ISSN: 2321-7782 (Online)
Impact Factor: 6.047

Volume 4, Issue 6, June 2016

International Journal of Advance Research in Computer Science and Management Studies

Research Article / Survey Paper / Case Study

Available online at: www.ijarcsms.com

Implementing Data Security in Cloud Computing

Mini Batra[1]
Department of Computer Science
Gateway Institute of Engineering & Technology (GIET),
Deenbandhu Chhotu Ram University of Science & Technology (DCRUST),
Sonepat – India

Anil Arora[2]
Department of Computer Science
Gateway Institute of Engineering & Technology (GIET),
Deenbandhu Chhotu Ram University of Science & Technology (DCRUST),
Sonepat – India

Abstract: In the digital world using technology and new technologies require safe and reliable environment, and it also requires consideration to all the challenges that technology faces with them and address these challenges. Cloud computing is also one of the new technologies in the IT world in this rule there is no exception. According to studies one of the major challenges of this technology is the security and safety required for providing services and build trust in consumers to transfer their data into the cloud. In this paper we attempt to review and highlight security challenges, particularly the security of data storage in a cloud environment. Also, provides some offers to enhance the security of data storage in the cloud computing systems. We propose an effective and flexible distributed scheme with explicit dynamic data support to ensure the correctness of users' data in the cloud.

Keywords: Cloud Computing Storage, Cloud computing Security, Erasable Correcting Code.

I. INTRODUCTION

Cloud Computing [1] provides us a means by which we can access the applications as utilities, over the Internet. It allows us to create, configure, and customize applications online. It offers online data storage, infrastructure and application. The term **Cloud** refers to a **Network** or **Internet**. In other words, we can say that Cloud is something, which is present at remote location. Cloud can provide services over network, i.e., on public networks or on private networks, i.e., WAN, LAN or VPN. Applications such as **e-mail, web conferencing, customer relationship management (CRM),** all run in cloud.

The cloud makes it possible for users to access information from anywhere anytime. It removes the need for users to be in the same location as the hardware that stores data. Once the internet connection is established either with wireless or broadband, user can access services of cloud computing through various hardware. This hardware could be a desktop, laptop, tablet or phone.

From the perspective of data security, which has always been an important aspect of quality of service, Cloud Computing inevitably poses new challenging security threats for number of reasons.

1. Firstly, traditional cryptographic primitives for the purpose of data security protection cannot be directly adopted due to the users' loss control of data under Cloud Computing. Therefore, verification of correct data storage in the cloud must be conducted without explicit knowledge of the whole data. Considering various kinds of data for each user stored in the cloud and the demand of long term continuous assurance of their data safety, the problem of verifying correctness of data storage in the cloud becomes even more challenging.

2. Secondly, Cloud Computing is not just a third party data warehouse. The data stored in the cloud may be frequently updated by the users, including insertion, deletion, modification, appending, reordering, etc. To ensure storage correctness under dynamic data update is hence of paramount importance.

These techniques, while can be useful to ensure the storage correctness without having users possessing data, cannot address all the security threats in cloud data storage, since they are all focusing on single server scenario and most of them do not consider dynamic data operations. As a complementary approach, researchers have also proposed distributed protocols for ensuring storage correctness across multiple servers or peers. Again, none of these distributed schemes is aware of dynamic data operations. As a result, their applicability in cloud data storage can be drastically limited.

In this paper, we propose an effective and flexible distributed scheme with explicit dynamic data support to ensure the correctness of users' data in the cloud. We rely on erasure correcting code in the file distribution preparation to provide redundancies and guarantee the data dependability. This construction drastically reduces the communication and storage overhead as compared to the traditional replication-based file distribution techniques.

II. Characteristics of Cloud Computing

To better understand Cloud computing, the US National Institute of Science and Technology (NIST) define it as: "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or client and service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models".

NIST define cloud computing essential characteristics as follows [3]:

1. **On-demand Self-service**: A cloud user can individually provision computing capabilities, such as server time and network storage, thus, eliminating the need for a mediator, since the user can manage automatically and access the resources required as needed without requiring human interaction with each service provider.
2. **Broad Network Access:** Regardless of the end-user platform, users benefit from the cloud and control them through standard mechanisms.
3. **Resource Pooling**: Cloud resources, such as storage, processing, memory, and network bandwidth are pooled to provide for multiple clients using a multi-tenant model, according to the user's demand. Private cloud may only be offsite at a location controlled by the owner or the provider may allow clients to specify general server locations.
4. **Rapid Elasticity**: In the cloud, provided resources can be dynamically and elastically allocated and released. This provides scalability for more or fewer resources on demand automatically. This is one reason Denial-of-Service (DoS) attacks are decreasing, as companies with adequate cloud accounts are no longer vulnerable.
5. **Measured services:** The control and optimization of resources is done automatically in the cloud using metering capability, according to the type of service storage, processing, bandwidth, and active user accounts. This provides transparency for both the cloud vendor and the clients by monitoring, controlling, and reporting resource usage for the utilized service.

III. Problem Statement

Moving data into the cloud offers great convenience to users since they don't have to care about the complexities of direct hardware management. The pioneer of Cloud Computing vendors, Amazon Simple Storage Service (S3) and Amazon Elastic Compute Cloud (EC2) [19] are both well-known examples. While these internet-based online services do provide huge amounts of storage space and customizable computing resources, this computing platform shift, however, is eliminating the responsibility of local machines for data maintenance at the same time. As a result, users are at the mercy of their cloud service providers for the availability and integrity of their data.

From the perspective of data security, which has always been an important aspect of quality of service, Cloud Computing inevitably poses new challenging security threats for number of reasons. Firstly, traditional cryptographic primitives for the purpose of data security protection cannot be directly adopted due to the users' loss control of data under Cloud Computing. Therefore, verification of correct data storage in the cloud must be conducted without explicit knowledge of the whole data. Considering various kinds of data for each user stored in the cloud and the demand of long term continuous assurance of their data safety, the problem of verifying correctness of data storage in the cloud becomes even more challenging. Secondly, Cloud Computing is not just a third party data warehouse. The data stored in the cloud may be frequently updated by the users, including insertion, deletion, modification, appending, reordering, etc. To ensure storage correctness under dynamic data update is hence of paramount importance. However, this dynamic feature also makes traditional integrity insurance techniques futile and entails new solutions. Last but not the least, the deployment of Cloud Computing is powered by data centers running in a simultaneous, cooperated and distributed manner. Individual user's data is redundantly stored in multiple physical locations to further reduce the data integrity threats. Therefore, distributed protocols for storage correctness assurance will be of most importance in achieving a robust and secure cloud data storage system in the real world.

IV. Ensuring Security in Cloud Data Storage

In cloud data storage system, users store their data in the cloud and no longer possess the data locally. Thus, the correctness and availability of the data files being stored on the distributed cloud servers must be guaranteed. One of the key issues is to effectively detect any unauthorized data modification and corruption, possibly due to server compromise and/or random Byzantine failures. Besides, in the distributed case when such inconsistencies are successfully detected, to find which server the data error lies in is also of great significance, since it can be the first step to fast recover the storage errors.

To address these problems, our main scheme for ensuring cloud data storage is presented in this section. The first part of the section is devoted to a review of basic tools from coding theory that is needed in our scheme for file distribution across cloud servers. Then, the homomorphic token is introduced. The token computation function we are considering belongs to a family of universal hash function [20], chosen to preserve the homomorphic properties, which can be perfectly integrated with the verification of erasure-coded data [21]. Subsequently, it is also shown how to derive a challenge response protocol for verifying the storage correctness as well as identifying misbehaving servers. Finally, the procedure for file retrieval & error recovery based on erasure-correcting code is outlined.

V. Implementation

Implementation is the stage of the project when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective. The implementation stage involves careful planning, investigation of the existing system and it's constraints on implementation, designing of methods to achieve changeover & evaluation of changeover methods.

Modules

Our Implementation of Security in Cloud Data Storage consists of multiple modules as described below:

1. Client Module: In this module, the client sends the query to the server. Based on the query the server sends the corresponding file to the client. Before this process, the client authorization step is involved. On the server side, it checks the client name and its password for security process. If it is satisfied and it then received the queries from the client and search the corresponding files in the database. Finally, find that file and send to the client (figure 5.1 below). If the server finds the intruder means, it set the alternative path to those intruders.

2. Cloud data storage Module:

Cloud data storage, a user stores his data through a CSP into a set of cloud servers, which are running in a simultaneous, the user interacts with the cloud servers via CSP to access or retrieve his data. In some cases, the user may need to perform block level operations on his data. 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. In case users do not necessarily have the time, feasibility or resources to monitor their data, they can delegate the tasks to an optional trusted TPA of their respective choices.

3. Cloud Authentication Server:

The Authentication Server (AS) functions as any AS would with a few additional behaviours added to the typical client-authentication protocol. The first addition is the sending of the client authentication information to the masquerading router. The AS in this model also functions as a ticketing authority, controlling permissions on the application network. The other optional function that should be supported by the AS is the updating of client lists, causing a reduction in authentication time or even the removal of the client as a valid client depending upon the request.

4. Unauthorized data modification and corruption module:

One of the key issues is to effectively detect any unauthorized data modification and corruption, possibly due to server compromise and/or random Byzantine failures. Besides, in the distributed case when such inconsistencies are successfully detected, to find which server the data error lies in is also of great significance

Activity Diagram

An activity diagram is characterized by states that denote various operations. Transition from one state to the other is triggered by completion of the operation. The purpose of an activity is symbolized by round box, comprising the name of the operation. An operation symbol indicates the execution of that operation. This activity diagram depicts the internal state of an object.

Figure 1 below shows the activity diagram of our implementation.

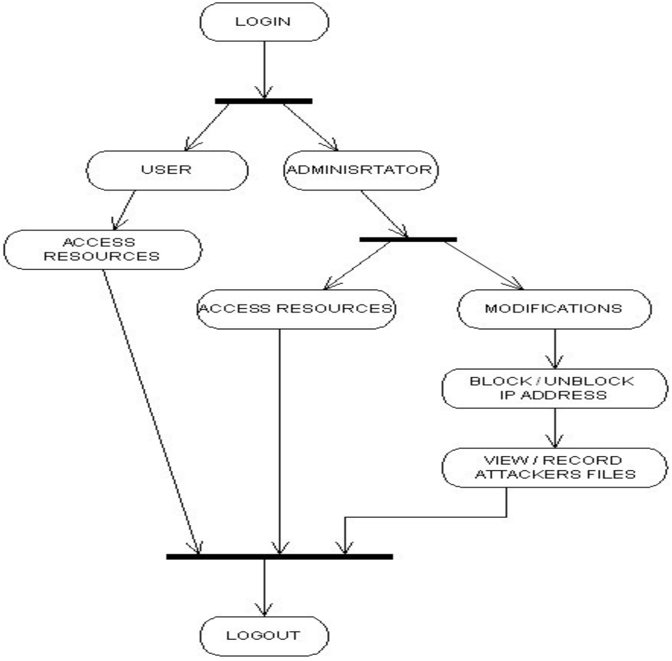

Figure 1: Activity Diagram

Sequence Diagram

The sequence diagrams are an easy and intuitive way of describing the system's behaviour, which focuses on the interaction between the system and the environment. This notational diagram shows the interaction arranged in a time sequence. The sequence diagram has two dimensions: the vertical dimension represents the time and the horizontal dimension represents different objects. The vertical line also called the object's *lifeline* represents the object's existence during the interaction.

Figure 2 shows the sequence diagram of our implementation.

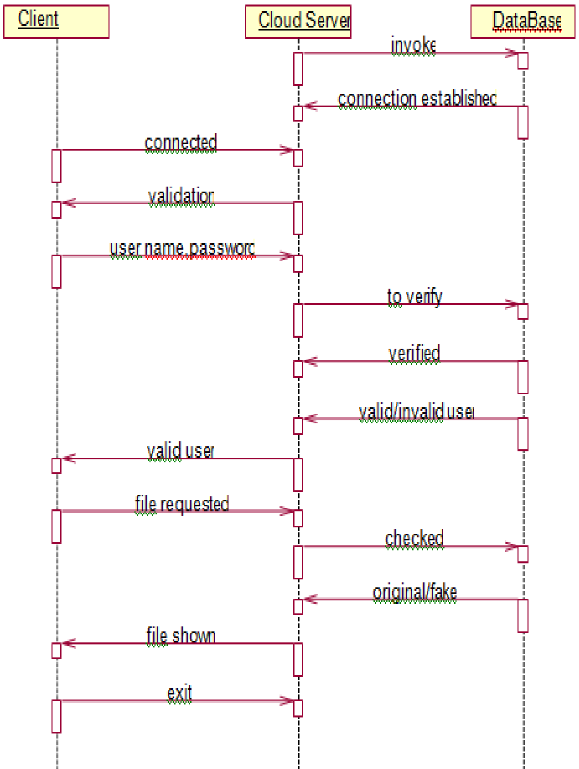

Figure 2: Sequence Diagram

VI. Conclusion and Future Scope

In this thesis, we investigated the problem of data security in cloud data storage, which is essentially a distributed storage system. To ensure the correctness of users' data in cloud data storage, we proposed an effective and flexible distributed scheme with explicit dynamic data support, including block update, delete, and append. We rely on erasure-correcting code in the file distribution preparation to provide redundancy parity vectors and guarantee the data dependability.

We believe that data storage security in Cloud Computing, an area full of challenges and of paramount importance, is still in its infancy now, and many research problems are yet to be identified. We envision several possible directions for future research on this area. The most promising one we believe is a model in which public verifiability is enforced. Public verifiability, supported in allows TPA to audit the cloud data storage without demanding users' time, feasibility or resources.

References

1. Anthony T.Velte, Toby J.Velte, Robert Elsenpeter, "Cloud Computing, A Practical approach"
2. B. Hayes, "Cloud Computing," Commun. ACM, vol. 51, no. 7, pp. 9–11, Jul. 2008.
3. P. Mell and T. Grance, "The NIST definition of cloud computing (draft)," NIST special publication, vol. 800, no. 145, p. 7, 2011.
4. V.KRISHNA REDDY, Dr. L.S.S.REDDY, "Security Architecture of Cloud Computing", Interna
5. Syam Kumar P and Subramanian R, "An Efficient and Secure Protocol for Ensuring Data Storage Security in Cloud Computing", IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 6, No 1, November 2011.

6. Abbas Amini, MSc thesis, “Secure Storage in Cloud Computing”, Department of Informatics and Mathematical Modelling (IMM), the Technical University of Denmark, May 2012.

7. K.Govinda and Dr.E.Sathiyamoorthy, "Identity Anonymization and Secure Data Storage using Group Signature in Private Cloud", Published by Elsevier Ltd., Procedia Technology, April, 2012.

8. SwarnalataBollavarapu and Bharat Gupta, “Data Security in Cloud Computing”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 3, March 2014.

9. S. Subashini and V. Kavitha, “A survey on security issues in service delivery models of cloud computing,” Journal of Network and Computer Applications, vol. 34, no. 1, pp. 1 – 11, 2011.

10. Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, “Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing,” IEEE Transactions on Parallel and Distributed Systems, vol. 22, no. 5, pp. 847–859, May 2011.

11. C. Modi, D. Patel, B. Borisaniya, H. Patel, A. Patel, and M. Rajarajan, “A survey of intrusion detection techniques in Cloud,” Journal of Network and Computer Applications, vol. 36, no. 1, pp. 42–57, Jan. 2013.

12. P. Gupta, A. Seetharaman, and J. R. Raj, “The usage and adoption of cloud computing by small and medium businesses,” International Journal of Information Management, vol. 33, no. 5, pp. 861 – 874, 2013.

13. A. Chonka, Y. Xiang, W. Zhou, and A. Bonti, “Cloud security defence to protect cloud computing against HTTP-DoS and XML-DoS attacks,” Journal of Network and Computer Applications, vol. 34, no. 4, pp. 1097 – 1107, 2011.

14. G. Reese, Cloud application architectures: [building applications and infrastructure in the Cloud]. Sebastopol, CA: O’Reilly Media, Inc, 2009.

15. J. W. Rittinghouse, Cloud computing: implementation, management, and security. Boca Raton: CRC Press, 2010.

16. S. Bugiel, S. Nürnberger, A.-R. Sadeghi, and T. Schneider, “Twin clouds: An architecture for secure cloud computing,” in Workshop on Cryptography and Security in Clouds, WCSC, 2011, vol. 2011.

17. A.-R. Sadeghi, T. Schneider, and M. Winandy, “Token-Based Cloud Computing,” in Trust and Trustworthy Computing, vol. 6101, A. Acquisti, S. Smith, and A.-R. Sadeghi, Eds. Springer Berlin Heidelberg, 2010, pp. 417–429.

18. U. Somani, K. Lakhani, and M. Mundra, “Implementing digital signature with RSA encryption algorithm to enhance the Data Security of cloud in Cloud Computing,” in Parallel Distributed and Grid Computing (PDGC), 2010 1st International Conference on, 2010, pp. 211–216.

19. Amazon.com, “Amazon Web Services (AWS),” Online at http://aws. amazon.com, 2008.

20. L. Carter and M. Wegman, “Universal Hash Functions,” Journal of Computer and System Sciences, vol. 18, no. 2, pp. 143–154, 1979.

21. J. Hendricks, G. Ganger, and M. Reiter, “Verifying Distributed Erasure coded Data,” Proc. 26th ACM Symposium on Principles of Distributed Computing, pp. 139–146, 2007.