Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 3, March 2014, pg.926 – 931

RESEARCH ARTICLE

RELIABLE AND SECURE AUDITING IN CLOUD DATA STORAGE

Mr.K.LOHESWARAN,
Assistant Professor,
Department of Information Technology,
Tamilnadu College of Engineering, Coimbatore.
loheswaran.k@gmail.com

Ms.S.JAYABHARATHI,
Student,
Tamilnadu College of Engineering,
Coimbatore.
jeya3bharthi@gmail.com

Ms.V.K.DEEPIKA,
Student,
Tamilnadu College of Engineering,
Coimbatore.
anudeeptha3@gmail.com

ABSTRACT

Cloud computing is the delivery of computing and storage capacity as a service to a community of end-recipients. Cloud computing entrusts services with a user's data, software and computation over a network. 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 unavoidably poses new security risks toward the correctness of the data in cloud. In order to address this new problem and further achieve a secure and dependable cloud storage service, we propose in this paper a flexible distributed storage integrity auditing mechanism Third Party Auditing (TPA) technique utilizing the homomorphism token and distributed erasure-coded data. The proposed design allows users to audit the cloud storage with very lightweight communication and computation cost. The auditing result not only ensures strong cloud storage correctness guarantee, but also simultaneously achieves fast data error localization, i.e., the identification of misbehaving server. Considering the cloud data are dynamic in nature, the proposed design further supports secure and efficient dynamic operations on outsourced data, including block modification, deletion, and append. Analysis shows the proposed scheme is highly efficient and resilient against Byzantine failure, malicious data modification attack, and even server scheming attacks.

***KEYWORDS**: Cloud, Third Party Auditing, Encryption, Integrity*

1. INTRODUCTION

Cloud computing is a type of computing that relies on sharing computing resources rather than having local servers or personal devices to handle applications. It achieves coherence and economies of scale, similar to a utility over a network. The term "cloud computing" is mostly used for hosted services in the sense of application service provisioning that run client server software at a remote location. Such services are given popular acronyms like 'SaaS' (software as a service), 'PaaS' (platform as a service), 'IaaS' (infrastructure as a service), 'HaaS' (hardware as a service) and finally 'EaaS' (everything as a service). End users access cloud-based applications through web browser, thin client or mobile applications while the business software and user's data are stored on servers at a remote location. Examples include Amazon Web Services and Google App engine, which allocate space for a user to deploy and manage software "in the cloud". The goal of cloud computing is to allow users to take benefit from all of these technologies, without the need for deep knowledge about or expertise with each one of them. The cloud aims to cut costs, and help the users focus on their core business instead of being impeded by IT obstacles.

In cloud computing, data owners may share their outsourced data with a number of users, who might want to only retrieve the data files they are interested in. One of the most popular ways to do so is through keyword-based retrieval [1] in which users retrieve relevant files in a file set based on keywords. A series of certain symmetric encryption techniques have been used to retrieve the data from the cloud. However when the data is retrieved from the cloud, the user may be prone to some attacks such as Malicious attacks, Data modification attacks, Server clouding attacks. Further tolerate faults or server crash occurs as user’s data grow in size and importance. In order to safeguard the data and to detect the misbehaving server or attacker’s intrusion, we propose in this system a technique called the Third Party Key Auditing Technique.

When data is stored in the cloud, especially in large volumes, it is burdensome to download the information and ensure the data is intact and uncompromised. It is expensive and time consuming to dedicate staff to review every detail. Therefore third-party auditing IS implemented to verify the data is secure and undamaged. Features for third-party auditing include the ability to challenge the system to ensure that changes are not allowed or tracked for analysis. Data is protected from view by the third party. To implement third party audit for cloud computing operations, the owner of the data must set up a private key and a public key. The private key allows total access to the data stored in the cloud. The public key allows access to certain blocks of data (primarily through tags or other qualifiers) that the independent verifier will use to test the security, integrity and vulnerability of the data stored. By initiating challenges to the system, the verifiers can detect modifications, corrupt files and deletions. Ignoring security assessment in cloud computing environments is risky business. Auditing actively provides search for vulnerabilities and engaging qualified, trustworthy third-party verifiers are intended to boost consumer confidence and protect privileges information from unauthorized access and corruption.

2. SCENARIOS

Cloud computing system provides a greater service in public and private sectors, business industries, mobile applications and many more activities. Cloud computing is about a very simple idea—consuming and delivering services from ‘the cloud’ issues regarding the types of cloud computing and the scope of deployment.

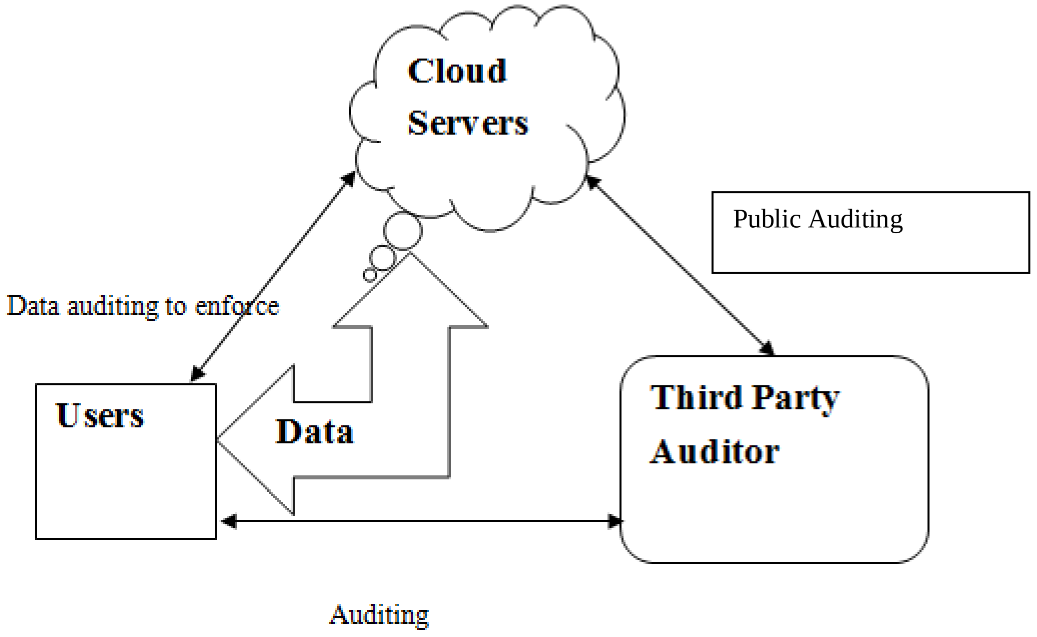
Key Findings- Many large enterprises are interested in cloud computing, but are concerned about security, regulatory compliance and uptime. The term ‘private cloud computing’ describes the style of computing used by a modern internal IT provider which is similar to that of an external cloud-computing service provider. Almost all Global 1000 organizations have server virtualization projects in place, and many consider those the basis for their private cloud computing strategies.

Market Implications- Cloud computing has a promising future, but many large enterprises will invest in the near term on private cloud-computing services, especially in the area of infrastructure-as-a- service (IaaS). Virtualization of servers and storage will be the basis for most (but not all) of these architectures, but virtualization alone is not sufficient. Large enterprises will be investing in technologies that enable service automation, chargeback and self-service. These changes will also help drive cultural, political, funding and organizational changes that will make a future migration to external cloud computing services an easier and more viable choice. This will also spur more enterprise IT organizations to operate like a business. Private cloud computing will not make sense for all organizations. Investment in private cloud computing requires a business case, and a return on investment before external cloud computing services mature. Private cloud computing will primarily make sense for larger enterprises, and enterprises with unique security and service requirements.

Enhancements-Understand your IT service portfolios, service-level requirements and service costs before building a private cloud service. Develop a separate strategic plan for all services under consideration, as well as an analysis against external service offerings. Build a private cloud service only after you have developed a complete business case analysis for doing so— it's all about return on investment, in terms of cost and business value. Evaluate and constantly benchmark yourself against external cloud service offerings, and ensure that you design in flexibility to migrate in the future.

3. THIRD PARTY AUDITING

Third party auditing is a technique which helps the user to audit the data. Third party auditing provides streamline processing. Third-party-auditor not only uses data but also modify the data than how data owner or user uses. Here the user has two types' keys, one of which only the owner knows called private key and another one which is known to anyone called public key. We match both the data it must be same as the sent one. The downloading of data for its integrity verification is not feasible task since it's very costly because of the transmission cost across the network. For well organization it is very essential that cloud that allows investigation from a single party audit the outsource data to ensure data security and save the user's computation and data storage. It is very important to provide public auditing service for cloud data storage, so that the user trusts an independent third party auditor (TPA). TPA checks the integrity of data on cloud on the behalf of users, and it provides the reasonable way for users to check the validity of data in cloud. Public auditing in addition to user provides the external party to verify the correctness of stored data against external attacks it's hard to find. So users depend on only TPA for their security storage.



Cloud service provider has significant storage space and computation resource to maintain the users' data. It also has expertise in building and managing distributed cloud storage servers and ability to own and operate live cloud computing systems. Users should be equipped with certain security means so that they can make sure that their data is safe. Cloud service provider always online & assumed to have abundant storage capacity and computation power. The third party auditor is invariably online, too. It makes every data access be in control.

When the user requests the cloud the information they need, cloud will verify the key and will provide the information back. Here auditing of information occurs to ensure its integrity and security. There are two keys public and private key. The user with the private key is given full access to the data after verification of the login. Whereas in public auditing the common users are given little access and full access is given only after verification of their login details. Cloud will always be online. But the users cannot be online every time, it depends upon user's comfortability. So a certain agreement is signed between the server and the user. It is a service level agreement in which the users can access the data they need even if they are in offline. It is limited to certain period of time, in which the agreement is made between the user and the server.

4. SYSTEM DESIGN

4.1. User Registration and Control When the user wishes to access the information, he needs to get registered. Registration of users supports 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 encrypt the original data and stored it in the 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.

4.2. CRM Service

Customer relationship management is a 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.

4.3. Encryption/Decryption Service

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 sends 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.

4.4. Accessing Storage service

Accessing Storage Service 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.

5. CONCLUSION AND FUTUREWORK

In this paper we have described the auditing process to identify the third parties who access the information or the server misbehaving. Third party auditing decrypts and encrypts the data as per the authorization provided. It establishes a relationship management between the customer and the server in accessing the data efficiently and reliably. It provides security services which secures user data. It reliefs the client from maintaining any kind of key information and allowing the client for using any browser enabled device to access the cloud services. It allows the client to verify the integrity of the data stored on download or retrieval of its own stored data in cloud. The client can share the data securely with specific band of people without any overhead of key distribution.

Third party auditing provides reliable and secure data sharing among users, it allows users to access the data in online mode. But if the user is in offline mode he cannot access the data. For that we can use a service called the service level agreement in which the user can access the data for a certain period of time by having an agreement between the server and the user. More enhancements can be done in the cloud data to provide a secure data access and retrieval for the users.

REFERENCES

[1] Jiadi Yu, Member, IEEE, Peng Lu, Yanmin Zhu, Member, IEEE, Guangtao Xue, Member, IEEE Computer Society, and Minglu Li "Toward Secure Multikeyword Top-k Retrieval over Encrypted Cloud Data", 2013

[2] Michael Armbrust, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy Katz, Andy Konwinski, Gunho Lee, David Patterson, Ariel Rabkin, Ion Stoica, and Matei Zaharia ,UC Berkeley Reliable Adaptive Distributed Systems Laboratory. "A View of Cloud Computing" http://radlab.cs.berkeley.edu/ February 10, 2009

[3] C. Wang, Q. Wang, K. Ren, and W. Lou, "Ensuring Data Storage Security in Cloud Computing," Proc. 17th Int'l Workshop Quality of Service (IWQoS '09), pp. 1-9, July 2009.

[4] Amazon.com, "Amazon Web Services (AWS)," http://aws. amazon.com, 2009.

[5] Sun Microsystems, Inc., "Building Customer Trust in Cloud Computing with Transparent Security,"https://www.sun.com/offers/details/sun_transparency.xml, Nov. 2009.

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

[7] M. Arrington, "Gmail Disaster: Reports of Mass Email Deletions," http://www.techcrunch.com/2006/12/28/gmail-disasterreportsof-mass-email-deletions, Dec. 2006.

[8] D. Song, D. Wagner, and A. Perrig, "Practical Techniques for Searches on Encrypted Data," Proc. IEEE Symp. Security and Privacy, 2000.

[9] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-Preserving Multikeyword Ranked Search over Encrypted Cloud Data," Proc. IEEE INFOCOM, 2011.

[10] J.-S. Coron, A. Mandal, D. Naccache, and M. Tibouchi, "Fully Homomorphic Encryption over the Integers with Shorter Public Keys," CRYPTO '11: Proc. 31st Ann. Conf. Advances in Cryptology, 2011.

[11] O. Regev, "New Lattice-Based Cryptographic Constructions," J. ACM, vol. 51, no. 6, pp. 899-942, 2004.