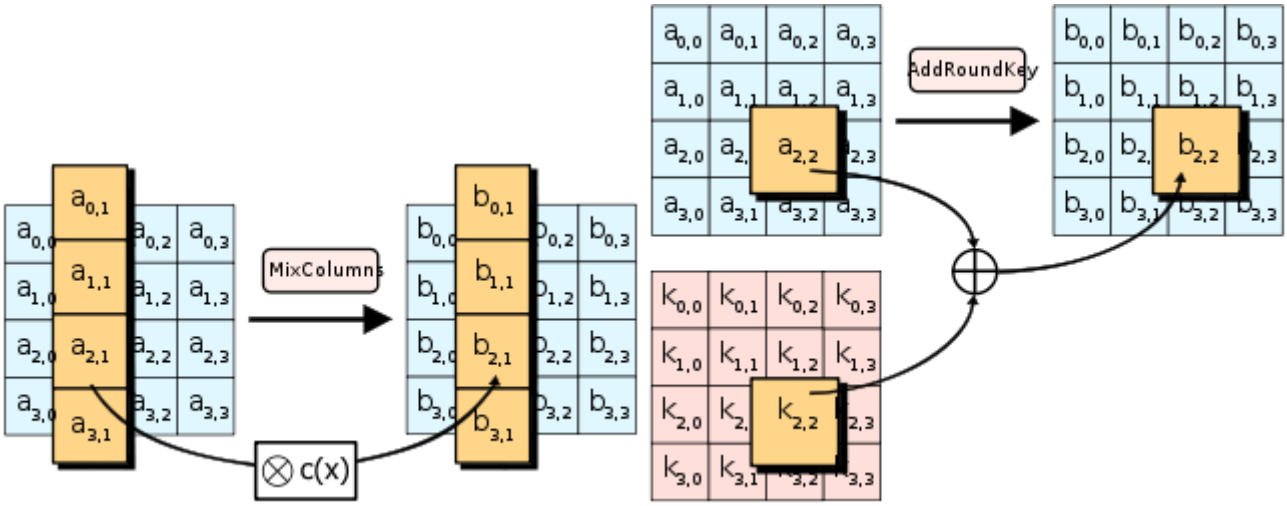
    2. **SubBytes**—a non-linear substitution step where each byte is replaced with another according to a lookup table.
    3. **ShiftRows**—a transposition step where the last three rows of the state are shifted cyclically a certain number of steps.
    4. **MixColumns**—a mixing operation which operates on the columns of the state, combining the four bytes in each column.
    5. **AddRoundKey**

- **Final Round (no MixColumns)**

    6. SubBytes
    7. ShiftRows
    8. AddRoundKey.



In the SubBytes step, each byte in the state is replaced with its entry in a fixed 8-bit lookup table, S; $b_{ij} = S(a_{ij})$.
In the ShiftRows step, bytes in each row of the state are shifted cyclically to the left. The number of places each byte is shifted differs for each row.



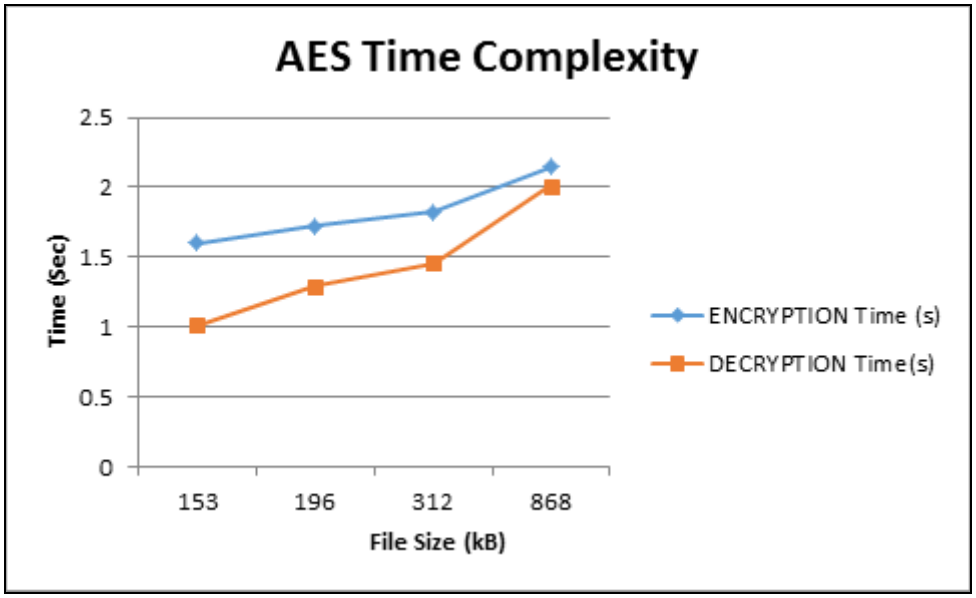
In the MixColumns step, each column of the state is multiplied by a fixed polynomial
In the AddRoundKey step, each byte of the state is combined with a byte of the round subkey using the XORoperation (⊕)..

5. SIMULATIVE RESULTS

The time complexity of AES is analyzed by varying the size of documents and usinf different file formats..

Table-1: Time Complexity for signature Generation for data auditing

File Name	File Size(KB)	Encryption time (in seconds)	Decryption Time (in seconds)
Cloud.txt	153	1.6	1.01
Cricket.docx	196	1.72	1.29
CustomerMgmt.pdf	312	1.823	1.46
HappyMood.txt	868	2.147	2.01



6. CONCLUSION

The public auditing system of data storage security in Cloud Computing and provide a privacy-preserving auditing protocol. It enables an external auditor to audit user's cloud data without learning the data content. This scheme is the first to support scalable and efficient privacy preserving public storage auditing in Cloud. Specifically, it achieves batch auditing where multiple delegated auditing tasks from different users can be performed simultaneously by the TPA in a privacy-preserving manner. It achieves two end data security level so it's more secure.

7. REFERENCES

[1] Qianhong Wu, Yi Mu, Willy Susilo, Bo Qin, and Josep Domingo-Ferrer," Asymmetric Group Key Agreement", In 6th International Conference on Cloud Computing,2015.
[2] Dr. Prerna Mahajan & Abhishek Sachdeva , "A Study of Encryption Algorithms AES, DES and RSA for Security", Global Journal of Computer Science and Technology Network, Web & Security Volume 13 Issue 15 Version 1.0 the Year 2013
[3] "What is Cloud Computing? A Webopedia Definition", 2015.[Online]. Available: http://www.webopedia.com/TERM/C/cloud_computing.html
[4] Daoyuan Li, "MD5 Analysis",2009[Online].http://daoyuan.li/category/projects/9-md5/

BIOGRAPHIES

Miss Anila Ashrafiwala
PG Student

She received B-Tech degree from the SRTM University, Nanded in 2012. She is currently pursuing Maters in MPGI, Nanded. Her Research interest is in the area of cloud computing.

Mr. Amol Patil
Assistant Professor

He has joined the computer science and engineering department, SRTM University from past 7 years. His current research interest includes network security, applied cryptography, cloud computing and protection in cyber physical system..

