IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

BIG DATA AUTHENTICATION USING CLOUD STORAGE WITH FINE GRAINED UPDATES.

[1]Shreya M. Kottawar, [2] Manisha R. Shire, [3] Vaishnavi S. Bidwai, [4] Tejal C.Wadile

[1]Student, [2]Student, [3]Student, [4]Student
[1]Department of Computer Engineering, G.H.R.C.E.M, Pune
[1]SavitribaiPhule Pune University, Pune, Maharashtra, India-411014

Abstract: Now a days, cloud computing is growing rapidly day by day where user can store big amount of data and can reduce huge capital investments in their IT infrastructure. cloud computing can store and access program over the internet without use of any hard disk, pen drive etc. which maintains direct control over the data ,which makes data secure proposed system will provide a system where it focuses on security of confidential and private data stored on the cloud. It also provide a formal analysis of fine grained updates that can support authorised auditing .Existing system also provide data auditing but it was time consuming process because system have to check whole data whether updates are going on or not in system. Proposed system divides the whole data in small blocks or chunks and will check only that particular block where exactly changes occurs. In proposed work we provide system which continuously interact with the content owner of cloud and gives continuous updates o content owner.

Keywords **- Fine grained, Data auditing.**

I. INTRODUCTION

Cloud computing is the most referred innovation in information technology in last few years. Today's world is moving with digitization and cloud computing is best way to store big data because it uses resource virtualization and use services in pay and use mode. Cloud computing services are divided into three main parts i.e Infrastructure-as-a-service, Platform-as-a-service and Software-as-a-service. Proposed system can entirely support authorized auditing and fine grained update requests instead of coarse grained updates. In our proposed work, we provide a system which cannot loss their direct control over their data. Cloud storage fine grained data updates and to implement a system that can completely support authorized auditing and fine grained update requests. We will work on problem of integrity verification of data for big data storage on cloud. This skim is called data auditing, verification is conducted by a third party i.e. TPA. In proposed system TPA works as auditor and it named as Auditing-as-a-service. Proposed system has following features:

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

Although existing data auditing schemes already have various properties , potential risks and inefficiency such as security risks in unauthorized auditing requests and inefficiency in processing small updates still exist. System focuses on better support for small dynamic updates, which benefits the scalability and efficiency of cloud storage server. Proposed system utilizes a flexible data segmentation strategy. Meanwhile, system addresses a potential security problem in supporting public variability to make the scheme more secure and robust, which is achieved by adding an additional authorization process among the three participating parties of client, CSS and a third-party auditor (TPA).

Cloud computing is one of the intensively referred to as one of the most dominant innovations in information technology in late few years. 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). Proposed system can entirely support authorized auditing and fine grained update requests instead of coarse grained updates. In our proposed work, propose system offers 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.

II. LITERATURE SURVEY

This section of the literature survey eventually reveals some facts based on thoughtful analysis of many authors work as follows.

1. "Secure authentication in cloud big data with hierarchical attribute authorization structure.",Jian Shen, member, IEEE, dengzhi liu, qi liu, xingming sun, senior member, IEEE, yan zhang, senior member, IEEE,2017 : The concept of the big data has been widely concerned among researchers. Nowadays, utilizing the big data to obtain valuable information has become an important trend. The primary goal of the big data research is to process large amounts of data to obtain significant information. Furthermore, in a long-term perspective, an appropriate approach for the big data processing is very critical. However, it is unable to use a single computer or server to deal with the big data. Therefore, the distributed structure is particularly important in the construction of the big data. Cloud computing is evolved from the distributed computing, which can provide a lot of necessary services for the big data, including distributed processing, virtualization, distributed database. In the cloud big data security assurance community, several access control schemes have been proposed, which mainly focus on the attribute-based encryption (ABE) to design the schemes. In the attribute-based access control system, only users with attributes that satisfy the access policy can access the cloud big data. In fact, users' attributes are distributed by the authority and the access policy is defined by the data owner. It is worth noting that only one authority in the system is not enough in realworld circumstances. In order to improve the security and management efficiency, the method of multiple authorities is put forward to design big data access control schemes. At the same time, a number of hierarchical authorization structures are also presented, which can be used in organizations or companies to meet the requirement of authorization grant right decentralization. In the hierarchical access control system, the root authority distributes security parameters and attributes to domain authorities. After that, domain authorities will distribute the security parameters and attributes to users or sub-domain authorities.

2. " Enhance big data security in cloud using access control. ", Young Wang,Ping Zhang,Int'l Conf. on Advances in Big Data Analytics,2017 : In past few years cloud computing facing several issues regarding security aspects. As internet becomes popular, big data transactions become a big concern in modern society. The data comes from online business, audios and videos, emails, search queries, health data, network traffic, mobile phone data, and many others. The data is stored in database. The data grows tremendously. The data becomes difficult to store, retrieval, analyze, and visualize using traditional database software to approaches. In 2012, The human face of big data was compeleted as globe project. The project collects, visualizes, and analyzes big data. For the social network, Facebook has 955 million monthly active accounts in various languages, and 140 billion photos display. The Google support many services with 7.2 billion pages every day. In the next decade, the amount of information managed by the data center will increase by 50 times as estimated. The number of IT professionals will grow by 1.5 times then. There are several kinds of clouding computing based on cloud location, or the service . Based on the service that cloud is offering, there are three kinds of service. These are lassS (Infrastructure as a Service), PaaS (Platform as a service) and SaaS (Software as service).

3. "Cloud computing: A new paradigm for data storage in indian universities",prateek bhanti, sushma lehri, narendra kumar, indian journal of Computer Science and Engineering (IJCSE). :The cloud computing is considered as fifth generation of computing with reference to mainframe, personal computer, client sever computing, and the web. In essence , cloud computing is a construct that allow you to access applications that actually reside at a location other than your computer or other Internet–connected device; most often , this will be a distant datacenter. It allows the viewers like student, faculties and staffs to use applications and access the information from any computer with internet access. The National Institute of Standards and Technology (NIST) defines cloud computing as a model for enabling on demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management efforts or service provider interaction. Cloud computing is a general term for anything that involves delivering hosted service over the Internet. The beauty of cloud computing lies in the fact that, other company hosts your application and they can handle the costs of servers and manage the software updates, and on the basis of the contract one will pay less for services.

III. PROPOSED SYSTEM

Objectives and Scope:
For providing more security system uses TPA (Third party authenticator) which is able to verify data from cloud and check data integrity.Proposed system works for authenticity to the TPA using MD5 hashing algorithm which is going to perform main funtion in proposed system. It will allow to achieve us the security of our data from TPA. MD5 hashing algorithm gives 128 bit hash key which will allocate to every TPA which should be given at the time of verifying data at cloud.

System Design Diagram:
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 users 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.

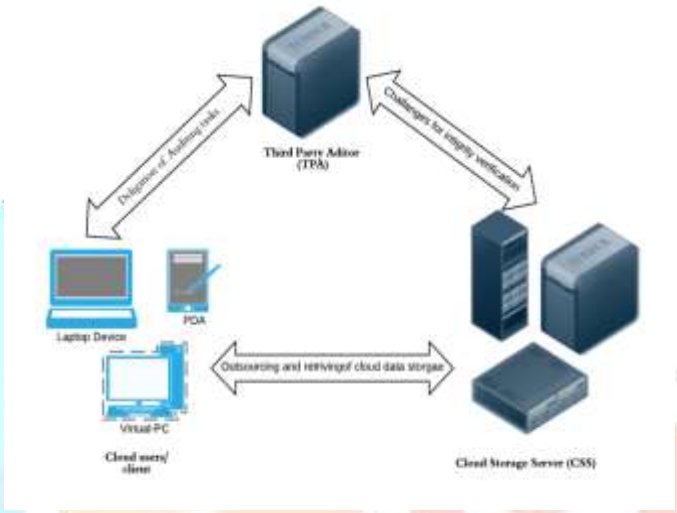

Figure1:System Design

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.

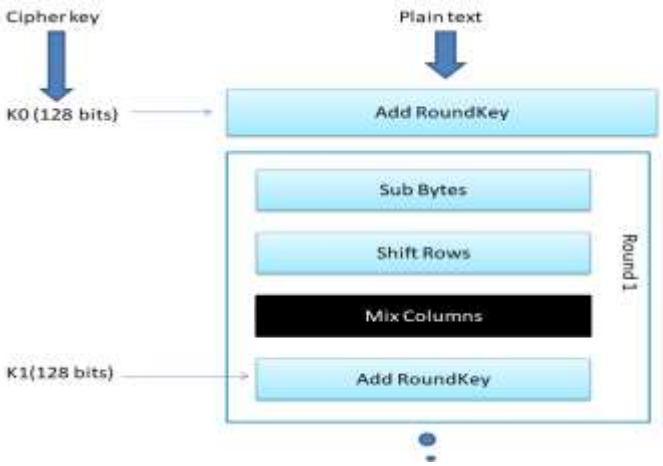

Figure2:AES Encryption

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.

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 cipher text 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 algorithms need to be separately implemented; even they are very densely related.

IV. CONCLUSION

By studying various 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.

V. REFRENCES

[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” ǁ. 2010. IEEE INFOCOM.