Cloud Computing: Overview of Storage Architecture and Data storage security

[1]Miss. Swati I. Bairagi, [2]Prof. Ankur O. Bang

[1]M.E. Computer Science and Engineering Scholar,
Pankaj Laddhad Institute of Technology and Management Studies,
Buldhana-443001 Maharashtra
Sant Gadge Baba Amravati University, Amravati

[2] Assistant Professor and M.E. Co-ordinator
Computer Science and Engineering Department,
Pankaj Laddhad Institute of Technology and Management Studies,
Buldhana-443001 Maharashtra
Sant Gadge Baba Amravati University, Amravati

***Abstract*— Now a day's Cloud Computing is recognized as the next-generation architecture of IT organization. In contrast to traditional solutions, where the IT services are under proper physical, logical and personnel controls, cloud computing is the only emerging trends which moves application software and databases to the large data centers, where the management of the data and services may not be fully trustworthy. This unique attribute, however, poses many new security challenges which have not been well understood. In this paper, we focus on cloud data storage security, which has always been an important aspect of quality of service. By the use of homomorphism token and distributed KDC (Key Distribution Centre) our scheme achieves the high storage correctness insurance and fast data error localization, i.e., the identification of misbehaving server (s). Unlike most prior works, this new scheme further supports secure and efficient dynamic operations on data blocks, including: data update, delete and append. The proposed scheme is highly efficient against malicious data modification attack, and even server colluding attacks.**

***Index Terms*- Cloud computing, Cloud storage, Distributed KDC, Homomorphism token, Third Party Auditor.**

I. INTRODUCTION

Cloud computing is the most emerging field throughout the world as it is on demand service, when needed anybody can have access to cloud data after following some authentication procedure. Cloud computing is an Internet based computer technology. Some of the major firms like Amazon, Microsoft and google have implemented the "CLOUD" and have been using it to speed up their business [1]. Cloud computing architecture is divided into the three layers of infrastructure (SaaS, PaaS and IaaS) i.e software as a service, platform as a service and infrastructure as a service also they provide ever cheaper powerful processor with this computing architecture. The major thing that a computer does is to store in the available space and retrieve information whenever requested by the authenticated user. Cloud computing now a days considered to be the most demanding service because of its high performance, high availability and low cost. In the cloud many services are provided to the client by cloud. Data store is main future that cloud service provides to the companies to store huge amount of storage capacity. There are number of threats to this cloud storage. As cloud data storage possesses vast data stored on the server securing that data is of most concern. Because the data or the authorized file stored on server may got stolen by unauthenticated person or may be the chances of spoofing of data. Ensuring cloud data storage is most important to prevent malicious data modification, to avoid collision attacks and to perform dynamic data operation on data. The term "Cloud" in phrase Cloud Computing refers to the internet and its infrastructure. Cloud computing is in general sense on demand utility computing for anyone with access to cloud. The advantages of cloud computing includes:

- Reduced hardware and maintenance cost,
- Accessibility around the world, and
- Flexibility and highly automated processes wherein the customers need not to worry about software up-gradation.

II. LITERATURE REVIEW

Cloud possesses vast data stored on the cloud server; there is a need to secure Cloud Data storage. Many schemes are

ISSN: 2278 – 1323

proposed under different systems and security models. In all these works, great efforts are made to design solutions that meet various requirements: high scheme efficiency stateless verification, unbounded use of queries and retrieve ability of data, etc. Considering the role of the verifier in the model, all the schemes presented before fall into two categories private verifiability and public verifiability. Although schemes with private verifiability can achieve higher scheme efficiency, public verifiability allows anyone, not just the client (data owner), to challenge the cloud server for correctness of data storage while keeping no private information Then, clients are able to delegate the evaluation of the service performance to an independent third party auditor (TPA) [5], without devotion of their computation resources. In the cloud, the clients themselves are unreliable or cannot afford the overhead of performing frequent integrity checks. Thus, for practical use, it seems more rational to equip the verification protocol with public verifiability, which is expected to play a more important role in achieving economies of scale for Cloud Computing. That is, the outsourced data themselves should not be required by the verifier for the verification purpose to consider the problem of efficiently proving the integrity of data stored at untrusted servers. In the provable data possession (PDP) model [4], the client preprocesses the data and then sends it to an untrusted server for storage, while keeping a small amount of meta-data. The client later asks the server to prove that the stored data has not been tampered with or deleted (without downloading the actual data). However, the original PDP (provable data possession) scheme applies only to static (or append-only) files.

III. RELATED WORK

As the Internet began to grow quickly in the 1990s and the increasingly sophisticated network infrastructure and increased bandwidth developed in recent year has dramatically enhanced the stability of various application services available to use s through the internet, thus marking the beginning of cloud computing network services. Many organizations tried to enhance for their security constraints, for their secure database, for their web application but they have not achieved a high security for their organizations. It is achieved by preventing accidental or deliberate but unauthorized insertion, modification or destruction o f data in a database. Ensuring the integrity of the data really means that it changes only in response to authorized transactions. The central challenge is to build systems that are both efficient and provably secure that is, it should be possible to extract the client's data from any provider that passes verification. Proposed a scheme called “provable data possession” (PDP) model [4] [5] for ensuring possession of file on untrusted storages. Their scheme utilized public key based homomorphic tags [8] for auditing the data file, thus providing public verifiability. They highlight issues around both internal and external auditing. This project allows TPA to audit the cloud data storage without demanding user’s time feasibility or resources. The proposed methods provide public key verification for secured storage and investigate the problem of fine - grained data error Localization in the cloud.

IV. SYSTEM ARCHITECTURE

System architecture of cloud data storage [2] consist of different network elements of the software systems which involved in the delivery of cloud computing services , generally it involves multiple cloud components communicating with each other over loose coupling mechanism like messaging queue. The most important components of the cloud computing architecture are front end and back end. Where the front end is the part seen by the client i.e the computer user, which includes the client’s computer and the applications used to access the cloud via a user interface such as a web browser or any system application. The back end of the cloud computing architecture is the cloud itself i.e. admin of cloud, which comprising various computers, servers and data storage devices.

The network architecture for cloud data storage is shown in above Figure 3.1 Three various network elements can be identified as follows [6].

Users: Who have data to be stored in the cloud and depend on the cloud for data computation, also consist of both individual consumers and organizations.

CSP (Cloud Service Provider): CSP is the person who can manage whole services as well as data storage and lot more thing of cloud computing like operate live Cloud computing system.

Optional TPA (Third Party Auditor): who has capabilities and authority that users may not have, TPA is trusted person to take a risk of cloud storage services on behalf of the users upon request.

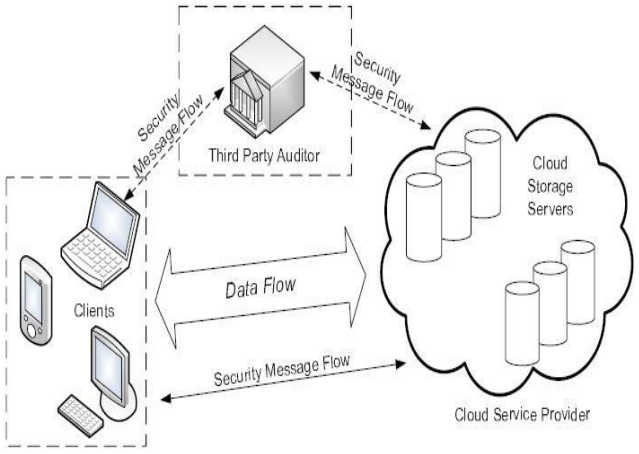

FIGURE 3.1 NETWORK ARCHITECTURE FOR CLOUD DATA STORAGE

V. PROPOSED SYSTEM

For the correctness of data stored on cloud server we tried to design a mechanism which supports the accuracy of stored data along with identification of misbehaving server.

ISSN: 2278 – 1323

Correctness of stored data: we must provide the appropriate data and kept that undamaged in the cloud at all times.

Fast localization of error data: we must efficiently modify the server even if the server failure occurs.

Dynamic operations support for data: It supports dynamic operations if the users modify the data such as insert, delete, append.

Dependability: It reduces the effect of data errors or server failures and protects the data against the byzantine failures, malicious data modification attack and server colluding attacks.

Light-weight communication: It enables users to perform checks whether the data stored correctly with minimum expenses.

The proposed decentralized architecture [11], also authenticate users, who want to remain anonymous while accessing the cloud. We proposed a distributed access control mechanism in clouds. Also we extend the previous work with added features which enables to authenticate the validity of the message without revealing the identity of user who has stored information in the cloud. Compared to many of its predecessors, which only provide binary results about the storage state across the distributed servers, the challenge-response protocol in our work further provides the localization of data error.

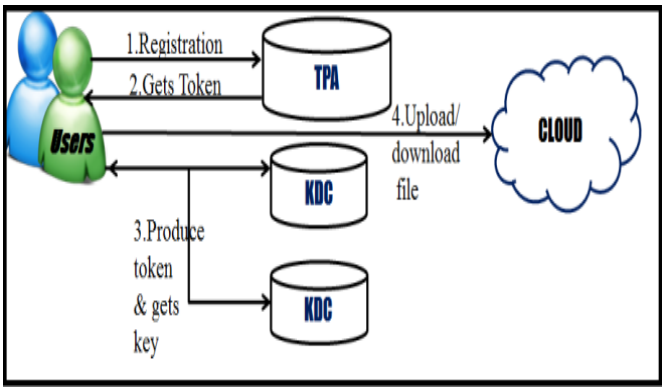

Fig. 4.1 Decentralized KDC architecture

The pictorial representation of the overall flow of the proposed architecture is depicted in Fig 4.1 The user who is the file owner has a collection of files stores the files in cloud server in the form of encrypted files and with indexing. The cloud authenticates the user even without knowing the original identity of the user; rather two step authentications takes place with the help of the Trusted Party Authenticator (TPA) and Key Distribution Center (KDC).

Service Request to TPA: The user registers with the original identity and enrolls with the Third Party Authenticator (TPA). The user sends request to the Third Party Authenticator (TPA) for registration.

TPA Policy Creation: The TPA along with token provides the rules and regulation to be followed by Creator, Reader and Writer.

User File Upload: The file creator after getting proper authentication encrypts the file and uploads his files in the cloud.

KDC Key Generation: The Key Distribution Centers which are decentralized generate different keys to different types of users after getting tokens from users

Key Revocation: Whenever there is misbehavior detected upon a user his key is revoked and that particular user can neither use nor reenter the cloud environment.

Cloud Admin: Cloud admin has the list of Key Distribution Centers (KDCs) and Third Party Authenticator (TPA) [5]. The cloud admin sets the norms to be followed by TPA and KDC [11]. It monitors the key generation policies and informs abnormal behaviors.

VI. DESIGN GOALS

In this paper we aim to design efficient mechanisms for dynamic data verification and operation to achieve the following goals:

- Distributed access control of data stored in cloud so that only authorized users with valid attributes can have access over stored data.
- The proposed scheme avoids replay attacks.
- The identity of the user is protected from the cloud during authentication.
- The architecture is decentralized, meaning that there can be several KDCs for key management. [11]
- The access control and authentication are both collusion resistant, meaning that no two users can collude and access data or authenticate themselves, if they are individually not authorized.
- Revoked users cannot access data after they have been revoked.

VII. SECURE DATA STORAGE IN CLOUD

WORKING

The Network Methodology [4] of this process consist of mainly six modules namely [6]

1. Authentication module
2. Web server identification
3. Encryption
4. Web server updation
5. Decryption
6. Data verification

Authentication Module: As the name suggest this module is to register the new users and previously registered users can have entry into the project. The Registerd user only can enter into Proposed Process in the Project.

Web Server Identification: After entering in the workgroup name the peer list is obtained. This is divided into active peer list and inactive peer list. The active peer list is divided into

ISSN: 2278 – 1323

long lived peer and short lived peer. The long lived peer list is selected and is used for further process.

Encryption: Encryption process used to securely transmit data in open networks. Data encryption needs to be secure by resisting statistical attacks and other types of attacks. In this module data encrypted in the use of key and stored in TPA part.

Web Server Updating: This module corresponds to the original data stored in a particular selected web server web server used for user processing. User can able to process these data without rules.

Decryption: Decryption is the reverse process to Encryption. Frequently, the same Cipher is used for both Encryption and Decryption. While Encryption creates a Cipher text from a Plaintext, Decryption creates a Plaintext from a Cipher text. In this module decrypt the encrypted information for verification

Data Verification: In this module data verification performed in the use of already decrypted content with old content. In this verification used to identify the changes in web server data.

In cloud storage system [6] [7], companies stores their data in the remotely located data server. Accordingly, correctness of the data is assured. Even though sometimes unauthorized person may modify or delete the data which leads to server compromise and/or random Byzantine failures, because it can be the first step for fast recovery of the storage errors.

VIII. MERITS

- Compared to many of its predecessors, which only provide binary results about the storage state across the distributed servers, the challenge-response protocol in our work further provides the localization of data error.
- Unlike most prior works for ensuring remote data integrity, the new scheme supports secure and efficient dynamic operations on data blocks, including: update, delete and append.
- Extensive security and performance analysis shows that the proposed scheme is highly efficient and resilient against Byzantine failure, malicious data modification attack, and even server colluding attacks.

IX. CONCLUSION

The main aim of this paper is to highlight the problems of data security in cloud data storage. And also provided a way out to ensure user correctness of stored data along with it preserved the user's identity. Also we propose a distributed scheme through homomorphism token with distributed KDC. Additionally, this technique provides a process to avoid colluding attacks of server modification by unauthorized users we believe that data storage security in Cloud Computing, an area of challenges and of dominant significance, is still in its infancy to be identified. We envision several possible directions for future research on this area. It allows Third Parity Auditor to audit the cloud data storage without demanding users' time, probability. Also we have presented a decentralized access control technique with anonymous authentication, which provides user revocation and prevents replay attacks. The cloud does not know the identity of the user who stores information, but only verifies the user's credentials. Key distribution is done in a decentralized way.

X. ACKNOWLEDGMENT

The real spirit of achieving a goal is through the way of excellence and lustrous discipline. I would have never succeeded in completing my task without the cooperation, encouragement and help provided to me by various personalities. I would like to take this opportunity to express my heartfelt thanks to my guide Prof. Ankur. O. Bang for his esteemed guidance and encouragement, especially through difficult times. His suggestions broaden my vision and guided me to succeed in this work. I am also very grateful for his guidance and learnt many things under his leadership. I extend my thanks to Prof. V. P. Narkhade, Head of Computer Science & Engineering Department, Pankaj Laddhad Institute of Technology and Management Studies, Buldana for their valuable support that made me consistent performer. I also extend my thanks to Dr. P. M. Jawandhiya, Principal, Pankaj Laddhad Institute of Technology and Management Studies, Buldana for their encouragement.

XI. REFERENCES

[1] Deepanchakaravarthi Purushothaman, Dr.Sunitha Abburu "An Approach for Data Storage Security in Cloud Computing" IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 2, No 1, March 2012, ISSN (Online): 1694-0814.

[2] Nikita pathrabe, Deepali khtawar "Ensuring data storage security in cloud computing" International Journal of Research in Advent Technology, Vol.2, No.2, February 2014, E-ISSN: 2321-9637

[3] Cong Wang, Qian Wang, KuiRen, Wenjing Lou, "Towards Secure and Dependable Storage Services in Cloud Computing," IEEE transactions on Services Computing, 06 May 2012.

[4] D. Kanchana, Dr. S. Dhandapani "A Novel Method for Storage Security in Cloud Computing", International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 2, Issue 2, March 2013.

[5] L. Geng F. David Z. Jinzy D. Glenn, ―Cloud computing: IT as Service, ―IEEE computer society IT Professional,‖ Vol. 11, pp.10-13, Apr. 2009.

[6] Marios D. Dikaiakos, Dimitrios Katsaros, Pankaj Mehra, George Pallis, Athena Vakali, ―Cloud Computing: Distributed Internet Computing for IT and Scientific Research,‖ IEEE Internet Computing Journal, vol. 13, issue.5, pp. 10-13, Sep.2009.

[7] R. Maggiani, Communication Consultant, Solari Communication, ―Cloud Computing is Changing How we Communicate,‖ 2009 IEEE International Professional Conference, IPCC, pp. 1-4, Waikiki, HI, USA, Jul. 2009.

[8] B.Anjani Kumar, K.Hari Prasad, C.Subash Chandra"Homomorphic Token and Distributed Erasure-Code for cloud",International Journal of Research in Computer and Communication Technology, Vol 2, Issue 10, October- 2013.

[9] B. Shwetha Bindu1, B. Yadaiah2**,"** Secure Data Storage In Cloud Computing" International Journal of Research in Computer Science ISSN 2249-8257 Volume 1 Issue 1 (2011) pp. 63-73

[10] Miss. Roopa G, Mr. Manjunath S "Secure Way of Storing Data in Cloud Using Third Party Auditor",IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 12, Issue 4 (Jul. - Aug. 2013), PP 69-74

ISSN: 2278 – 1323

[11] R.Vaishali ,M.Menaka"Attribute based Encryption and Key Distribution for Secure Storage in Clouds ",© 2014 IJEDR | Conference Proceeding (NCISECT 2015)|ISSN: 2321-9939

[12] S Divya Bharathy,T RameshS Divya Bharathy et al,"Securing Data Stored in Clouds Using Privacy Preserving Authenticated Access Control" International Journal of Computer Science and Mobile Computing, Vol.3 Issue.4, April- 2014, pg. 1069-1074.

AUTHORS:

Miss. Swati I. Bairagi Student of First year M.E. (Computer Science And Engineering) PLITMS Buldhana- Sant Gadge Baba Amravati University. Has earned degree of B.E.(Computer Science and Engineering) from Sant Gadge Baba Amravati University in 2014.

Prof. A.O.Bang Assistant Professor and M.E. Co-ordinator Computer Science and Engineering Department, Pankaj laddhad Institute of technology and management studies, Buldana. Has earned M.E. (CSE) from Amravati University, Amravati and B.E.(CSE) From Amravati university, Amravati

ISSN: 2278 – 1323