Enabling Cloud Storage Auditing with Key Exposure Resistance

MITTAL DISHA RAVIKUMAR[1], HARSH ASHOKBHAI PATEL[2], RAJ JAYANTIBHAI BHAVANI[3], YASH BHARATBHAI BHUVA[4]

[1]Data Engineer at Datagrokr Analytics pvt. Ltd., Banglore, India
[2]UG student Department of Computer Engineering, LJ institute of engineering and technology, Gujarat, India
[3-4]UG student Department of Computer Engineering, Charotar University of science and Technology, Gujarat, India

Abstract - The term "cloud computing" refers to internet-based computing that allows users to share services. Many people use the cloud to store their data. Data integrity protection in cloud computing is a challenging and sometimes risky undertaking, especially for users with limited computing resources and knowledge, because users no longer have physical control over potentially huge volumes of outsourced data. As a result, the accuracy and security of data are critical. The topic of ensuring the integrity and security of data storage in the Cloud Computing environment is investigated in this article. The data block is signed before it is transferred to the cloud, which ensures cloud security. Users can use Cloud Storage to store their data remotely and access high-quality on-demand apps and services from a shared pool of programmable computing resources, eliminating the need for local data storage and maintenance. Data integrity security in Cloud Computing is a problematic issue, especially for users with limited computing resources, because users no longer have physical control over the outsourced data. Users should also be able to access cloud storage as if it were local, without having to worry about its security. As a result, providing public auditability for cloud storage is critical, allowing clients to rely on a third-party auditor (TPA) to confirm the integrity of outsourced data while staying worry-free. The auditing procedure should introduce no new vulnerabilities to user data privacy and no more online burden for the user in order to securely implement an effective TPA. We present a safe cloud storage architecture that allows for privacy-protected public auditing in this study. We improve our result so that the TPA can audit multiple users at once and efficiently. The proposed solutions are both provably secure and exceedingly efficient, according to extensive security and performance studies.

***Key Words*: Cloud Storage, Sharing Data, Security, Internet, Easy Backup**

1. INTRODUCTION

Validating data in the cloud necessitates the use of auditing. The bulk of auditing protocols are based on the assumption that the auditing secret key held by the client is secure. Security is not totally achieved due to the client's lax security needs.

The client's data will inevitably be leaked if the auditing protocol is not secure. A new cloud auditing methodology is implemented in this study. Also, in cloud storage audits, look into measures to limit the impact of client key disclosure. The design is built upon here in order to overcome the week key auditing process. With the help of important exposure resilience experts, the auditing process was developed. To update the client's secret keys, the proposed architecture uses a binary tree structure and pre-order traversal methodology. Cloud storage auditing with key exposure resilience is incredibly successful, as evidenced by the security proof and performance.

The TCP/IP Internet is based on the idea of enabling end-to-end data flow by combining potentially divergent link-layer technologies. There are several data connection layer protocols that have been designed and are widely used around the world. However, there are numerous instances where internet assumptions are incorrect. A TCP/IP network begins to run inefficiently or stops to operate altogether when there is no end-to-end path between source and destination for the duration of a communication session, or when communication is inconsistent and may only exist for limited periods of time. The Interplanetary Internet is a good example of such a setting. The speed of light between Earth and Mars is roughly 4 minutes when they are at their closest approach. The one-way light time between Earth and Mars can approach 20 minutes when they are in opposition. The time it takes for the outer planets to reach the speed of light increases considerably. It could take up to an hour to send a file from a base station on Earth to a satellite orbiting Mars, merely to start the transfer. The File Transfer Protocol requires authorisation and authentication orders to be delivered before a data transfer can begin. For each FTP instruction, TCP uses a handshaking technique and sends three packets. Given that the round trip time for a TCP packet is at least Delay-tolerant networks (DTN) were designed to function in situations where the Internet Protocol Suite appears to be malfunctioning. A message-oriented overlay with intermittent connectivity is used in delay-tolerant networks. overcomes snarls and delays in communication It is also possible to send data between a source and a destination that is not present at the time of communication. To achieve all of the aforementioned properties, the store-and-forward message mechanism is used. The method provides services that are similar to electronic mail but with improved naming, routing, and security characteristics.

2. EXISTING SYSTEM

These protocols focus on a range of auditing issues, with one of the most pressing concerns being how to achieve high bandwidth and computing efficiency. The Homomorphic Linear Authenticator (HLA) technique, which supports blockless verification, is being investigated for this purpose in order to reduce computation and communication overheads in auditing protocols, allowing the auditor to verify the integrity of cloud data without retrieving the entire data.

Another important component of cloud storage auditing is data privacy security. A third-party auditor (TPA) is introduced to aid the client in periodically confirming the integrity of the data in the cloud, reducing the customer's computing burden. The TPA, on the other hand, may access the client's data after repeatedly performing the auditing protocol.

Wang et al. proposed a protocol for auditing that allows for fully dynamic data operations including update, insertion, and deletion.

3. DISADVANTAGES OF EXISTING SYSTEM

Despite the fact that many research studies on cloud storage auditing have been conducted in recent years, a critical security risk that is the key exposure worry for cloud storage auditing has gone unexplored in previous studies. While all previous protocols concentrated on the cloud's weaknesses or deception, they overlooked the prospect of a client's lack of security knowledge and/or inadequate security settings.

Unfortunately, previous auditing methods failed to address the critical issue of how to deal with the client's secret auditing key exposure for cloud storage auditing, and any exposure of the client's secret auditing key would render most existing auditing procedures useless.

4. PROPOSED SYSTEM

We'll look at how to reduce the impact of a client's major exposure in cloud storage audits in this article. Our goal is to develop a cloud storage auditing methodology that incorporates key-exposure resilience. How to do so in this new problem setting efficiently raises a plethora of new challenges, which will be discussed further below. To begin with, cloud storage auditing is impractical when utilising traditional key revocation techniques. This is because if a client's auditing secret key is exposed, the client must create a new combination of public and secret keys and regenerate the authenticators for the client's previously stored data in the cloud. Our goal is to provide a practical auditing protocol with key-exposure resilience, where the operational difficulties of key size, computation overhead, and communication overhead are all less than T. We use the pre-order traversal methodology on a binary tree structure to appoint time periods and associate periods with tree nodes to achieve our purpose. The secret key for each time period is organised as a stack. At each time interval, the secret key is updated via a forward-secure technique. While reaching our efficiency goals, the auditing technique assures key-exposure resilience. As we'll see later, the client can still audit the integrity of the cloud data in aggregated form, i.e. without requesting the entire data set from the cloud, using our protocol.

5. ADVANTAGES OF PROPOSED SYSTEM

We are the first to investigate how to create key-exposure resilience in storage auditing protocols, and we propose a novel concept called auditing protocol with key-exposure resilience. Even if the cloud has the client's current secret key for cloud storage auditing, dishonest acts, such as deleting or changing some client's data stored in the cloud in previous time periods, can all be identified in such a protocol.

This significant issue has not been addressed in previous auditing protocol designs. We further formalise the auditing protocol's concept and security architecture for safe cloud storage with key exposure resilience.

We develop the first realistic cloud storage auditing solution with built-in key-exposure resilience. To achieve our goal, we update the client's secret keys using the binary tree structure, which has been employed in a few previous works on different cryptographic designs. This type of binary tree structure can be regarded of as a simplified version of the HIBE scheme's tree structure. Furthermore, each binary tree node is associated with each time period using the pre-order traversal mechanism. In our whole protocol, the stack structure is used to achieve preorder traversal of the binary tree. In addition, we develop a unique authenticator to aid forward security and we also develop a revolutionary authenticator to assist with forward security and authentication property dependability

We demonstrate the security of our protocol and explain its performance using concrete asymptotic analysis in the formalised security model. The proposed approach, in fact, adds only a little amount of complexity to achieve key exposure resilience. We also show how our proposed

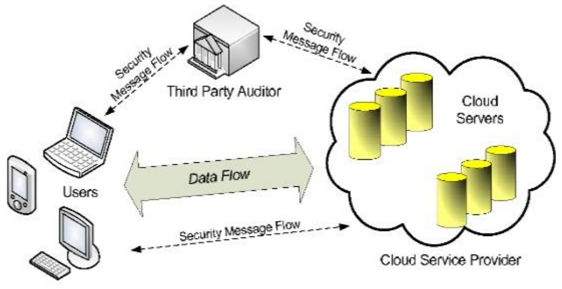


Fig. 1: The architecture of cloud data storage service

system may be modified to support TPA, lazy updating, and a variety of sectors.

6. PROJECT ENHANCEMENT

The ability to public audit allows someone other than the user to assess the validity of data saved remotely using a public key based homomorphic linear authenticator. A public auditing system is made up of four algorithms (KeyGen, SigGen, GenProof, VerifyProof)

The user configures the scheme using KeyGen, which is a key generation algorithm.SigGen is used by the user to generate verification metadata, which could contain MACs, signatures, or other data that will be used for auditing. The TPA runs VerifyProof to audit the evidence created by the cloud server, while the cloud server runs GenProof to generate a proof of data storage correctness.

There are two steps to the operation of a public auditing system:

6.1 SETUP

To generate the verification metadata, the user uses KeyGen to initialise the system's public and secret parameters, as well as SigGen to pre-process the data file F. The user then uploads the data file F to the cloud server, together with the verification information, and deletes the local copy. The user can alter the data file F as part of the pre-processing by extending it or adding additional information to be saved on the server.

6.2 AUDIT

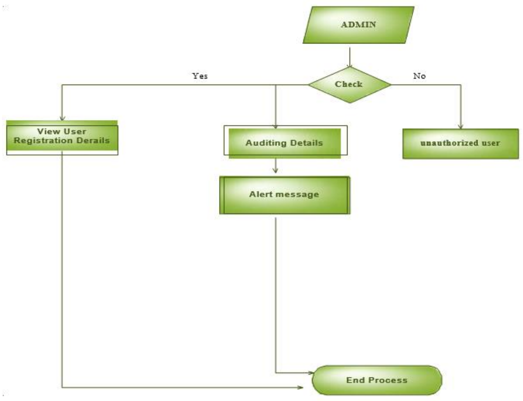
To guarantee that the data file F is correctly retained at the time of the audit, the TPA sends an audit message or challenge to the cloud server. The cloud server generates a response message based on a function of the stored data file F and its verification metadata when GenProof is launched. The TPA then validates the response with VerifyProof. A privacy-preserving public auditing tool for data storage security in Cloud Computing. We use the homomorphic linear authenticator and random masking to ensure that the TPA does not learn anything about the data content stored on the cloud server during the efficient auditing process, which not only relieves the cloud user of the time-consuming and potentially costly auditing task, but also allays their fears of data leakage. We extend our privacy-preserving public auditing protocol into a multi-user setting, where the TPA can perform multiple auditing tasks in a batch manner for improved efficiency, given that the TPA may handle multiple audit sessions from different users for their outsourced data files at the same time. Extensive testing has shown that our methods are both provably secure and extremely efficient.

7. SYSTEM DESIGN

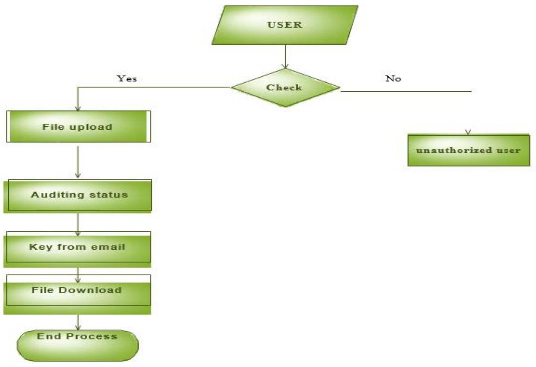
Data Flow Diagram / Use Case Diagram / Flow Diagram

A bubble chart is another name for the DFD. It's a basic graphical formalism for depicting a system in terms of its input data, various processing performed on those data, and the system's output data.

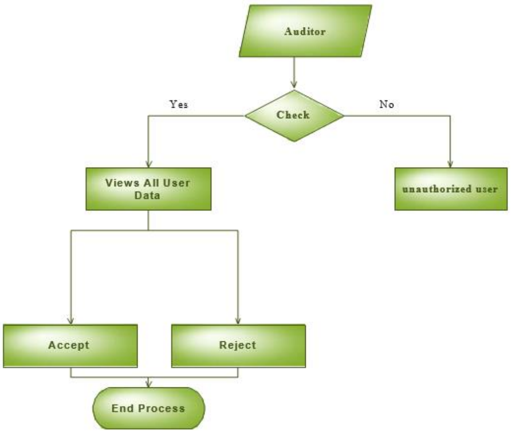
7.1 SYSTEM ADMIN



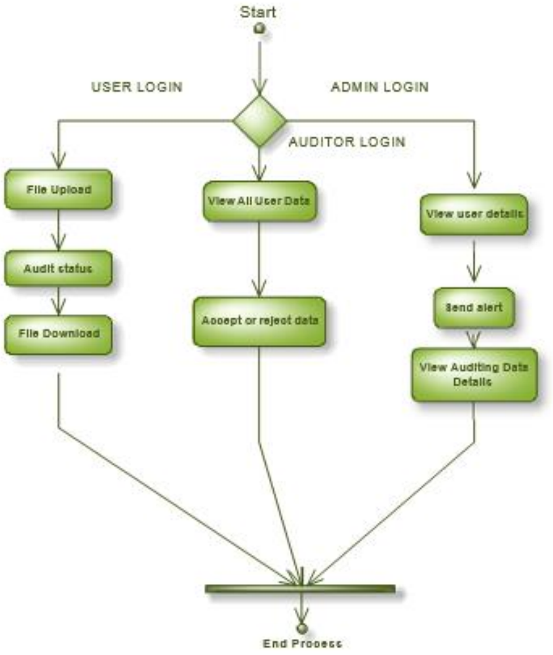
7.2 USER



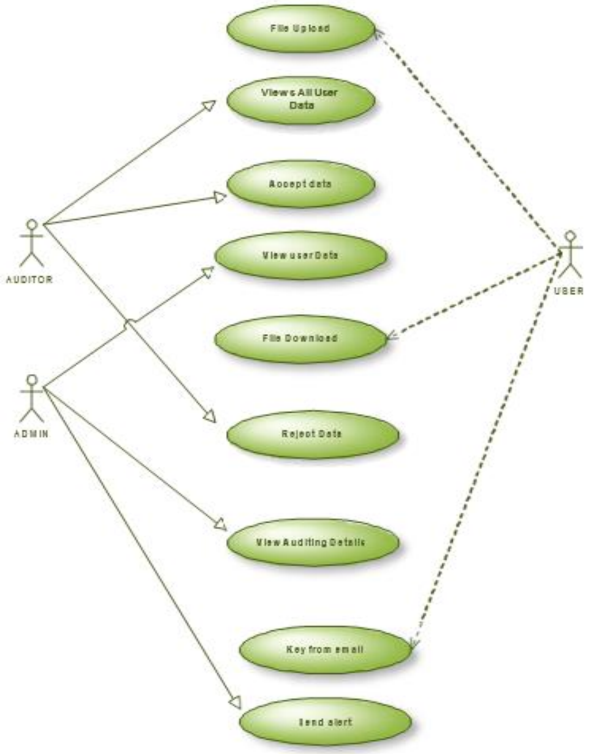
7.3 AUDITOR



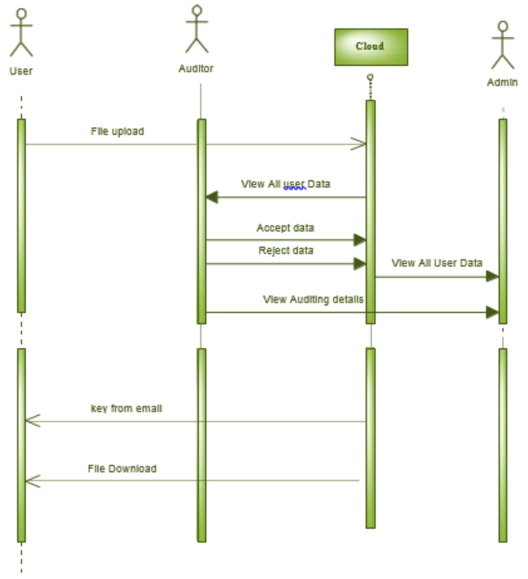
7.4 USER CASE DIAGRAM



7.5 ACTIVITY DIAGRAM



7.6 SEQUENCE DIAGRAM



REQUIREMENTS

This project contains both hardware and software requirements.

HARDWARE REQUIREMENTS:

Processor above 500 MHz

RAM: 4 GB

Hard Disk: 4 GB

Input Device: Standard Keyboard and mouse

Output Device: High Resolution monitor

SOFTWARE REQUIREMENTS:

OS: Windows 7 or higher

Front End : HTML, Java, Jsp

Script : JavaScript.

Technology: Java7, J2ee

Web Technologies: Html, JavaScript, CSS

IDE: Eclipse Juno

Web Server: Tomcat

Database: Mysql

Java Version: J2SDK1.5

8. CONCLUSION

We recommend Enabling Cloud Storage Auditing with Key-Exposure Resistance for data storage security in cloud computing. We use the homo-morphic linear authenticator and random masking to ensure that the TPA does not learn anything about the data content stored on the cloud server during the efficient auditing process, which not only relieves the cloud user of the time-consuming and potentially costly auditing task, but also allays their fears of data leakage. We extend our privacy-preserving public auditing protocol into a multi-user setting, where the TPA can perform multiple auditing tasks in a batch manner for improved efficiency, given that the TPA may handle multiple audit sessions from different users for their outsourced data files at the same time. Extensive testing has shown that our methods are both provably secure and extremely effective.

REFERENCES

[1] P. Mell and T. Grance, “Draft NIST working definition of cloud computing,” Referenced on June. 3rd, 2009 Online at http://csrc.nist.gov/groups/SNS/cloud-computing/index. html, 2009.

[2] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D.

[3] Patterson, A. Rabkin, I. Stoica, and M. Zaharia, “Above the clouds: A berkeley view of cloud computing,” University of California, Berkeley, Tech. Rep.

[4] UCB-EECS-2009-28, Feb 2009.

[5] M. Arrington, “Gmail disaster: Reports of mass email deletions,” Online at http://www.techcrunch.com/2006/12/28/gmail-disasterreports-of-mass-email-deletions/, December 2006.

[6] J. Kincaid, “MediaMax/TheLinkup Closes Its Doors,” Online at http://www.techcrunch.com/2008/07/10/media maxthelinkup-closes-its-doors/, July 2008.

[7] Amazon.com, “Amazon s3 availability event: July 20, 2008,” Online at http://status.aws.amazon.com/s3- 20080720.html, 2008.

[8] S. Wilson, “Appengine outage,” Online at http://www.cioweblog.com/50226711/appengineoutage.php, June 2008.

[9] B. Krebs, “Payment Processor Breach May BeLargest Ever,” Online at http://voices.washingtonpost.com/securityfix/ 2009/01/payment processor breach may b.html, Jan. 2009.

[10] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, “Provable data possession at untrusted stores,” in Proc. of CCS’07, Alexandria, VA, October 2007, pp. 598–609.

[11] M. A. Shah, R. Swaminathan, and M. Baker, “Privacypreserving audit and extraction of digital contents,” Cryptology ePrint Archive, Report 2008/186, 2008.

[12] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, “Enabling public verifiability and data dynamics for storage security in cloud computing,” in Proc. of ESORICS’09, volume 5789 of LNCS. Springer-Verlag, Sep. 2009, pp. 355–370.

BIOGRAPHIES

Ms. Disha Mittal, is a software engineer,currently working at Datagrokr Analytics pvt ltd as a Data Engineer

Mr. Harsh Ashokbhai Patel, is a final year student of Computer engineering, LJ institute of engineering and technology

Mr. Raj Jayantibhai Bhavani, is a final year student, department of Computer engineering, Charotar University of science and Technology

Mr. Yash Bharatbhai Bhuva, is a final year student of Computer engineering, Charotar University of science and Technology