Impact Factor (SJIF): 4.542

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444

Volume 4, Issue 5, MaY-2017

IMPROVE AES ALGORITHM TO MAINTAIN DATA INTEGRITY USING THIRD PARTY AUDITING IN CLOUD COMPUTING

Khant Drashti[1] ,

[1] *M.E. Student, Computer Department, B.H.Gardi College of Engineering & Technology*

Abstract— Cloud computing is a new concept of Data processing .In cloud computing client are allowed to use variety of IT services to large poll of computer resources , using the internet as a computation bus. In cloud computing all resources are available in 24*7 hours, used on demand and paid according to use resource. It is a distributed computing, parallel computing and grid computing development. Cloud storage is one of the service provided by Cloud computing in which data is maintained, managed, backed up remotely and made available to users over a network (typically the Internet). The user is concerned about the integrity of data stored in the cloud as the user's data can be attacked or modified by outside attacker. Therefore, a new concept called data auditing is introduced which check the integrity of data with the help of an entity called Third Party Auditor (TPA). The purpose of this work is to develop an auditing scheme which is secure, efficient to use and possess the capabilities such as privacy preserving, public auditing, maintaining the data integrity along with confidentiality. Thus the new auditing scheme has been developed by considering all these requirements. It consist of three entities: data owner, TPA and cloud server. The data owner performs various operations such as splitting the file to blocks, encrypting them, generating a hash value for each, concatenating it and generating a signature on it. The TPA performs the main role of data integrity check. It performs activities like generating hash value for encrypted blocks received from cloud server, concatenating them and generates signature on it. It later compares both the signatures to verify whether the data stored on cloud is tampered or not. It verifies the integrity of data on demand of the users. The cloud server is used only to save the encrypted blocks of data. This proposed auditing scheme make use of AES-200bit algorithm for encryption, Markel Hashing Tree and SHA-512 for integrity check and RSA signature for digital signature calculation.

Keywords: cloud computing, Third party auditor,integrity ,AES128,AES 192,AES 200 bit, Markel hash Tree.

I. INTRODUCTION

Cloud computing is a new concept of Data processing .In cloud computing client are allowed to use variety of IT services to large poll of computer resources , using the internet as a computation bus. In cloud computing all resources are available in 24*7 hours, used on demand and paid according to use resource. It is a distributed computing, parallel computing and grid computing development. The cloud is a set of hardware, networks, storage, services, and interfaces and that enable the delivery of computing as a service. In a cloud computing provide service like , delivery of software, infrastructure, and storage over Internet based on user demand. Cloud Computing is rapidly being accepted as a universal access appliance on the Internet. Many conceptual definition has been given to the Cloud Computing. many time the definitions of Cloud Computing remain controversial. But we have considered the standard definition which was given by the National Institute of Standards and Technology (NIST): "Cloud computing is a model for enabling convenient, on demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction"[2].

II. SERVICE MODEL OF CLOUD COMPUTING

According to NIST, the cloud model is composed of three service models[2]:

Software as a Service (SaaS): cloud computing provide a different different type of services .software as a service is a one of them .user use a any software as a service. business user use a that kind of services , to complete business tasks. Email, CRM , website testing, wiki blog ,virtual Desktop.. it's an example of a software as a service. [2]

Platform as a Service (PaaS):this type of cloud computing provide a deployment environment as a service. Developer and deplorers use a that kind of cloud service .to create or deploy application and services for user at that purpose paas is use. service are available in pass service and application test, development, integration and deployment. [2]

Infrastructure as a Service (IaaS): user use a some type of infrastructure that time this service is used. Manly system manager are use a this service. to create platforms for service and application test, development, integration and deployment. the customer can control the environment as a service. [2].

III. ABOUT THIRT PARTY AUDITOR

Third party Auditor (TPA)*: The cloud user is a one of the person who has stored a large amount data files stored in a cloud; the cloud server is the one who provides the data storage service like resources, software to the user. Cloud service provider manage a cloud; the third- party auditor is the one who has belief to access the cloud storage service for the benefit of user whenever user request for data access. The TPA has capabilities and competence that the user does not have. Every time it is not possible for user to check the data which(data stored in cloud) is stored on cloud server that arrives online burden to the user, that's why to reduce online burden and maintain that integrity cloud.[10]*

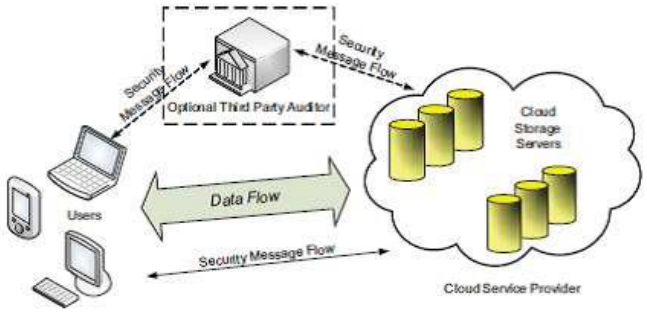

Fig 1: Cloud computing TPA service provisioning architecture[3]

User may resort to TPA. When data owner stored data in cloud server then after internal and external attacks, which is having data integrity threads like hardware failure, software bug, hackers, and management errors. The Cloud Server can maintain reputation for its self-serving and The CS might even decide to hide these data correction incidents to user, So that's why here we are giving third-party auditing service for users to gain belief on cloud.

TPA, who is in the business of auditing, is reliable and independent, and thus has no incentive to collude with either the CS or the owners during the auditing process. The TPA should be able to efficiently audit the cloud data storage without local copy of data and without any additional online burden for data owners.

IV. EXISTING SCHEME [5]

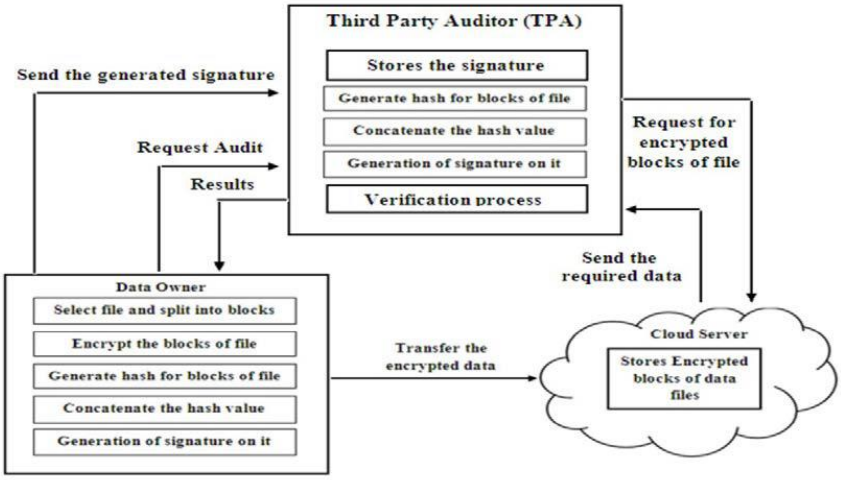

Fig 2 Existing Scheme of Third Party Auditor[5]

4.1Existing Algorithms[5]

- **Data Owner :**First data owner Select file and then Split into the number of blocks. Then After Apply a AES Encryption Algorithm on normal data. Then after Generate hashing value for block files using a SHA-2 hash function and then RSA Use for Generate digital signature. Data Owner Already Transfer the Encrypted data to a Cloud Server.
- **Cloud Server :** Cloud Server Stored the Encrypted form of data. When TPA send Request for Encrypted block of files then Cloud Service Provider send a Encrypted block of files.
- **Third Party Auditor**: when data owner send order to third party auditor to audit a data then after TPA send a request to a cloud service provider to send a data owner encrypted data .then third party auditor apply same hashing algorithm to an encrypted data and then generate a digital signature. Then after compare this digital signature and data owner digital signature. If these both signature are same so integrity is maintain other wise integrity is break.

4.2 Disadvantages of Existing system

- Authors were not takedata dynamic operations such as updation, deletion and insertion of data.

V. PROPOSED SCHEME

5.1 Proposed Scheme

- Using a AES 200 bit algorithm For Encryption .
- **Data Dynamics**: includes block level operations of modification, deletion and insertion.This is achieved by using the data structure Merkle Hash Tree (MHT), data changes in a certain way; new data is added in some places.

5.2 Proposed Algorithm

- **Encryption:** 200 bit input is copied to the State array of 5*5 matrix. The data bytes are filled first in the column then in the rows, Then after the initial round key addition, ten rounds of encryption are performed. The first nine rounds are same, with small difference in the final round and each of the first nine rounds consists of 4 transformations:
  - SubBytes,
  - ShiftRows,
  - MixColumns
  - AddRoundKey. But in final round Mix columns transformation is not used.
- **Decryption :**
  - InvSubBytes,
  - InvShiftRows,
  - InvMixColumns, and
  - AddRoundKey

5.3 **Key Expansion** :

Key expansion of AES 200 bit algorithm.

```
Key Expansion (byte Key [5*Nk] word W[Nb*(Nr+1)])
        {
                For(j=0;j<Nk,j++)
                W[j]=(key[5*j],key[5*j+1],key[5*j+2],key[5*j+3],key[5*j+3],key[5*j+4]);
                For(j=NK; j<Nb * (Nr+1);j++)
                {
                        Temp =W[j-1];
                        If(j%NK==0)
                        Temp = SubByte(RotByte(temp))^Rcon[j/NK];
                        W[j] = W[j-NK]^temp;


        }
```

5.4 Advantage of Proposal scheme

- To privacy-preserving public auditing scheme and its support of data dynamics.
- Markel Hashing Tree Support a Data Dynamics operations such as updation, deletion and insertion of data.

VI. EXPERIMENTAL RESULT

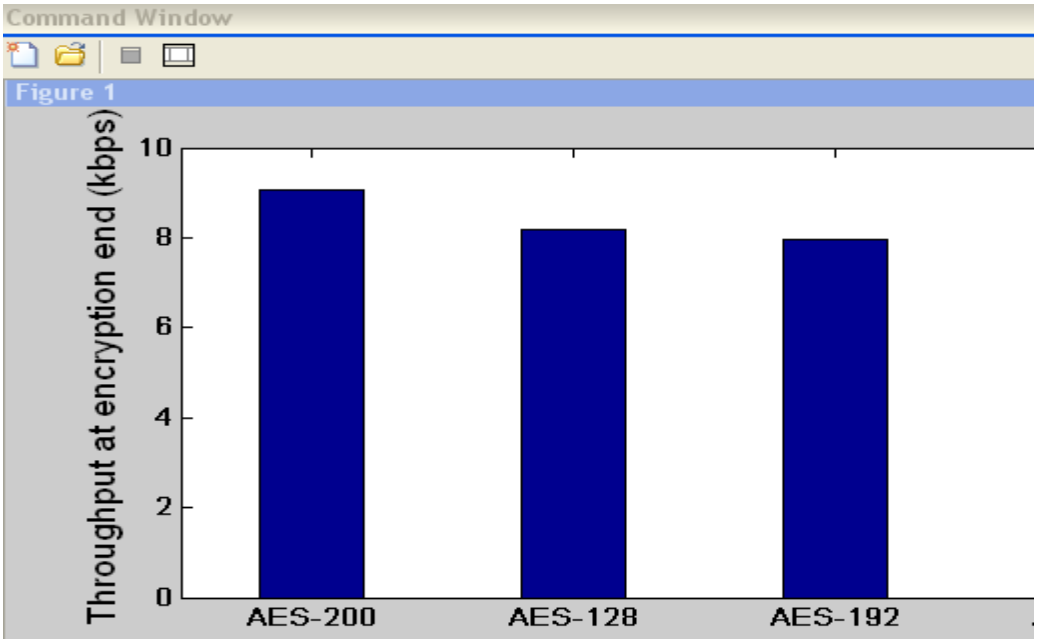

Fig 3: Comparison of throughput at encryption side of various AES standards.

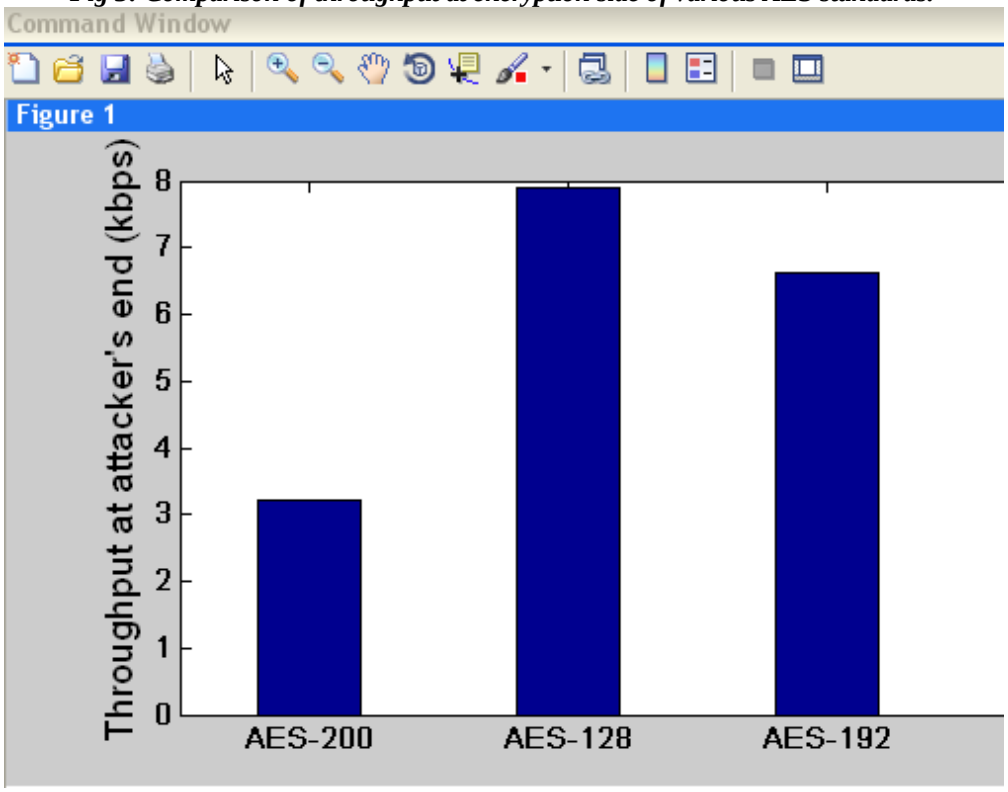

Fig 4: Comparison of throughput at decryption side of various AES standards.

VII. REFERENCE

1] Ms. Bhor Priti1, Ms. Kakade Priyanka2, Ms. Kale Ashwini3, Miss. Dere Archarana4," SURVEY OF PUBLIC AUDITING IN CLOUD", *IJARIIE-ISSN(O)-2395-4396, 2015*

2] J.SRINIVAS, K.VENKATA SUBBA REDDY, Dr. A.MOIZ QYSER,"Cloud Computer Basics"," International Journal of Advanced Research in Computer and Communication Engineering", Vol. 1, Issue 5, July 2012

3]Swapnali Morea, Sangita Chaudharib," Third Party Public Auditing scheme for Cloud Storage", 7th International Conference on Communication, Computing and Virtualization 2016.

4] Prof. V. B. Gadichha," Enhancing cloud data security and Integrity using third party auditing Service", ",International Journal on Recent and Innovation Trends in Computing and Communication,
2013

5**]** Salve Bhagyashri1, Prof.Y.B.Gurav " Privacy-Preserving Public Auditing For Secure Cloud Storage", IOSR Journal of Computer Engineering,2014.

6] SwapnaliMorea, SangitaChaudharib," Third Party Public Auditing scheme for Cloud Storage" ELSEVIER,2016.