IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 18, Issue 6, Ver. I (Nov. - Dec. 2016), PP 11-15
www.iosrjournals.org

Big Data Authentication Using Cloud Storage with Fine Grained Updates

Manoj Kottawar[1], Omshankar Swami[2], Govind Sakhare [3], Gaurav Shiraskar[4], Prof. Sachin Patil[5]
Department of Computer Engineering, G.H.R.C.E.M,Pune.
SavitribaiPhule Pune University,PuneMaharashtra (India)-412207

Abstract: *Now a days cloud computing is one of the intensively growing technology.Cloud computing is storing and accessingbased program over the internet without use of your computer's hard drive. Proposed system mainly focuses on security of private confidential data stored on cloud. Now a day's use of cloud increasing rapidly.In order to manage security of private/confidential data we need an effective system. In proposed work we provide system which continuously interact with the content owner of cloud and gives continuous updates to content owner.Existing system also audits data which result in time consuming process.Instead of checking on whole data whether the updates are going on or not in system, proposed system divides the whole data in blocks and system checks that particular updated block where changes occurs. Hence proposed systemprovides reliability and enhanced security.*

I. Introduction

CLOUD computing is one of the intensively referred to as one of the most dominant innovations in information technology in late fewyears. By using resource virtualization cloud delivers us computing resources and services in a pay and use mode. Today world is moving with digitization and cloud computing is best way to manage big datasets. Cloud computing services are divided into three main parts i.e. Infrastructure-as-a Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS).

Now a days many international IT companies and organization provide powerful public cloud services to users on a range from individual end user, business person to enterprise all over the world various examples of this are Microsoft Azure, Google Drive, Justcloud andDropbox. As we all know the current technology and escalation of cloud computing is rapidlygrowing, debates and temporization on the usage of cloud still present. Cloud computing mainly focuses on data security and data privacy. As compared to conventional system in cloud computing user loss their direct control over their data. In our proposed work we will work on problem of integrity verification of data for big data storage on cloud. This Scheme is called as data auditing when the verification is conducted by a third party i.e. TPA. In our system TPA works asauditor. From cloud users point of view it is named as auditing-as-a-service. In a centrally monitored verification scheme, the cloud storage server systemvalid integrity proof of a given proportion of data to a verifier cannot provideuntil all these data is inviolate. Our system recommends it is important to conduct data auditing on a regular basis.Our proposed work has following features:

- Data security.
- Privacy protection to data.
- Audit details to content owner.
- Auditability aware data preparation system.
- To provide scalability and reliability of cloud.
- Key generation for each block.
- Increased auditing speed.

II. Literature Review

In past few years cloud computing facing several issues regarding security aspects. In recent days research they enhanced the security schemes, previoussystem suffer from variousdrawbacks. First, there was no secured system for authorization and authentication process between the auditor and cloud service provider, i.e. anyone can stand against the cloud service provider for a evidence of decency of certain data, moreover some of the recent work based on BLS signature can already support fully dynamic data updates over specified-size data blocks, they only support updates or changes on fixed-sized blocks as basic unit, which we say coarse-grained updates [1]. As a result, every small update will have several problems such as re-computation forwholefileblock,whichinturncauseshigherstorageand take much time for auditing i.e.communicationoverheads, they also provide a formal system analysis for possible types of fine-grained data updates and provide a system

that can fully support secured auditing and fine-grained update alerts. Based on this scheme, they also provide demagnification that can dramatically reduce communication overheads for verification of small updates [2]. Another research by surapriya swain says audit ability aware data scheduling scheme where theyc lustered different tasks submitted in an application both from the user and auditor on the basis of their priority [3].one more research focuses on security, robustness, scalability feature of system. This scheme proposes of a public auditing scheme based on ECC signature and data auditing protocol that can support full-grained update requests [4]. The HASBE method is provided for realizing efficient, flexible and fine-grained access mechanism in cloud computing. The HASBE method coherently incorporates a hierarchical structure of system users by applying a similar algorithm to ASBE. HASBE not only intend to compound attributes due to flexible attribute set combinations [5]. Another author mandeep kaur gives comparative analysis between KP-TSABE scheme and advanced KP- ABE scheme [6].

III. System Architecture

Proposed system can entirely support authorized auditing and fine-grained update requests instead of coarse grained updates. In our proposed work, we also offer an inflation that can goodly reduce communication overheads for verification of small updates. Cloud storage fine grained data updates and to implement a system that can completely support authorized auditing and fine grained update requests. In proposed work AES algorithm is used for better result which reduces time requirements.

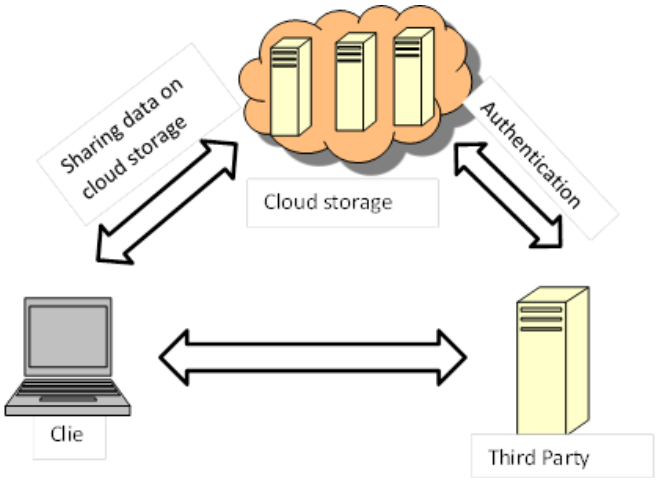


Figure 1: Architecture Diagram

This system categorized in three parts:
1. Content owner
2. Cloud service provider
3. Third party authentication (TPA)

IV. Methodology

1. Registration and login for user:
In this user fill his/her own complete data. Request will send to the CEO for confirmation. CEO confirms his/her request and assigns attribute and time period for that user.In account verification, it will confirm password and key will send to that user by email so he/she can login to his/her account.

2. Approve User and Assign attributes:
Out of the selected attributes according the roles defined in hierarchy of the system the attribute visibility access is decided. Each attribute is encrypted.

3. Key Generation and Verification
Key is generated based on the data and attributes filled by the user in user registration form. In attribute key verification, when a key is used for login, it verifies with first key stored in the database. If a key matches found then user is allowed for next process else the user is unacceptable for next process.

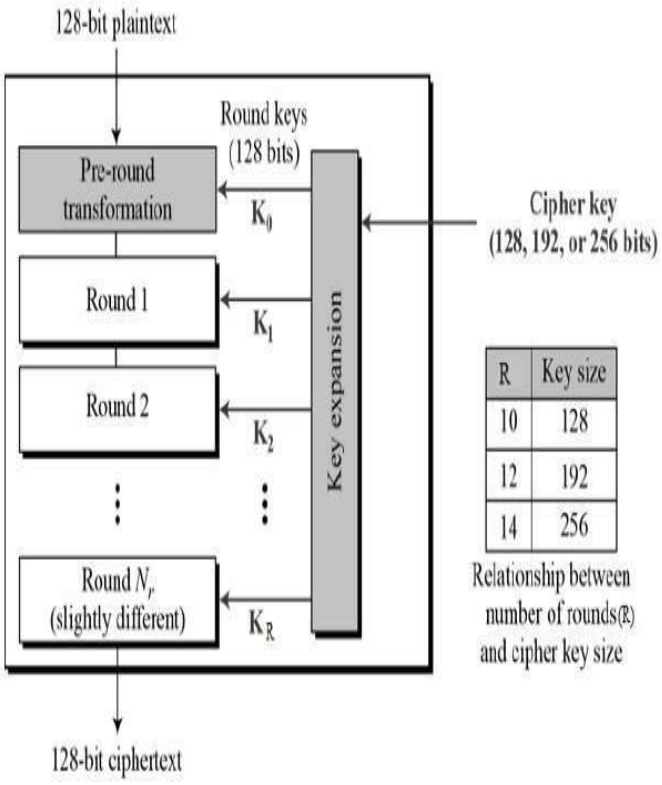
4. Encryption and decryption of data
User fills his/her data during registration. Once it is click on submit button data is send to encryption algorithm that are DES and AES. After performing encryption data is stored in encrypted format in database.

5. Access Right:
The user deserves authority once he/she register for system, selected attributes of the same level as well as other levels according to the access authority using attribute key.

6. Fine Grained Access
In our propose system instead of using coarse grained method i.e. instead of checking on all data, the fetching of necessary data is allowed. Due to this system provides a quick response time.
7. Request for extra attribute:
The user is allowed to access attributes of same level as inter level counterparts. User is allowed to request for extra attributes in case of emergency as well as ease of work.
8. Flexibility
In this module suppose when user transfer from one location to another location at that time new location does not having rights to access data of that user .In this situation request to view attributes of required user and grant for accessing data of that user by admin is necessary. When user's data is accessible from new location then it cannot access from old location.
9. Scalability:
Since performing hierarchical structure so even if lower authority is absent for particular days at that time higher authority handles all work of lower authority so work of company will not be stopped.
10. Efficient User Revocation:
It can be done by two steps request to the admin and response to the user from admin within expiration time.
11. Privacy:
Default it is public but a user can set intra-level privacy by restricting access to attributes.

V. Algorithm

In our proposed work, for encryption/decryption process AES (Advanced Encryption Standard) algorithm is used.It is based on 'substitution-permutation network'.it comprises of series of linked operation, some of which involve replacing inputs by specific outputs and other involve shuffling bits around.AES performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of plaintext block as 16 bytes.



R	Key size
10	128
12	192
14	256

Relationship between number of rounds(R) and cipher key size

Figure 2: AES Schematic

AES Analysis

In present day cryptography, AES is used and supported in both hardware and software. Up till now, no practical attacks against AES algorithm has been discovered. Moreover, AES has built-in flexibility of key length, which allows a degree of 'future-proofing' against process in the ability to perform exhaustive key searches. However, just as for DES, the AES security is assured only if it is correctly implemented and good key management is employed.

Encryption process

Here, we limit to description of a typical round of AES encryption. Each round comprise of four processes. The first round process is shown below-

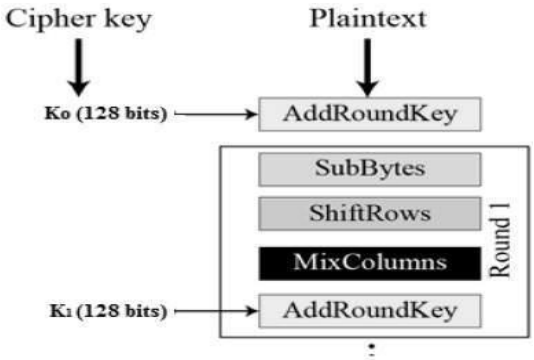


Fig 3: AES encryption

Byte Substitution:

The result is stored in matrix of four rows and four columns.The 16 inputs are stored in matrix of four rows and four columns

Shift rows

In shift row column each of the four rows of the matrix is shifted to the left side. 'Fall off' entries are re-inserted on the right side of row. Shift is carriedas given below:

In matrix, first row is not shifted. Again second row is shifted one byte position from right to the left. Third row is shifted two positions to the left from right. Where fourth row is shifted three positions to the left.

The newly generated result is a new matrix consisting of the 16 bytes but shifted with respect to each other.

Mix Columns

In this each column of four bytes is now transformed using a particular mathematical function. This function takes as input the four bytes of one column and outputs four completely new bytes, which changes to the original column. The new result is another matrix consist of 16 new bytes. It should be noted that this step is not performed in the last round.

Addroundkey

The 16 bytes of the matrix are now considered as 128 bits and are XoRed to the 128 bits of the round key. If this is the last round then the output is the cipher text. Else, the resulting 128 bits are interpreted as 16 bytes and we need to start another similar round.

Decryption Process

In the process of decryption of an AES ciphertext is similar to the encryption process in the reverse order. In which each round consists of the four processes arranged in the reverse order:

Add round key

Mix columns

Shift rows

Byte substitution

Since sub processes in each round are in reverse order, unlike for a Feistel Cipher, the encryption and decryption algorithmsneed to be separately implemented; even they are very densely related.

VI. Result And Future Work

By studyingvarious research papers we come to result. In previous work auditing was done with use of coarse grained updates now it is replaced with fine grained updates.Proposed work generating encryption/decryption key for each block which will dramatically enhance security, although proposed scheme providing third party auditing scheme and we are designing application which will keep interaction between third party auditor and user of the system. During our work we studied several aspects and found improvement in each paper. In future by using AES algorithm it is possible to improve overall response time of the system and reduce communication overheads by providing fine grained updates.Based on the review work of this paper we found improved data auditing, we proposed further work to investigate the next step on how to improve other server side protection system for reliable data security with effective data integrity and availability.

Acknowledgement

We would like to acknowledge the grateful support of our guide Prof Sachin Patil sir who was always available for our queries and generously gave us his valuable time and vast knowledge. His encouragement and faith on us throughout have been extremely helpful. His valuable feedback always guides us in proper direction.

References

[1]. "Fine Grained Updates in Cloud Using Third Party Auditing" M Paventhan, C Murugavel, S Rajadurai
[2]. "Authorized Public Auditing of Dynamic Big Data Storage on Cloud with Efficient Verifiable Fine-Grained Updates"
[3]. "Authorized Public Auditing of Dynamic Big Data Storage on Cloud with Efficient Verifiable Fine-Grained Updates".Chang Liu, Jinjun Chen, Senior Member, IEEE, Laurence T. Yang, Member, IEEE, Xuyun Zhang, Chi Yang, Rajiv Ranjan, and Ramamohanarao
[4]. " Public Auditing of Dynamic Big Data Storage with Efficient High Memory Utilization and ECC Algorithm"G.Janani1, C.Kavitha2 P.G Scholar, Department of CSE, Sri Shanmugha College of Engineering and Technology, Pullipalayam, Salem (Dt), India1 Assistant Professor, Department of CSE, Sri Shanmugha College of Engineering and Technology, Pullipalayam, Salem (Dt), India2
[5]. "Improving Flexibility, Scalability and Fine-Grained Access Control using Hierarchical Attribute Set Based Encryption (HASBE) and Security in Cloud Computing". Prashant A. Kadam*, Dinesh M. Yadav Department of Computer Engineering & Savitribai Phule Pune University, Maharashtra, India.
[6]. "Comparative Analysis of Two Fine Grained Data Access Control Techniques in Cloud Computing". Mandeep Kaur MTECH (CSE), Punjab Technical University Punjab, India
[7]. "A Survey of Public Auditing for Secure Data Storage in Cloud Computing".Wei-Fu Hsien1, Chou-Chen Yang1, and Min-Shiang Hwang2,3 (Corresponding author: Min-Shiang Hwang)Department of Management Information System, National Chung Hsing University1 Department of Computer Science and Information Engineering, Asia University2 No. 500, Lioufeng Rd., Wufeng, Taichung 41354, Taiwan (Email: mshwang@asia.edu.tw) Department of Medical Research, China Medical University Hospital, China Medical University3 No. 91, Hsueh-Shih Road, Taichung 40402, Taiwan
[8]. "Shucheng Yu, Cong Wang, Kui Ren, and Wenjing Lou. Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing" ‖. 2010. IEEE INFOCOM