Ensuring Data Storage Security in Cloud Computing using Java

Ms. Vidushi Rawal, Assistant Professor
Lingaya's University, Faridabad

Abhijay Vashisht,Student
Lingaya's University, Faridabad

Mansi Bhardwaj, Student
Lingaya's University, Faridabad

ABSTRACT

Cloud Computing is now popular as the next generation architecture of the IT Enterprise. The situation in the conventional solutions is that the IT services are under proper physical, logical and personnel controls whereas Cloud Computing moves the application software and databases to the large data centers, where the management of the data and services may not be fully reliable. This special attribute poses many new security challenges which have not been well understood. Here we will talk about the cloud data storage security, which has always been an essential aspect of quality of service. To ensure the exactness of users' data in the cloud, we propose an effective and versatile classified strategy with two features, opposing to its predecessors. By using the homomorphic token with distinguished affirmation of erasure-coded data, our strategy achieves the integration of storage correctness insurance and data error localization which is the identification of misbehaving server(s). The new strategy further supports efficient and secure the dynamic operations on data blocks, which includes like data update, delete and append. Performance and the immense security analysis shows that the proposed strategy is highly resilient and efficient against malicious data modification attack, and even server colluding attacks.

Keywords

Cloud Computing, Security, Data Security, Java, Privacy, Computational Modeling, Servers, Data Privacy, Security of Data, Cloud Computing Security, Security Models, Security Threats, Internet, Cloud Services, Data Centers, Security Concerns, Security Cloud, Virtual Resources, Secure Cloud Computing.

1. INTRODUCTION

Most of the trends are opening up the period of Cloud Computing, which is an Internet-based development and use of computer technology. Really cheaper and more powerful processors, together with the Software as a service (Saas) computing architecture, are converting data centers into pools of computing service on a huge scale. Constant network bandwidth and reliable and flexible network connections make it even possible that users can now get high quality services from data and software that reside entirely on remote data centers. After moving data into the cloud offers great comfort to users as they don't have to care about the complications of direct hardware management. The invention of Cloud Computing vendors, Amazon Simple Storage Service (S3) and Amazon Elastic Compute Cloud (EC2) [1] are well-known examples. Whereas these internet-based online services do provide large amounts of storage space and modifiable computing resources, this computing platform shift is omitting the responsibility of local machines for data maintenance at the same time. The result analyze that the, users are at the mercy of their cloud service providers for the availability and completeness of their data. The downtime of Amazon's S3 is best example [2]. Data security has always been an important aspect of quality of service, Cloud Computing itself poses new challenging security threats for Number of reasons.

1.1 Cryptographic primitives for the purpose of data security protection cannot be directly adopted as the user's loss control of data under Cloud Computing. Hence, verification of correct data storage must be conducted in the cloud without explicit knowledge of the whole data. We will consider that various kinds of data for each user stored in the cloud and there is demand of long term continuous assurance of their data safety, even a bigger challenge is the problem of verifying exactness of data storage in the cloud.

1.2 Cloud Computing is not just a third party data warehouse, as the data stored in the cloud may be frequently updated by the users, like insertion, deletion, modification, appending, reordering, etc. For ensuring storage exactness under dynamic, data update is important. Hence, this dynamic feature also makes conventional integrity insurance techniques futile and need new solutions.

1.3 Deployment of Cloud Computing is powered by data centers which are running in a simultaneous, cooperated and classified manner. The individual user's data is redundantly stored in multiple physical locations in order to reduce the data integrity threats. Therefore the classified protocols will be the most importance for storage exactness assurance in achieving a robust and secure cloud data storage system in the real world. Such important area still to be fully explored in the literature. The importance of ensuring the remote data integrity has been highlighted by the following research works [3]-[7]. These techniques, can be highly useful to ensure the storage exactness without having users possessing data, cannot address all the security threats in cloud data storage, as they all are concentrating on single server scenario and mostly they do not consider dynamic data operations. As a complementary approach, researchers have also proposed classified protocols [8]-[10] for ensuring storage exactness across multiple servers or peers. But, none of these distributed schemes is aware of dynamic data operations.

Therefore, their applicability in cloud data storage can be drastic. We propose an effective and flexible strategy with explicit dynamic data support to make sure the exactness of users' data in the cloud. We somehow depend on the erasure of correcting code in the file distribution preparation in order to provide redundancies and to guarantee the data dependability. With this construction there is drastic reduction in the communication and storage overhead as compared to the conventional replication-based file Distribution techniques. By using the homomorphic token with distributed verification of erasure-coded data, and the strategy applied we successfully achieves the storage exactness insurance along with data error localization. Whenever there has been detection of data corruption during the storage exactness verification, our strategy can almost guarantee the simultaneous localization of data errors, or we can say our strategy will surely identify the misbehaving server(s). Our contribution can be summarized in following three aspects:

1.3.1 With comparison to many of its predecessors, which only provide binary results about the storage state across the distributed servers, with work, the challenge-response protocol further provides the localization of data error.

1.3.2 Unlike the most prior works done for ensuring remote data integrity, the new introduced strategy supports the efficient and secure dynamic operations on data blocks, which includes: append, delete and update.

1.3.3 The immense security and performance analysis shows that the proposed strategy is highly efficient and flexible against malicious data, modification attack, and even server colluding attacks.

2. MAIN MODULES:-

2.1 Client Module:

In this module, the query is sent to the server by the client. The corresponding file is sent to the client based on the query that the server sends. Before this process, the client authorization step is involved. In the server side, it checks the client name and its password for security process. If it is satisfied and then received the queries form the client and search the corresponding files in the database. In the last step, the file is found and sent to the client. If the server finds the intruder, it sets the alternative Path to those intruder.

2.2 System Module:

Below is the illustration of Network architecture for cloud data storage. Three different network entities are known as:

2.2.1 User:

Users who use cloud to store data and rely on the cloud for data computation, can include both individual consumers and organizations.

2.2.2 Cloud Service Provider (CSP):

A CSP is the one who owns and operated live Cloud Computing Systems. He has several resources and expertise in building, as well as, managing distributed cloud storage servers.

2.2.3 Third Party Auditor (TPA):

A TPA is an optional entity who is a trusted expert who is capable of assessing and exposing the risk of cloud storage services as per the requests of the users.

2.3 Cloud data storage Module:

In Cloud data storage, data is stored by the user through a CSP into a set of cloud servers that are running in a simultaneous manner, the interaction of the user with the cloud servers takes place via CSP in which he can access or retrieve his data. The user may also need to perform block level operations on his data in some cases. To make continuous exactness assurance of the data stored, user should be equipped with some security means which can be done even without the existence of local data copies. The users, if in case lack time, feasibility or resources to monitor their data, the responsibilities can be delegated to an optional trusted TPA of their own choices. The Point-to-point communication channels is assumed authenticated and reliable here.

2.4 Cloud Authentication Server:

The Authentication Server (AS) functions typically, except a few more behavioral additions to the traditional client-authentication protocol. The client authentication information is sent to the simulating router as the first addition. 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. The Authentication Server also functions as a ticketing authority which means it controls permissions on the application network.

2.5 Unauthorized data modification and corruption module:

Any sort of modification in data and corruption possible caused by server compromises is one of the key issues to be detected effectively. Also, the cherry on the cake is to identify that in which server the data error lies in the distributed case where such data inconsistencies are detected successfully.

2.6 Adversary Module:

Basically, there are two sources where security threats are faced by cloud data storage occur. A self-interested, malicious and untrusted CSP can be one of the reasons. This leads to the hiding a data loss due to errors in the management, also, it makes a desire to move rarely accessed data to a much lower tier of storage for some monetary reasons. This storage tier is lower than the one that was agreed.

There can be a tough/economically motivated situation in which a number of cloud servers might be compromised in different intervals of time. Modification or Deletion of the user data might also take place in this condition and the worst is that even CSP might not detect this flaw for that particular moment or period of time.

Two different types of considered adversary with different capability levels are as follows:

2.6.1 Weak Adversary: The adversary is interested in corrupting the user's data files stored on individual servers. A comprised server can lead the adversary to pollute the original data files via means of modification or embedding the fraud data which might cause the changing of the original data to the fraudulent data.

2.6.2 Strong Adversary: In this case, the storage servers are compromised by the adversary so that the data files can be modified intentionally till the time that they are consistent internally. This case is known as worst case scenario in case of both adversary. This situation can be compared and contrasted to the case where servers involved collude together in order to hide corruption, as well as, a data loss.

3. FIGURES

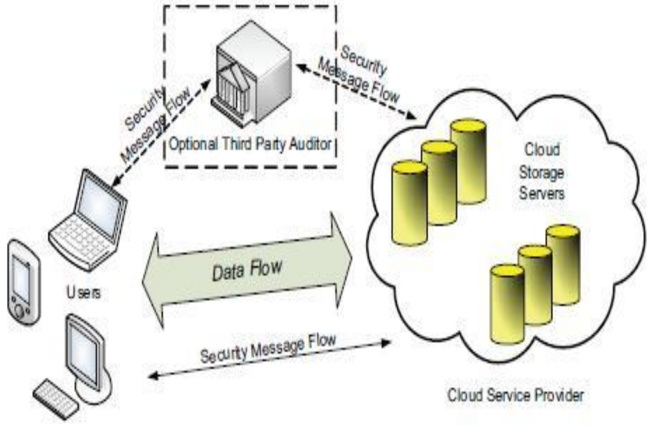

Figure: Cloud data storage architecture

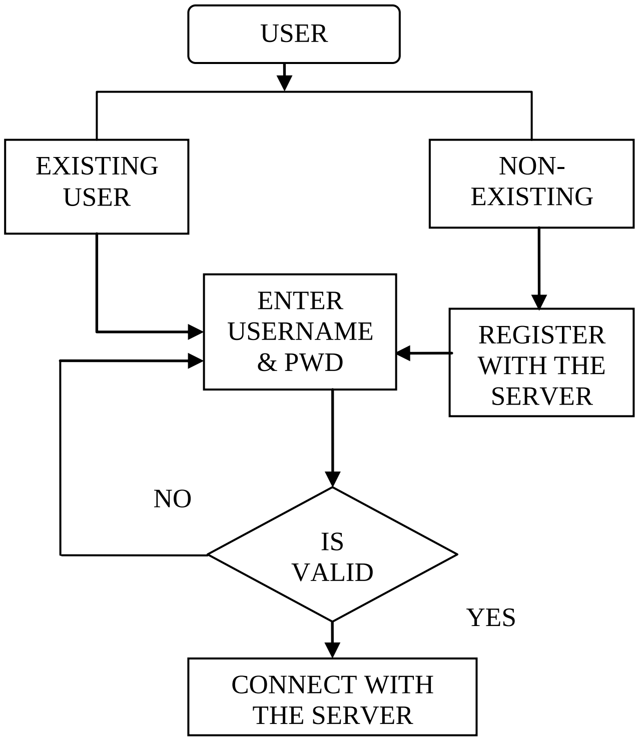

Figure: Activity Diagram

4. CONCLUSION

After studying the papers we felt the concern for data security in cloud data storage, which is a distributed storage system. To ensure the correctness of users' data stored in cloud storage, we suggested an effective and flexible distributed strategy with dynamic data support without commotion, including block update, delete, and append. We rely on the eradication-correcting code in the file distribution preparation to provide redundancy parity vectors and promise the data dependability. With the use of homomorphic token with distributed verification of erasure coded data, our strategy is to get the combination of storage exactness insurance and data error localization, i.e., whenever data corruption has been detected during the storage exactness verification across the distributed servers, we almost assure the simultaneous identification of the misbehaving server. By complete/ security and performance analysis, by doing all this we disclose that our strategy is systematic/productive and strong to malicious data, modification attack, and even server attacks. Till now data storage security in Cloud Computing is an area full of challenges and of great importance and is still in its early stage now. More over many research matters are still to be identified. We envision several possible directions for future research on this area. Most promising one according to us is a model in which public verifiability is imposed. Public verifiability, supported in, it allows TPA to audit the cloud data storage without demanding users' time, feasibility or resources. An interesting question arises in this model is that can we find a strategy to achieve both public verifiability and storage of dynamic data.

5. FUTURE SCOPE

This system can be enhanced in a lot of ways. A backup and recovery system can be added in order to recover the lost or corrupted files from the backup section. During recovery process, instead of fetching entire file from the backup data base, recovery can be done by fetching only the infected block. This will greatly lessen the communication cost. Secondly we can say, a dynamic auditing method can be implemented so that the auditor can regualrly check for the files without waiting for the request from the client. This method will completely eliminate the client's overhead. The client will simply get a notification if any of his files are lost or corrupted and asked for the recovery option. Also instead, the auditor can simply correct the content and maintain the client's data safely. Thirdly, the system can be designed to support multiple auditors so that if an auditor temporarily goes down, the other one can provide his service to the client without delay.

6. REFERENCES

[1] Amazon.com, "Amazon Web Services (AWS)," Online at http://aws. amazon.com, 2008.

[2] N. Gohring, "Amazon's S3 down for several hours," Online at http://www.pcworld.com/businesscenter/article/142549/amazons s3 down for several hours.html, 2008.

[3] A. Juels and J. Burton S. Kaliski, "PORs: Proofs of Retrievability for Large Files," Proc. of CCS '07, pp. 584–597, 2007.

[4] H. Shacham and B. Waters, "Compact Proofs of Retrievability," Proc. of Asiacrypt '08, Dec. 2008.

[5] K. D. Bowers, A. Juels, and A. Oprea, "Proofs of Retrievability: Theory and Implementation," Cryptology ePrint Archive, Report 2008/175, 2008, http://eprint.iacr.org/.

[6] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable Data Possession at Untrusted Stores," Proc. of CCS '07, pp. 598–609, 2007.

[7] G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, "Scalable and Efficient Provable Data Possession," Proc. of SecureComm '08, pp. 1– 10, 2008.

[8] T. S. J. Schwarz and E. L. Miller, "Store, Forget, and Check: Using Algebraic Signatures to Check Remotely Administered Storage," Proc. of ICDCS '06, pp. 12–12, 2006.

[9] M. Lillibridge, S. Elnikety, A. Birrell, M. Burrows, and M. Isard, "A Cooperative Internet Backup Scheme," Proc. of the 2003 USENIX Annual Technical Conference (General Track), pp. 29–41, 2003.

[10] K. D. Bowers, A. Juels, and A. Oprea, "HAIL: A High-Availability and Integrity Layer for Cloud Storage," Cryptology ePrint Archive, Report 2008/489, 2008, http://eprint.iacr.org/.