Proc. of the Intl. Conf. on Advances In Engineering And Technology - ICAET-2014

ISBN: 978-1-63248-028-6 doi: 10.15224/ 978-1-63248-028-6-01-110

Efficient Method for Cloud Data Storage and Security Based on Third Party Auditor

Mr. Chadchankar Amarnath S.

***Abstract*—This cloud computing to realize being shifted into the next generation with. Application software and database are stored has changed. Now they cloud data centers in which safety is a concern from the point of view of the client are stored in the. Batteries that store and manage data without capital investment are used which are not well understood is the many security challenges paper cloud data integrity and security of data stored in the servers is focused on data integrity verification is a third party auditor that data integrity check from time to time on behalf of the client is authorized to use.**

Customer data from third party auditor of information gets lost when data integrity is not only data integrity verification, the proposed system also supports data mobility. The work that has been done in this online data mobility to public audit and sham Supporting. Audit for inserting and deleting data modifications functions, monitors the proposed system's ability to audit both public and data mobility support. A review of the literature the problems with existing systems revealed and that's the driving force behind this work take up Merkle hash tree. To improve the block-level authentication is used to handle auditing tasks at the same time, the overall signature bilinear transform is used for multiple clients concurrently TPA enables audit. So here I present are multi-user based TPA system. Experiments shows that the proposed system is very the efficient and safe.

Keywords—Data Security, Cloud server, data dynamic, multiple clients, Third Party Auditor, Hash Tree, Data Blocks,CSS.

I. INTRODUCTION

Is it a next generations enterprise application software and database to move the large centralized data enters, cloud computing, where data and services management is not completely reliable. Several trends which is an Internet based development and use of computer technology is kla Open up computing, us era. Ever cheaper and more powerful processors, coupled with "software-as-a-service (SaaS)"architecture, computing are transforming data centers into pools a large scale service computing. Meanwhile increasing network bandwidth and reliable INEA is flexible network connections clients now only high-quality services of data and software that reside on remote data centers can subscribe also possible. Although a promising service for the Internet to suit as a platform, the new paradigm of 'cloud' data storage choose in Autipurn design issues which deeply effects the overall system performance and security brings about. Cloud data storage is one of the biggest concerns with data integrity validation of untrusted servers. What is more serious is that the service provider money and storage difference to keep ik sha neglect or deliberately delete rarely relate to which no ordinary customer data files accessed. outsourced electronic data and the customer's constrained resource capability, original size, how big a problem customer data file local copy Script to perform periodic integrity without verifications can find an efficient manner as can be generalized to consider the role of all plans, models considering the Verifier, fall into two categories: before submitting personal ability to audit and Ability to audit public. Public audit ability allows anyone with private audit qualifications, although plans may receive a higher plan efficiency, not just keeping a personal information cloud client (Server data storage to challenge the accuracy of ate owner of the data.), Then, customers an independent third party auditor (TPA), evaluation of the performance of the service for their computing resources without the representative of devotion. Cloud, customers are often incredible integrity check itself performing overhead may not be able to afford.

Mr. Chadchankar Amarnath Shivanand
Sinhgad Institute of Technology, Lonavala, Pune
Pune University
Maharastra , India

II. LITERATURE SURVEY

Recently increasing interests i in the context of remotely stored data validation efforts. Ateniese et al. [1] his Government defined audit ability to consider for the first time are "provable data possession" (PDP) model to ensure the right files on untrusted stores. Their plan, outsource data auditing for RSA-based homomorphism tags, thus public audit ability is achieved. However, Ateniese et al. consider the case of dynamic data storage, and direct extension from their plan to the dynamic static data storage design and safety problems may suffer his later work in [2], Ateniese et al. propose a dynamic version of the former PDP plan. However, the system imposes on the number of queries and bound a priori totally does not support dynamic data operations, i.e., it only blocks very basic with limited functionality allows operations and block insertion is not supported. [20], Wang et al. Consider the scenario in which a distributed dynamic data storage, and proposed the challenge-response protocol to determine the accuracy of the data can both detect possible errors and. [2] likewise, they only consider partial support for dynamic data action. Juels et al. [10] describes a proof of "irretrievability" (sequence) model, where the spot-checking and error correcting code "right" and "data collection" service system files used for ensuring irretrievability. In particular, the "sentinels" for certain blocks

Proc. of the Intl. Conf. on Advances In Engineering And Technology - ICAET-2014

ISBN: 978-1-63248-028-6 doi: 10.15224/ 978-1-63248-028-6-01-110

irregular detection data are embedded in the file F, and F forward these particular blocks to protect encrypted positions. However, [2], such as reusing a client can perform a certain number of priorities, and the introduction of dynamic data update ”sentinels” recomputed realizing development.

They publicly verifiable based on homomorphism authenticators BLS signatures [4], the use made of the evidence can be collected in a small authenticator value, and the public has gained irretrievability. Still, the authors only consider static data files. Elway et al. [9] to capture dynamic provable data to explore the first constructions. They skip the rank-based authenticated lists using collected data files to support updates to provable [1] extend the PDP model scheme is essentially a PDP resolution POORI is the dynamic version. Updates, especially support for the block to insert Atenieses PDP model [1] “tags” to eliminate the computed index information and authenticated before the employment verification process first challenged or tagged blocks updated information To validate the data structure in the list. However, your planning efficiency remains unclear although current plans for different data storage integrity systems aim at providing, to support both public audit ability and data Dynamics problem fully addressed. How original data storage service to integrate these two important components in a safe and efficient design to achieve cloud computing remains an open challenging tasks in two basic solutions (i.e., MAC-based and signature-based YojanaAon)realizing data audit ability and ability to public audit and data in support of mobility faults discussed. Secondly, General Dynamics both proof of provable data possession and irretrievability (order) (PDP) model and overall system efficiency to discuss the impact of dynamic data operations on data. In particular, emphasize that while dynamic data updates can be performed efficiently in PDP models more efficient protocols need to be designed for the update of the encoded files in PoR models.

III. PROPOSED APPROACH FRAMEWORK AND DESIGN

A. Proposed Approach Framework and Design

Institutions proposed in the network client, cloud storage servers and third party auditor is a person or organization that is customer data files to store and maintain them depends on the cloud service provider. Cloud storage servers are lots of storage space and computational resources is maintained by the cloud service provider. Third-party auditor is reliable and the customer’s ability to audit data on demand.

As can be seen in Fig. 1, it’s clear that customers were provided by the cloud service provider cloud storage server stores your data. This model is two things they are) can delete the files in the data provider the cloud client. B) Cloud data providers data center could be hiding potential problems in keeping these assumptions. The mechanism proposed is designed into the system.

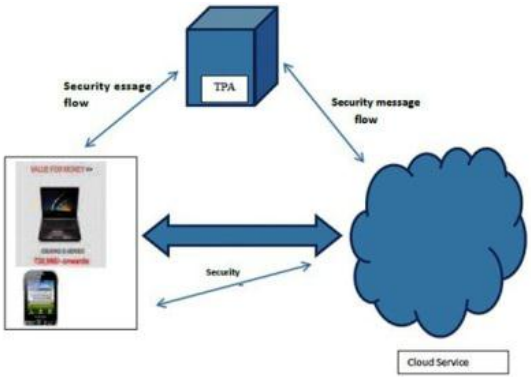

Fig. 1. Proposed Architecture

B. Proposed Work

In this paper a framework for seamless integration of these two components and a skilled construction exists in our Protocol designs. Our contributions can be summarized as follows:

1) I achieved what block verification data to cloud storage, public verifiability with a general offer of formal order model;
2) I especially block insertions, which are missing in most existing schemes for supporting fully dynamic data operations, build support for the proposed sequence of the function;
3) Our proposed building safety to prove and solid implementation and State-of-the-art through comparison with our plan to justify the performance of. Merkle hash tree.
4) classic building block tag authentication to achieve efficient data mobility by manipulating the evidence storage to improve existing models.
5) I, with our main result is a composite signature bilinear transform multiple auditing tasks a user can perform in settings where TPA, to expand the technology to figure out.
6) Comprehensive protection and performance analysis shows that the proposed plan is highly efficient and provably secure.

C. Approach

In cloud computing data storage for safety and clearly efficient to increase the scheme with dynamic data operations therefore, this dynamic case, where a variety of block-level performance updates, removal and storage accuracy assurance while maintaining data modifying file attached might want to consider is trivial and important way to support these operations All data for cloud server for downloading and full parity blocks as well as recalculate token validation.

- **Update Operation**

In cloud data storage, sometimes the user may need to modify some data block(s) stored in the cloud, from its current value fi to a new one, fi + fi. I refer this operation as data update.

- **Delete Operation**

Sometimes, after being stored in the cloud, some data blocks to be removed. Delete operation are considered a common one, which replaces zero or certain user all rights reserved data symbol data segment. From this perspective, the delete

ISBN: 978-1-63248-028-6 doi: 10.15224/ 978-1-63248-028-6-01-110

operation where the original data blocks with zero can replace or update the data block certain predetermined action, Is actually a special case.

- **Append Operation**

Is dynamic operating metrics, where 0 is unchanged blocks [8] indicating the blocks I need to change and 1 indicating construction performance? I have a cloud atmosphere where users, TPA and cloud servers are connected to each other. Accuracy of data in the public audit system, keyed, sagging, checked by proof and proof

General algorithms verifies. Auditing with random masking Homomorphism authenticator scheme Protection of privacy is used to achieve bi-linear composite signature techniques to obtain the batch audit is used remains constant data in the cloud, I clear dynamic data blocks with operations to enhance the system.

D. Algorithms

1) Algorithm for Data Integrity Verification

a) Start
b) TPA generates a random set
c) CSS computes root hash code based on the filename/blocks input
d) CSS computes the originally stored value
e) TPA decrypts the given content and compares with generated root hash
f) After verification, the TPA can determine whether the integrity is breached.
g) Stop

2) Algorithm for Updating and Deleting Data Present in CSS

a) Start
b) Client generates new Hash for tree then sends it to CSS
c) CSS updates F and computes new R
d) Client computes R
e) Client verifies signature. If it fails output is FALSE
f) Compute new R and verify the update
g) Stop

IV. SYSTEM DESIGN

A. Design Goals

Our design goals can be summarized as following:

1) Storage accuracy assurance public verification: anybody who basically demand for cloud servers; to verify the accuracy of the data stored on the ability to store the file, not just to allow customers

2) Dynamic data operations support: block-level data in data files on the same level while maintaining accuracy assurance to allow clients. Design as efficient so public verifiability and dynamic data to ensure seamless integration of operational support as possible;

3) Challenges: validation file blocks block less Verifier (for example, TPA) by both efficiency and safety concerns should be retrieved during verification process.

4) Stateless during long term data storage validation: Verifier-party audits at the State information between eliminate the need for maintenance.

5) The TPA by the multi-user support.

B. System Major Operations

1) Security Analysis

The proposed system public audit data blocks a file without the need to recover enables the ability to ”homomorphism authenticator technique [1] [3] is used to separate data from the metadata section inexcusable. The proposed is two authenticators and signatures such as BLS [3] RSA signature-based authenticator. This security mechanism and process of the Protocol Setup described here. Assure data integrity validation and default integration with dynamic operation is divided into the last phase, data modification, data. The insertion, deletion and data part one. Later on batch processing with multiple customer data is also discussed here.

2) Setup

In this step Eigen () method to generate public key and private key is applied to Siegen () processing and homomorphism authenticators and means along with metadata. Siegen method takes two arguments i.e. secret key file contents and file divided into blocks... then the signature is computed for each block for each block hash codes and to generate the next hash two nodes in a node merge The process has been all leaf node is found in the tree node until released. Root element is taken by the customer and sends the signal to the server and cloud storage.

3) Data Integrity Verification

Outsource data by either the client or the contents of the TPA can be verified by this challenging some server file and randomly block. Up challenge on cloud storage server file and computes the hash code and then blocks root hash code computation and originally stored along with the hash code signing. the TPA or client public key and private key to decrypt the content and root The hash code is given by the client’s root hash code to compare with the process that uses the following algorithm is specified.

4) Data Modification and Data Insertion

Data modifications are continually on cloud storage action. Meet new people with a specified block of replacing process. Revision process customer data can not affect the logic of the structure of a convergence and operations known as data. Data insertion to insert existing data is a process of the new record. Block specified locations or the new data file are inserted in f block.

5) Batch Auditing for Multi-client Data

Simultaneous access to support cloud servers. This means that the server is running various sessions of this parallel. It works for many concurrent user sessions that have auditing functionality. The proposed scheme based on provable data update and validation of client systems to get increased. Here is an important decision made “Bilearaggregate signature scheme” to use.

C. Design Considerations

The main design is consideration to achieve mobility and

Proc. of the Intl. Conf. on Advances In Engineering And Technology - ICAET-2014

ISBN: 978-1-63248-028-6 doi: 10.15224/ 978-1-63248-028-6-01-110

data audit ability. BLS-based solution and it can be used with RSA-based signature. BLS is 160 bits RSA solution where as 1024 bits. At least query and response is possible with BLS. RSA also supports variable block size MHT (Merkle hash tree). Solutions used to obtain. Other idea design data mobility. Data mobility to obtain PDP and order plans could be enhanced. However, security problems, as discussed previously can enter an opponent and execute actions with ease, H (name —I've changed the update operation). Insert f at any point in a file that has been saved to the server cloud storage may be denoting, while amending the existing blocks. Basic PDP system error correction capabilities bin constructions the device stores the static files the proposed objective of the

scheme is to reduce a block design and the stateless data verification does not require actual data TPA as important. real data into a hash value is only shown and secure turn keys validation rather than actual data is used to deliver yet another design idea is to support storage security when customers are stored in multiple cloud Server data, retrieve data and data needs a mechanism to manage. Data is on the number of places to withstand repeated defects. F the file is stored in multiple cloud storage servers.

V. BASIC SYSTEM IMPLEMENTATION

A. Hardware Requirements:

- Processor : Pentium IV 2.6 GHz
- Ram : 512 mb dd ram
- Monitor : 15 color
- Hard disk : 20 GB
- Keyboard : standard 102 keys

B. Software Requirements:

- Front End : JAVA
- Tools Used : Net beans
- Operating System : Windows XP/7

VI. RESULTS OF PRACTICAL WORK

Cloud Server

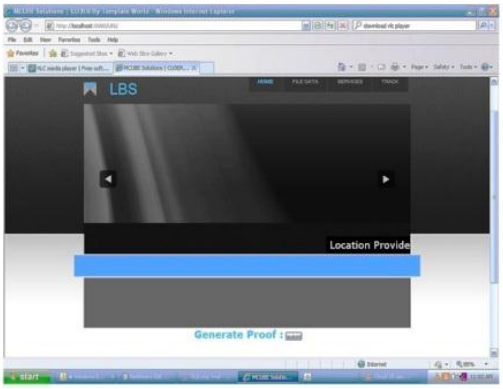

Fig. 2. Cloud Server

Start Service

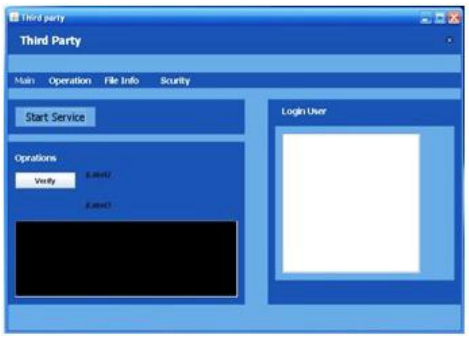

Fig. 3. Start Service

File Selection

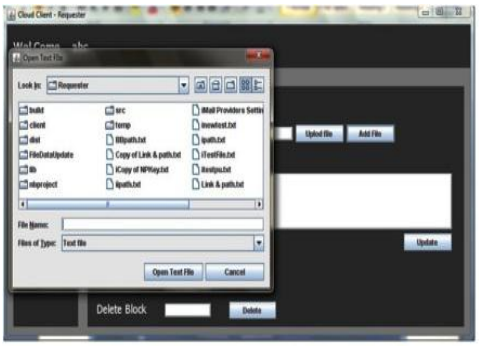

Fig. 4. File Selection

VI. CONCLUSION

Cloud data storage is to ensure the safety of an objective and independent approach to assessing the quality of service to enable a TPA. public audit ability TPA for integrity check tasks delegating while they are not independently reliable computing performance in a sustainable manner the necessary verifications of resources cannot commit to allow clients to enable a Verifying Protocol which concern more important dynamic data files may be able to adjust to the process for building the paper, remote data integrity check for simultaneous public audit ability in cloud computing and data mobility jobs asamanYa explored. The main goal to complete these two building design

ISBN: 978-1-63248-028-6 doi: 10.15224/ 978-1-63248-028-6-01-110

has been set as main target but efficiency. data mobility that are in effect to achieve storage block tag existing certificate authentication models classic Merkle hash trees enhanced through the creation of manipulation. Good handling to support multiple numbers of auditing functions, bilinear transform method of overall signature a multiple user settings, to give where the main result in a simultaneous way TPA is enabled to multiple auditing actions explored. Heavy security as well as performance analysis is proves that the proposed plan is efficient and to a large extent to be safe.

REFERENCES

[1] A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, M. Zaharia, "Above the clouds: A berkeley view of cloud computing," University of California, Berkeley, Tech. Rep, 2009.

[2] Cong Wang,Qian Wang,Kui Ren,Wenjing Lou (2009),"Ensuring Data Storage Security in Cloud Computing".

[3] Cong Wang,Qian Wang,Kui Ren,Wenjing Lou (2010),"Privacy Preserving Public Auditing for Data Storage Security in Cloud Computing". [4] A. L. Ferrara, M. Greeny, S. Hohenberger, M. Pedersen (2009), "Practical
short signature batch verification", in Proceedings of CT-RSA, volume 5473 of LNCS. Springer-Verlag, pp. 309324.

[5] H. Shacham, B. Waters (Dec 2008), "Compact proofs of retrievability", in Proc. of Asiacrypt 2008, vol. 5350, pp. 90107

[6] M.A.Shah, R.Swaminathan, M. Baker (2008), "Privacypreserving audit and extraction of digital contents", Cryptology ePrint Archive.

[7] M.A. Shah, R. Swaminathan, and M. Baker, "Privacy-PreservingAudit and Extraction of Digital Contents," Report 2008/186,Cryptology ePrint Archive, 2008.

[8] A. Oprea, M.K. Reiter, and K. Yang, "Space-Efficient Block Storage Integrity," Proc. 12th Ann. Network and Distributed System Security Symp. (NDSS 05), 2005.

[9] T. Schwarz and E.L. Miller, "Store, Forget, and Check: UsingAlgebraic Signatures to Check Remotely Administered Storage,"Proc. 26th IEEE Intl Conf. Distributed Computing Systems (ICDCS06), p. 12, 2006.

[10] Q. Wang, K. Ren, W. Lou, and Y. Zhang, "Dependable and Secure Sensor Data Storage with Dynamic Integrity Assurance," Proc.IEEE INFOCOM, pp. 954-962, Apr. 2009.

[11] G. Ateniese, R.D. Pietro, L.V. Mancini, and G. Tsudik, "Scalableand Efficient Provable Data Possession," Proc. Fourth Intl Conf.Security and Privacy in Comm. Networks (SecureComm 08), pp. 1-10,2008.

[12] C. Wang, Q. Wang, K. Ren, and W. Lou, "Ensuring Data StorageSecurity in Cloud Computing," Proc. 17th IntlWorkshop Quality of Service (IWQoS 09), 2009.

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

[14] K.D. Bowers, A. Juels, and A. Oprea, "Hail: A High-Availabilityand Integrity Layer for Cloud Storage," Proc. 16th ACM Conf.Computer and Comm. Security (CCS 09), pp. 187-198, 2009.

[15] D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggregate and Verifiably Encrypted Signatures from Bilinear Maps," Proc. 22ndIntl Conf. Theory and Applications of Cryptographic techniques (Eurocrypt 03), pp.

About Author (s):

Mr. Chadchankar Amarnath S.

ME in Sinhgad Institute of Technology, Lonavala, Pune University, Pune ,India