ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 2, Issue 2, February 2013

Enhanced audit services for the correctness of outsourced data in cloud storage

V.Venkatesh, P.Parthasarathi

Abstract— **Introduction of cloud storage service has made the users to access their data anywhere anytime without any trouble. Available systems that provide support for the remote data integrity are useful for quality of service testing but do not deal with server failure or handling misbehaving servers. The proposed system ensures storage integrity in the server where the cloud user's data is stored. It achieves strong cloud storage security and fast data error localization with the results provided by the auditing mechanism that is carried out by the Third Party Auditor. Also it further supports secure and efficient dynamic operations on outsourced data. Third Party Auditor carries out the public auditing in-order to maintain the integrity for the data stored in cloud. The user delegates the integrity checking tasks of the data stored in the cloud storage to the Third Party Auditor, who then does the auditing process. Reed Solomon Erasure correcting code is used in the file distribution and dependability against Byzantine failure. Data integrity in ensured with the help of verification key along with erasure coded data which also allows handling of storage correctness and identification of misbehaving cloud server. The audit protocol blocker is introduced to monitor the correctness of the user and Third Party Auditor. It prevents the cloud users from misusing the privileges that are provided to them by the cloud server.**

Index Terms— Data integrity, outsourced data, Third Party Auditor (TPA), Audit Protocol Blocker (APB), cloud server provider (CSP), cloud user, Reed Solomon code (RS), error localization.

Manuscript received Feb , 2013.

***V.Venkatesh**, Department of Computer Science and Engineering, Sri Krishna College of Technology, Coimbatore, India.*
***P.Parthasarathi**, Department of Computer Science and Engineering, Sri Krishna College of Technology, Coimbatore, India.*

I. INTRODUCTION

Cloud storage offers huge amounts of storage space and resources to the cloud users. Due to this the users depend on the providers in order to access their data stored in the cloud storage. The outsourced data is vulnerable to various internal and external threats which challenge the data integrity. To achieve the assurance of data integrity efficient methods of correctness verifications are to be carried out on behalf of the cloud users.

The proposed system provides the verification of cloud storage and correctness with the Third Party Auditing. The internet-based online services provide various computing resources and huge amounts of storage space. However this trend is eliminating the need for local machines to handle and maintain the user's data. Due to this platform shift the users depend on their cloud service providers for the availability and integrity of the stored data. The cloud infrastructures are being more powerful and reliable than personal computing devices, yet there are number of internal and external threats for the integrity of data stored in cloud server.

As the user don't have the local copy of outsourced data, the cloud service providers can behave unfaithfully to them regarding the status of their outsourced data. Outsourcing data into the cloud helps in reducing the cost and complexities of maintaining the data, but there is no strong assurance of data integrity and availability for both enterprise and individual cloud users. In order to achieve the assurances of cloud data integrity and availability methods that enable on-demand data correctness verification has to be done on behalf of cloud users.

The data stored in the cloud database may not only be accessed but also be frequently updated by the users that which includes insertion, deletion, modification, and appending. Thus, it is also imperative to support the integration of this dynamic feature into the cloud storage correctness assurance, which makes the system design even more challenging. Last but not the least, the deployment of cloud computing is powered by data centers running in a simultaneous, cooperated, and distributed manner.

In the file preparation to provide redundancies and guarantee the data dependability against Byzantine server's Reed Solomon erasure correcting code is used, where a storage server may fail in arbitrary ways. By utilizing the unique verification key with erasure-coded data, whenever data corruption has been detected during the storage correctness verification the identification of the misbehaving servers can be done. In order to save the time, computation resources, and the online burden of users, we also provide the extension of the proposed main scheme to support third-party auditing, where users can safely delegate the integrity checking tasks to TPA and can be worry-free to use the cloud storage services.

II. RELATED WORKS

Kui Ren [7], proposed the publicly auditable cloud data storage which is able to help the cloud economy become fully established. This auditing service helps the data owners' to maintain their data effectively that is present in the cloud storage. The proposed system accounts the users regarding the usage of their data by both the user himself and the TPA. Services for the legacy users is made available, who may not only access but also modify the data in the cloud.

Qian Wang [9], proposed a system that deals with the problem of ensuring the integrity of data storage in cloud with the help of a Third Party Auditor. Data integrity is achieved through the public auditing that is carried out on the users data by the Third Party Auditor. Block tag authentication is made to handle the data from the cloud storage efficiently. For the data that is stored in the cloud database, there is need for remote data integrity check which assurers the cloud users with a sense of security regarding their data. The third party audit ting has to be made available in such a way that no additional burden is introduced to the cloud users. A single Third Party Auditor is capable of handling multiple auditing tasks, which is achieved with the bilinear aggregate signature technique.

Cong Wang [6], proposed an auditing system which is carried out in such a way that the Third Party Auditor does its job without demanding the copy of user's data. Also the Third Party Auditor is not capable of deriving the user's data while performing the auditing task. To verify the correctness of the cloud data on demand from the cloud users the Third Party Auditor is used, who without retrieving a copy of the whole data or introducing additional online burden to the cloud users performs the auditing.

Mehul A. Shah [5], proposed a system that describes approaches and system hooks that support both internal and external auditing of online storage services. Online service oriented economy is which businesses and end users purchase IT services from a variety of online service providers. Third-party auditing is an accepted method for establishing trust between two parties with potentially different incentives. Auditors assess and expose risk, enabling customers to choose rationally between competing services.

III. PROPOSED SCHEME

The proposed system is to provide the cloud users dependable cloud storage where they can safely store their data. The main goal of the proposed system is to increase the storage security for the user's outsourced data.

Fig.1 represents the block diagram of the dependable cloud storage services scheme. First the users have to be authenticated in order to use the services offered to them by the cloud service provider. Once the users are approved by the Cloud Administrator, a mail containing a unique verification key is sent to them. The user uses this verification key as a second login key in order to use the services offered to them.

For uploading a file into the cloud storage the user selects the file from the local storage. This file is then encoded using the Reed Solomon erasure correcting code. The users encoded file is then moved to the cloud storage which the user can access anywhere anytime. The TPA is used to audit the users outsourced files in-order to maintain integrity. If the user's encoded file is same as it was stored in the cloud storage, it is decoded and used by the user. Suppose if the file is found to be corrupted the erasure correcting code is used to correct the errors and then the file is decoded.

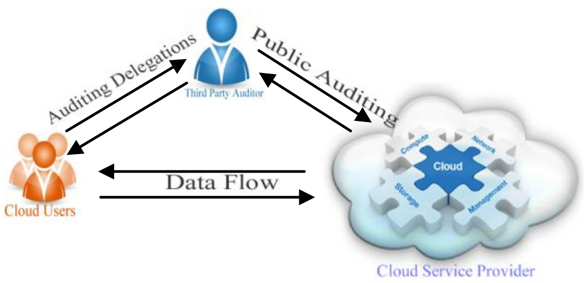

Fig 1. Overall Process of the Proposed System

A. System model

Fig. 1 represents the network architecture for cloud storage service. Here the User is an entity who relies on the cloud for data storage and computation. Cloud Server Provider is an entity to provide data storage service with significant storage space and computation resources. Third-Party Auditor who has expertise and capabilities to assess and expose risk of cloud storage services on behalf of the users upon request.

In cloud data storage, a user's stores their data through a CSP into a set of cloud servers, which are running in a simultaneous, cooperated, and distributed manner. Data redundancy can be employed with a technique of erasure correcting code to further tolerate faults or server crash as user's data grow in size and importance. For application purposes, the user's interacts with the cloud servers via CSP to access or retrieve their data. Here the focus is mainly on the support of file-oriented cloud applications other than non-file application data, such as social networking data. In other words, the cloud data that is considered here is not expected to be rapidly changing in a relative short period.

Users should be equipped with security means so that they can make continuous correctness assurance of their stored data even without the existence of local copies. If the users do not have the time, feasibility or resources to monitor their data online, they can delegate the data auditing tasks to an optional trusted TPA of their respective choices. However, to securely introduce such a TPA, any possible leakage of user's outsourced data toward TPA is to be prohibited with the help of Audit Protocol Blocker.

B. Authenticating cloud users and Third Party Auditor using verification key

The user and Third Party Auditor must be authenticated in order to use the services provided by the cloud service provider. Once the users or the Third Party Auditor has successfully completed the registration process, the verification code is sent to the mail id provided during the registration time. The cloud service provider decides the fate of the cloud user and the TPA. On the confirmation by the CSP the users will receive a conformation mail regarding their services.

Now the users can login into the cloud server in order to request the service form the cloud server. Each and every time the user or the TPA tries to access their account a verification key is generated to authenticate them. This verification key is generated by using the time and date function which can be used to provide maximum security. Verification key that is generated is unique and so it can be generated only once for that particular time when the user or the Third Party Auditor is login to use the cloud service. This verification code is used to grant access to the user and the Third Party Auditor.

C. File distribution to the cloud storage

After successful login the cloud user can carry on the file operations that are granted by the CSP. In cloud data storage, we rely on erasure-correcting code to distribute the data file across a set of servers. Reed-Solomon erasure-correcting code is used to create redundancy parity vectors from data vectors in such a way that the original data vectors can be reconstructed from data and parity vectors.

By placing each of the vectors on a different server, the original data file can survive the failure on the server without any data loss. The encoded file is obtained by multiplying the data file and the dispersal matrix, derived from a Vander monde matrix.

D. Correctness verification and error localization

Localization of the error is a potential way to eliminate errors in storage systems. It is also of critical importance to identify potential threats from external attacks. However, many previous schemes do not explicitly consider the problem of data error localization. The proposed scheme integrates the correctness verification and error localization i.e., misbehaving server identification with the help of the auditing results provided by the TPA along with the distributed erasure correcting code. The user verifies whether the received values remain a valid codeword determined by the secret matrix. The inconsistency among the storage is successfully detected by using the audit reports, the erasure codes are used to further determine where the potential data error lies in.

E. Third Party Auditor

As discussed, in case the user does not have the time, feasibility, or resources to perform the storage correctness verification, they can optionally delegate this task to an independent third-party auditor, making the cloud storage publicly verifiable. However, to securely introduce an effective TPA, the auditing process should bring in no new vulnerabilities toward user data privacy.

The TPA should not learn user's data content through the delegated data auditing. If the blinding of data vector is done before file distribution encoding, the storage verification task can be successfully delegated to third party auditing in a privacy-preserving manner. The correctness validation and misbehaving server identification for TPA is enhanced with the usage of the Audit Protocol Blocker. There is no way for TPA to learn the data content information during auditing process as the APB monitors the entire transaction.

F. Audit Protocol Blocker

The proposed system incorporates the previous system advantages and extends to find the unauthorized user, to prevent the unauthorized data access for preserving data integrity. The proposed system monitors the user requests according the user specified parameters and it checks the parameters for the new and existing users.

The system accepts existing validated user, and prompts for the new users for the parameter to match requirement specified during user creation for new users. If the new user prompt parameter matches with cloud server, it gives privileges to access the audit protocol otherwise the system automatically blocks the audit protocol for specific user.

If the TPA tries to read the user's content at the time of auditing the APB comes into light and blocks the appropriate TPA form granted accesses. This remains the same for the authorized users also.

IV. RESULTS AND DISCUSSION

The proposed storage of data into cloud server is demonstrated using the private cloud setup with open stack. The visual studio 2008 and SQL server 2005 is used in building the ASPX pages that are used in demonstration of the proposed work.

Microsoft Visual Studio 2008 helps individual developers and small development teams accelerate solution development. Deliver breakthrough user experiences for all the users. Collaborate more effectively while building solutions for the Web, Windows, the Microsoft Office system, and Windows Mobile.

Visual Studio is a complete set of development tools for building ASP.NET Web applications, XML Web Services, desktop applications, and mobile applications. Visual Basic, Visual C#, and Visual C++ all use the same integrated development environment, which enables tool sharing and eases the creation of mixed-language solutions. In addition, these languages use the functionality of the .NET Framework, which provides access to key technologies that simplify the development of ASP Web applications and XML Web Services.

Regardless of which platform is being targeted, Visual Studio 2008 delivers the productivity, performance, and stability required to help developers remain focused on the real business challenges, along with a broad ecosystem that helps ensure they can always find the partners, information, and other community members to help them deliver great software. Also included is SQL Server 2005 Compact Edition, SQL Server 2005 Express Edition and MSDN Express documentation.

The following are the visual studio 8 run-time member functions that are involved in the proposed system.

- Conversion Functions
- Math Functions
- String Functions

- Type Conversion Functions
- CType Function

V. CONCLUSION

The problem of data security in cloud data storage is the main focus here, which is essential in distributed storage system. To achieve the assurances of cloud data integrity and availability and enforce the quality of dependable cloud storage service for users, an effective and flexible distributed scheme with explicit dynamic data support is proposed. Erasure-correcting code is used in the file distribution preparation to provide redundancy parity vectors and guarantee the data dependability against several internal and external attacks. By utilizing the unique verification key along with distributed verification of erasure coded data, identification of the misbehaving servers is made possible. The proposed main scheme is further made to support third-party auditing, where users can safely delegate the integrity checking tasks to Third Party Auditor at times when they are busy with their works and are worry-free to use the cloud storage services. The Audit Protocol Blocker is the main part that which monitors the working of the Third Party Auditor and ensures that the integrity of the user's data that is outsourced in the cloud storage is the same as the user had outsourced.

REFERENCES

[1] Bowers .K.D, Juels .A, and Oprea .A, "Proofs of Retrievability: Theory and Implementation," Proc. ACM Workshop Cloud Computing Security (CCSW '09), pp. 43-54, 2009.

[2] Dodis .Y, Vadhan .S, and Wichs .D, "Proofs of Retrievability via Hardness Amplification," Proc. Sixth Theory of Cryptography Conf. (TCC '09), Mar. 2009.

[3] Erway .C, Kupcu .A, Papamanthou .C, and Tamassia .R, "Dynamic Provable Data Possession," Proc. 16th ACM Conf. Computer and Comm. Security (CCS '09), pp. 213-222, 2009.

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

[5] Shah .M.A, Baker .M, Mogul .J.C, and Swaminathan .R, "Auditing to Keep Online Storage Services Honest," Proc. 11th USENIX Workshop Hot Topics in Operating Systems (HotOS '07), pp. 1-6, 2007.

[6] Wang .C, Chow .S.S.M, Wang .Q, Ren .K, and Lou .W, "Privacy-Preserving Public Auditing for Secure Cloud Storage," IEEE Trans. Computers, preprint, 2012, doi:10.1109/TC.2011.245.

[7] Wang .C, Ren .K, Lou .W, and Li .J, "Towards Publicly Auditable Secure Cloud Data Storage Services," IEEE Network Magazine, vol. 24, no. 4, pp. 19-24, July/Aug. 2010

[8] Wang .Q, Wang .C, Li .J, Ren .K, and Lou .W, "Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing," Proc. 14th European Conf. Research in Computer Security (ESORICS '09), pp. 355-370, 2009.

[9] Wang .Q, Wang .C, Ren .K, Lou .W, and Li .J, "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing," IEEE Trans. Parallel and Distributed Systems, vol. 22, no. 5, pp. 847-859, 2011.

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

Mr. V.Venkatesh has received Bachelor of Engineering degree in Computer Science and Engineering from SNS College of Engineering under Anna University, Chennai in 2011. He is currently pursuing Master of Engineering degree in Computer Science and Engineering in Sri Krishna College of Technology under Anna University, Coimbatore, India. His areas of interest are Operating System, Networks, and Cloud Computing.

Mr. P.Parthasarathi received B.E (CSE) in 2007 from Mookambigai college of Engineering, M.E (CSE) in 2010 from Bannari Amman Institute of Technology. Since 2010, he has been working as Assistant Professor in the department of Computer Science & Engineering, Sri Krishna College of Technology. His Research interests include Operating System, Virtualization Techniques, and Cloud Computing