ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 2, February 2014

Data Storage and Data Security in Cloud Server

Kajal Sharma[1], Love Verma[2]

RITEE, Raipur, India [1]

Assistant Professor, Information Technology, RITEE, Raipur, India [2]

Abstract: Cloud Computing can be defined as a new style of computing in which dynamically scalable and often virtualized resources are provided as services over the internet. With Cloud Computing Technology, users utilize a variety of devices, including PCs, laptops, smart phones to access data, programs, storage, and application development platforms over the internet, through services accessible by cloud computing providers. Cloud Computing moves the application software and databases to the large data centers. We recommend in this paper a more valuable secure storage of data in the cloud with the authentication scheme. It allows users to store data in secure mode with less communication and low computation cost. This scheme supports secure and efficient dynamic operations on data blocks, including: data update, delete and append because the cloud data are dynamic in nature. Extensive detailed security and performance analysis shows that the proposed method is highly efficient and resilient against Byzantine failure, malicious data modification attack, and server attacks. This scheme can almost guarantee the simultaneous localization of data errors, i.e., the identification of the misbehaving server(s).

Keywords: Cloud Computing, Byzantine failure, authentication scheme, sentinels, Cryptographic techniques.

I. INTRODUCTION

This Cloud Computing means “Internet Computing”. The term “Cloud Computing” is comes because internet is viewed as clouds; hence computation done through internet is called Cloud Computing. With the help of cloud computing the user can store and access their data via internet without worrying about the local maintenance and administration of data. Cloud computing is a universal term for anything that involves delivering hosted services over the internet [1].

These services are broadly classified into three categories: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS). Cloud computing is used by many software industries nowadays. Many industries adopt their unique security structure as the security is provided in cloud, the cloud data may be accessed from anywhere via the internet [1].

- **Infrastructure as a service (IaaS):**

In the most basic cloud-service model, providers of IaaS offer computers – physical or (more often) virtual machines – and other resources. Cloud support large numbers of virtual machines and the ability to scale services up and down according to customers' varying requirements. IaaS clouds usually offer additional resources such as a virtual-machine disk image library, raw (block) and file-based storage, firewalls, load balancers, IP addresses, virtual local area networks (VLANs), and software bundles. IaaS-cloud providers supply these resources on-demand from their large pools installed in data centers. For wide-area connectivity, clients can use either the Internet or carrier clouds (dedicated virtual private networks)

- **Platform as a service (PaaS):**

In the PaaS model, cloud providers deliver a computing platform, generally including operating system, programming language execution environment, database, and web server. Application developers can develop and run their software solutions on a cloud platform without the cost and complexity of buying and managing the underlying hardware and software layers. With some PaaS provides, the underlying computer and storage resources scale automatically to match application demand so that the cloud user does not have to assign resources manually.

- **Software as a service (SaaS)**

In the business model using software as a service (SaaS), users are provided access to application software and databases. Cloud providers handle the infrastructure and platforms that run the applications. SaaS is sometimes referred to as "on-demand software" and is usually priced on a pay-per-use basis. SaaS providers usually price applications using a subscription fee. In the SaaS model, cloud providers install and operate application software in the cloud and cloud users access the software from cloud clients. Clients of cloud do not manage the cloud infrastructure and platform where the application runs. This removes the need to install and run the application on the cloud user's have computers, which simplifies maintenance and support.

This is in essence means that the client nothing but owner of the data moves its data to a third party cloud storage server which authentically stocks up the data with it and offer it back to the client whenever necessary. An enterprise deals with huge amount of data. Generation of data is very easy but the storage of data needs the hardware to be updated frequently in order to give space to the large volume of data. In addition to data storage data maintenance also poses vast problem. Storage outsourcing of data to cloud storage helps such firms by reducing the costs of storage, maintenance and personnel. It can also guarantee a reliable storage of important data by keeping multiple copies of the data thereby reducing the chance of losing data by hardware failures. Cloud computing

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 2, February 2014

provides solution to both these problems in an effective manner. Many problems like data authentication and integrity arises when outsourcing the data. To ensure data security the cloud provider stores the data in an encrypted form. Also the scheme should minimize the local computation at the client as well as the bandwidth consumed at the client.

Moving data into the cloud offers great convenience to users and they don't have to care about the complexities of hardware management. Amazon, Google, IBM, Sun, Microsoft, Dell, HP, Intel, Novell, and Oracle have invested in cloud computing and offers a range of cloud-based solutions. Google and Microsoft are one of the well known examples. These internet-based online services, provides vast amounts of storage space and customizable computing resources and eliminating the responsibility of local machines for data maintenance at the same time.
From the perspective of data security, which has always been an important feature of quality of service (QoS), Cloud Computing certainly 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. So, verification of correct data storage in the cloud must be conducted without explicit knowledge of the complete data [4].

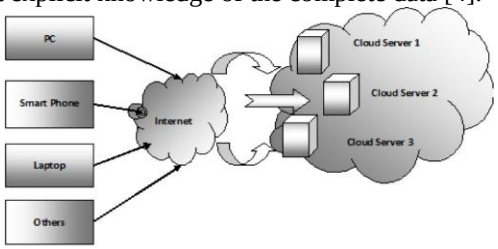

Fig.1: Cloud Data Storage Architecture

II. LITERATURE REVIEW

In the simple client server scenario, the server does not provide the resources as the cloud server provides recourses as required to clients.

In the following research works, the importance of ensuring the remote data integrity has been highlighted. 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, most of them do not consider dynamic data operations and they are all focusing on single server scenario. None of these distributed schemes is aware of dynamic data operations. As an outcome their applicability in cloud data storage can be drastically limited [3]. As a complementary approach, researchers have also proposed distributed protocols for ensuring storage correctness across multiple servers.

It is a huge problem that how to efficiently verify the correctness of data stored in cloud server without the help of local data files becomes a great challenge for data storage security in cloud computing. To guarantee the data security does not directly adopted [5].

Special blocks (called sentinels) hidden among other blocks in the data file (generated by cryptographic technique). To make the sentinels identical from the data blocks, the complete modified file is encrypted and stored at the archive. The sentinels indistinguishable from other file blocks because the use of encryption here. This scheme is best suited for storing encrypted files. It becomes computationally difficult when the data to be encrypted is large, encryption of the file using a secret key. Hence, this proves disadvantages to small users with limited computational power (PDAs, mobile phones etc.). The client needs to store all the sentinels with it, which may be storage overhead to thin clients (PDAs, low power devices etc.). The newly inserted sentinels and the error correcting codes, these create storage overhead at the server [4].

The point-to-point communication channels between each cloud server and the user is legal and consistent, which can be achieved in practice with little overhead. In Cloud Computing, data privacy is necessary but in research we do not find the data privacy and security as much [6]. The prime disadvantage is security in prior work. Cloud computing is used by many software industries nowadays. Many companies are adopting their unique security structure because the security is not provided in cloud. For example: Google has its own security structure. In this paper introducing a new and uniform security structure for all types of cloud is the problem we are going to tackle. The data placed in the cloud is available to everyone; security is not assured. Storing the most secret data in cloud is becomes risky because the data leakage by third party may possible, who is not authorize to access the cloud server. To avoid this problem we introducing a scheme called watermarking based on Steganography [2].
Firstly, for the purpose of data security protection cannot be directly adopted traditional cryptographic primitives due to the user's loss control of data under Cloud Computing. As a result, verification of correct data storage in the cloud must be conducted without knowledge of the whole data. The long term continuous assurance of user's data safety and the problem of verifying correctness of data storage in the cloud become even more challenging as we consider various kinds of data for each user stored in the cloud. Secondly, Cloud Computing is not just a third party data warehouse. The data stored in the cloud may be regularly updated by the users [3].

The work is among the first few ones in this field to consider distributed data storage in Cloud Computing [1]. The work was summarized as the following three aspects:
1) The challenge-response protocol in our work further provides the localization of data error. As compared to many of its previous work, that provides only binary results about the storage state across the distributed servers.
2) Our scheme supports secure and efficient dynamic operations on data blocks, including: update, delete and append, unlike most prior works for ensuring remote data integrity,

3) Extensive detailed 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.

IV. PROPOSED OUTCOME

In this paper, we propose an effective and flexible distributed scheme with explicit dynamic data support to ensure the correctness of user's data in the cloud. This reduces the communication and storage overhead as compared to the file distribution techniques. With the help of token the authenticated user can only access the cloud server, so the security will be increased. It provides the storage correctness insurance and data error localization. At any time data corruption has been detected during the storage correctness verification is done. This scheme can almost guarantee the identification of the misbehaving server or the simultaneous localization of data errors.

V. CONCLUSION

In this paper, we investigated the problem of data security in cloud data storage, which is essential for a distributed storage system, with the help of authentication scheme. The authenticated user can only access the cloud server. To ensure the correctness of user's data in cloud data storage, we proposed a novel and flexible distributed scheme with explicit dynamic data support, including block update, delete and append and to obtain the integration of storage correctness insurance and data error localization, i.e., at any time data corruption has been detected during the storage correctness verification across the distributed servers, by utilizing the homomorphic token with our scheme we can almost guarantee the simultaneous identification of the misbehaving server(s). We show that our scheme is highly efficient and resilient to Byzantine failure and malicious data modification attack through detailed security and performance analysis.

REFERENCES

[1] Cong Wang, Qian Wang, and Kui Ren, Wenjing Lou, "Ensuring Data Storage Security in Cloud Computing", US National Science Foundation, 2009.

[2] R.Narendran, S. Varadharajan, N.Delhiganesh, "Secure Practical Outsourcing Dependable Storage and in Cloud Computing Using honeypot", International Conference on Computing and Control Engineering (ICCCE 2012), 12 & 13 April, 2012.

[3] K.Valli Madhavi, R.Tamilkodi, R. Bala Dinakar, "Data Storage Security in Cloud Computing for Ensuring Effective and Flexible Distributed System", International Journal of Electronics Communication and Computer Engineering, 2012.

[4] Neha T, P.S Murthy, "A Novel Approach to Data Integrity Proofs in Cloud Storage", International Journal of Advanced Research in Computer Science and Software Engineering, October 2012.

[5] Vadty Redya, CH. ShivaRamaKrishna, CH. Sandhya Rani, "Providing Data Integrity for Dynamic Cloud Storage", International Journal of Emerging Trends in Engineering and Development, 2012.

[6] Durgarajesh Rachamsetty, Prof Ramakrishna Rao TK, "A Process for Data Storage security in Cloud Computing", (IJCSIT) International Journal of Computer Science and Information Technologies,2011.

[7] Keiko Hashizume, David G Rosado, Eduardo Fernández-Medina and Eduardo B Fernandez,"An analysis of security issues for cloud computing", Journal of Internet Services and Applications 2013.

[8] Srinivasa Rao V, Nageswara Rao N K, E Kusuma Kumari, "Cloud Computing: An Overview", Journal of Theoretical and Applied Information Technology, 2009.

[9] Mark Lillibridge Sameh Elnikety Andrew Birrell Mike Burrows Michael Isard, "A Cooperative Internet Backup Scheme", Proceedings of the General Track: 2003 USENIX Annual Technical Conference, 2003.\

[10] Malathi.M and Murugesan.T,"A Scheme for Checking Data Correctness in the Cloud", International Conference on Information and Network Technology (ICINT 2012).