IJDCST @Feb-March-2015, Issue- V-3, I-3, SW-03
ISSN-2320-7884 (Online)
ISSN-2321-0257 (Print)

Public Auditing for Shared Data in the Cloud by Using AES

[1] Syagamreddy Subbareddy, [2]P.Tejaswi, [3]D.Krishna
[1]M.Tech(CSE) Pursuing, [2]Associate Professor,[3]Associate Professor,HOD,
[1,2,3]Dept. of Computer Science and Engineering,
[1,2,3]Jawaharlal Nehru Institute of Technology.

Abstract: In this paper, we tend to propose a completely unique privacy-preserving mechanism that supports public auditing on shared information hold on within the cloud. Particularly, we tend to exploit ring signatures to cipher verification data required to audit the correctness of shared information. With our mechanism, the identity of the signer on every block in shared information is unbroken personal from public verifiers, WHO square measure ready to expeditiously verify shared information integrity while not retrieving the complete file. Additionally, our mechanism is in a position to perform multiple auditing tasks at the same time rather than substantiative them one by one. The propose system Oruta, a privacy-preserving public auditing mechanism for shared information within the cloud. we tend to utilize ring signatures to construct homomorphism authenticators, in order that a public friend is in a position to audit shared information integrity while not retrieving the complete information, nonetheless it cannot distinguish WHO is that the signer on every block. To boost the potency of sustentative multiple auditing tasks, we tend to any extend our mechanism to support batch auditing. There square measure 2 attention-grabbing issues we are going to still study for our future work. One in every of them is traceability, which suggests the power for the cluster manager to reveal the identity of the signer supported verification data in some special things

Keywords: auditing, privacy, shared information

I. INTRODUCTION

Cloud service suppliers supply users economical and scalable data storage services with a way lower marginal cost than ancient approaches [2]. It's routine for users to leverage cloud storage services to share knowledge with others in a group, as knowledge sharing becomes a customary feature in most cloud storage offerings, as well as Dropbox, iCloud and Google Drive.The integrity of knowledge in cloud storage, however, is subject to skepticism and scrutiny, as knowledge hold on within the cloud will easily be lost or corrupted thanks to the inevitable hardware/ software failures and human errors [3], [4]. To form this matter even worse, cloud service suppliers is also reluctant to inform users regarding these knowledge errors so as to maintain the name of their services and avoid losing profits [5]. Therefore, the integrity of cloud knowledge ought to be verified before any knowledge utilization, like search or computation over cloud knowledge [6]. The traditional approach for checking knowledge correctness is to retrieve the whole knowledge from the cloud, so verify data integrity by checking the correctness of signatures (e.g., RSA [7]) or hash values (e.g., MD5 [8]) of the whole data. Certainly, this typical approach is in a position to with success check the correctness of cloud knowledge. However,the potency of exploitation this ancient approach on cloud data is doubtful [9]. The main reason is that the dimensions of cloud knowledge is giant in general. Downloading the whole cloud knowledge to verify data integrity can value or perhaps waste users amounts of computation and communication resources, especially when knowledge are corrupted within the cloud. Besides, many uses of cloud knowledge (e.g., data processing and machine learning) don't essentially want users to transfer the entire cloud knowledge to native devices [2]. It's as a result of cloud providers, like Amazon, offers users computation services directly on large-scale knowledge that already existed in the cloud.

II. LITERATURE SURVEY

Certificate-Less Public Auditing for Data Integrity in The Cloud:

Due to the existence of security threats in the cloud, many mechanisms have been proposed to allow a

user to audit data integrity with the public key of the data owner before utilizing cloud data. The correctness of choosing the right public key in previous mechanisms depends on the security of Public Key Infrastructure (PKI) and certificates. Although traditional PKI has been widely used in the construction of public key cryptography, it still faces many security risks, especially in the aspect of managing certificates.

Towards Secure and Dependable Storage Services in Cloud Computing:

Cloud storage enables users to remotely store their data and enjoy the on-demand high quality cloud applications without the burden of local hardware and software management. Though the benefits are clear, such a service is also relinquishing users' physical possession of their outsourced data, which inevitably poses new security risks towards the correctness of the data in cloud. In order to address this new problem and further achieve a secure and dependable cloud storage service,

Data Storage Security Model for Cloud Computing:

Data security is one of the biggest concerns in adopting Cloud computing. In Cloud environment, users remotely store their data and relieve themselves from the hassle of local storage and maintenance. However, in this process, they lose control over their data. Existing approaches do not take all the facets into consideration viz. dynamic nature of Cloud, computation & communication overhead etc. In this paper, we propose a Data Storage Security Model to achieve storage correctness incorporating Cloud's dynamic nature while maintaining low computation and communication cost.

Auditing Data Integrity and Data Storage Using Cloud:

Cloud Computing is the long dreamed vision of computing as a utility, where users can remotely store their data into the cloud so as to enjoy the on-demand high quality applications and services from a shared pool of configurable computing resources. By data outsourcing, users can be relieved from the burden of local data storage and maintenance. However, the fact that users no longer have physical possession of the possibly large size of outsourced data makes the data integrity protection in Cloud Computing a very challenging and potentially formidable task.

Secure Cloud Storage Auditing:

Outsourcing storage into the cloud is economically attractive for the cost and complexity of long-term large-scale data storage. At the same time, though, such a service is also eliminating data owners' ultimate control over the fate of their data, which data owners with high service-level requirements have traditionally anticipated. As owners no longer physically possess their cloud data, previous cryptographic primitives for the purpose of storage correctness protection cannot be adopted, due to their requirement of local data copy for the integrity verification.

II. PROPOSED SYSTEM

The propose system Oruta, a privacy-preserving public auditing mechanism for shared data in the cloud. We utilize ring signatures to construct homomorphism authenticators, so that a public verifier is able to audit shared data integrity without retrieving the entire data, yet it cannot distinguish who is the signer on each block. To improve the efficiency of verifying multiple auditing tasks, we further extend our mechanism to support batch auditing. There are two interesting problems we will continue to study for our future work. One of them is traceability, which means the ability for the group manager to reveal the identity of the signer based on verification metadata in some special situations

III. ADVANTAGES:

- The proposed system can perform multiple auditing tasks simultaneously
- They improve the efficiency of verification for multiple auditing tasks.
- High security provide for file sharing.

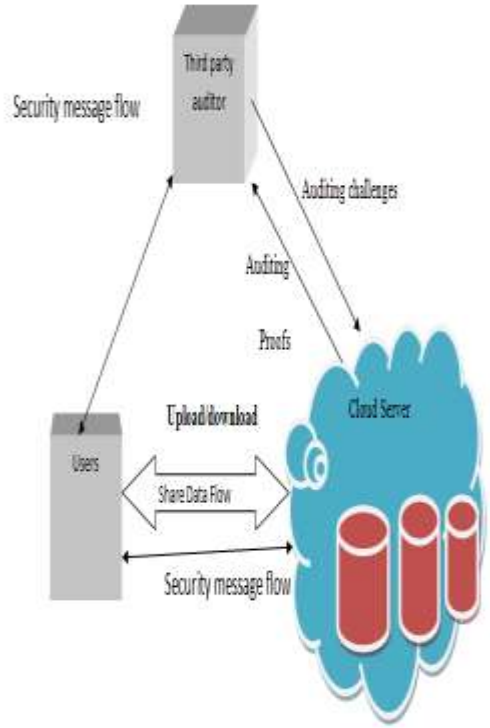

FIG:1 ARCHITECTURE DIAGRAM

PROPOSED WORK:

User Registration and Control:

This module can be also used to register users for custom modules that support personalization and user specific handling. If the users wish to create their own user accounts, i.e. register, then registration checks for the username availability and assign unique ID. User Control means controlling the login with referring the username and password which are given during the registration process. After login, the user can encrypts the original data and stored it in database, and the user can retrieve the original data which gets decrypted after checking the unique ID and searched data. Based on their logins, they have rights to view, or edit or update or delete the contents of resources. Part of the stored data are confidential, but when these institutions store the data to equipment afforded by cloud computing service provider, priority accessing to the data is not the owner, but cloud computing service provider. Therefore, there is a possibility that stored confidential data cannot rule out being leaked. Also there is no possibility to track the original data for the hackers.

IV. CRM SERVICE

This module is customer relationship management, where the user can interact with the application. CRM is concerned with the creation, development and enhancement of individualised customer relationships with carefully targeted customers and customer groups resulting in maximizing their total customer life-time value. CRM is a business strategy that aims to understand, anticipate and manage the needs of an organisation's current and potential customers. It is a comprehensive approach which provides seamless integration of every area of business that touches the customer- namely marketing, sales, customer services and field support through the integration of people, process and technology.

CRM is a shift from traditional marketing as it focuses on the retention of customers in addition to the acquisition of new customers. The expression Customer Relationship Management (CRM) is becoming standard terminology, replacing what is widely perceived to be a misleadingly narrow term, relationship marketing (RM). The main purpose of CRM is:

- The focus [of CRM] is on creating value for the customer and the company over the longer term.
- When customers value the customer service that they receive from suppliers, they are less likely to look to alternative suppliers for their needs.
- CRM enables organisations to gain 'competitive advantage' over competitors that supply similar products or services.

CRM consists of index page, registration page, login page, etc. Through this, the user can register with the user details, after registration the user can send the original data, which gets encrypted and stored in database; also the user can retrieve the original data which they stored only after decrypting the encrypted data by giving the decryption key.

V. ENCRYPTION/DECRYPTION SERVICE

This module describes about the encryption and decryption process for the original data. The encryption process is needed while storing the data, and the data decryption is needed while retrieving the data. After the user's login has been successfully

verified, if the CRM Service System requires client information from the user, it sends a request the information (for encryption and decryption) to the Storage Service System.

Encryption: In this (data storage service), the CRM Service System transmits the user ID to the Storage Service System where it searches for the user's data. This original data, once found, a request must be sent to the Encryption/Decryption Service System along with the user ID. It shows the Storage Service System executing the transmission of client data and the user ID to the Encryption/Decryption Service System. Here, the user sent original data gets encrypted and stored in storage service as per the user request. That data cannot be hacked by unauthorized one, that are more confidential and encrypted.

Decryption: In this (data retrieval service), if the user request the CRM service to retrieve the data which are stored in Storage service, the CRM sends the user ID and the search data to the Encryption/Decryption Service System. It authenticates whether the user ID and search data are owned by the same user. If authenticated, the encrypted data from the storage service system is send to the Encryption/Decryption Service System for the decryption process. In that process, it checks for decryption key, if it OK, then decrypts the encrypted data and the original data retrieved, and send to the user.

VI. ACCESSING STORAGE SERVICE

This module describes about how the data gets stored and retrieved from the database. The original data which given by the user gets encrypted and request for the storage, the storage service system store the encrypted data with the user ID for avoiding the misuse of data. Also during retrieval, the user request for retrieving the data by giving the search data, the storage service system checks for user ID and search data are identical, if so it sends the encrypted data to the Encryption/Decryption Service System for the decryption process, it decrypts the data and sends to the user. The user interacts with the database every time through the CRM service only.

The user's goal in logging into the CRM Service System is possibly to maintain part of the client data, thus the system design must take data maintenance into consideration. Feasible design methods include matching the encrypted client data with the corresponding user ID and client ID, thus allowing for the indexing of the user ID to obtain the corresponding client data. Then the client ID can be used to index the client data the user wishes to maintain. Considering the massive amount of client data, search efficiency could be improved by combining the user ID and client ID to form a combined ID used for searching for a specific client's data.

In the new business model, multiple cloud service operators jointly serve their clients through existing information technologies including various application systems such as ERP, accounting software, portfolio selection and financial operations which may require the user ID to be combined with other IDs for indexing stored or retrieved data. In addition, the foregoing description of the two systems can use Web Service related technology to achieve operational synergies and data exchange goals.

Conclusion:

In this paper, we tend to propose Oruta, a privacy-preserving public auditing mechanism for shared information within the cloud. We utilize ring signatures to construct homomorphic authenticators, so that a public booster is in a position to audit shared information integrity while not retrieving the complete information, nonetheless it cannot distinguish World Health Organization is that the signer on every block. To improve the potency of validatory multiple auditing tasks, we further extend our mechanism to support batch auditing.

References:

[1] B. Wang, B. Li, and H. Li, "Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud," Proc. IEEE Fifth Int'l Conf. Cloud Computing, pp. 295-302, 2012.

[2] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A. Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A View of Cloud Computing," Comm. ACM, vol. 53, no. 4, pp. 50-58, Apr. 2010.

[3] K. Ren, C. Wang, and Q. Wang, "Security Challenges for the Public Cloud," IEEE Internet Computing, vol. 16, no. 1, pp. 69-73, 2012.

[4] D. Song, E. Shi, I. Fischer, and U. Shankar, "Cloud Data Protection for the Masses," Computer, vol. 45, no. 1, pp. 39-45, 2012.

[5] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing," Proc. IEEE INFOCOM, pp. 525-533, 2010.

[6] B. Wang, M. Li, S.S. Chow, and H. Li, "Computing Encrypted Cloud Data Efficiently under Multiple Keys," Proc. IEEE Conf. Comm. and Network Security (CNS '13), pp. 90-99, 2013.

[7] R. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public Key Cryptosystems," Comm. ACM, vol. 21, no. 2, pp. 120-126, 1978.

SYAGAMREDDY SUBBAREDDY

M.Tech(CSE) Pursuing
subbareddy4it@gmail.com

P.Tejaswi, B.Tech (CSE) M.Tech (CSE) is having

6+ years of relevant work experience in Academics, Teaching, she is working as an Associate Professor, Jawaharlal Nehru Institute of Technology, Ibrahimpatnam, Hyderabad, Telangana and utilizing her teaching skills, knowledge, experience and talent to achieve the goals and objectives of the Engineering College in the fullest perspective. She has attended seminars and workshops. Her areas of interest Network security, Image processing, Computer networks & C Programming.

D.Krishna, B.Tech (CSE) M.Tech (CSE) is having 12+ years of relevant work experience in Academics, Teaching, and Lifetime Member of ISTE. At present, he is working as an Associate Professor, HOD of CSE Dept, Jawaharlal Nehru Institute of Technology, Ibrahimpatnam, Hyderabad, Telangana State, India and utilizing his teaching skills, knowledge, experience and talent to achieve the goals and objectives of the Engineering College in the fullest perspective. He has attended seminars and workshops. He has published more than fifteen research papers in International journals. He has also guided ten postgraduate students. His areas of interest Data Mining, Data Warehousing, Cloud computing, Network security, Automata theory & Compiler Design.