Volume 4, Issue 6, June 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Enhancing Security in Cloud Computing for Dynamic Data Storage

R.Brintha*
Research Scholar
Department of Computer Science
Pondicherry University, Karaikal
India

M.Dhanavalli
Department of Computer Science
Pondicherry University
Karaikal
India

S.Bhuvaneshwari
Head Department of Computer Science
Pondicherry University
Karaikal
India

Abstract*— This paper concentrate on cloud data storage security, which has dependably been an imperative part of quality of service. To guarantee the correctness of users 'data in the cloud, we propose a powerful and adaptable appropriated plan with two striking characteristics, contradicting to its ancestors. By using the homomorphic token with appropriated check of eradication coded data, our plan accomplishes the integration of storage correctness insurance and data error localization, i.e., the malicious server (s). Unlike most earlier works, the new plan further backings secure and productive element operations on data blocks, including: data update, delete and append. Broad security and performance analysis indicates that the proposed plan is profoundly proficient and versatile against Byzantine failure, malicious data modification attack, and considerably server conspiring attacks.

***Keywords*— Byzantine Failure, Dynamic Data Storage, homomorphic token, SAAS, Third Party Auditor,CSP.**

I. INTRODUCTION

Several trends are opening up the era of Cloud Computing, which is an Internet-based development and use of computer technology. The ever cheaper and more powerful processors, together with the software as a service (SaaS) computing architecture, are transforming data centers into pools of computing service on a huge scale. The increasing network bandwidth and reliable yet flexible network connections make it even possible that users can now subscribe high quality services from data and software that reside solely on remote data centers.

Moving information into the cloud offers incredible comfort to clients since they don't need to think about the complexities of immediate equipment administration. The pioneer of Cloud Computing sellers, Amazon Simple Storage Service (S3) and Amazon Elastic Compute Cloud (Ec2) are both well known samples. While these web based online administrations do give tremendous measures of storage room and adjustable figuring assets, this registering stage shift, nonetheless, is killing the obligation of nearby machines for data upkeep in the meantime. Therefore, clients are helpless before their cloud administration suppliers for the accessibility and honesty of their data. Late downtime of Amazon's S3 is such an illustration. From the viewpoint of information security, which has dependably been an imperative part of nature of administration, Cloud Computing inexorably postures new testing security dangers for number of reasons. Firstly, universal cryptographic primitives with the end goal of information security insurance cannot be specifically received because of the clients' misfortune control of information under Cloud Computing. In this way, confirmation of right information stockpiling in the cloud must be directed without express learning of the entire information. Recognizing different sorts of information for every client put away in the cloud and the interest of long haul consistent certification of their information wellbeing, the issue of confirming rightness of information stockpiling in the cloud gets much all the more testing. Besides, Cloud Computing is not only an outsider Data warehouse. The information put away in the cloud may be often upgraded by the clients, including insertion, erasure, change, annexing, reordering, and so forth.

To guarantee stockpiling accuracy under dynamic information upgrade is consequently of foremost criticalness. In any case, this element offer additionally makes universal uprightness protection strategies pointless and involves new results. Keep going not the slightest, the organization of Cloud Computing is controlled by server farms running in a concurrent, participated and circulated way. Singular client's information is needlessly put away in various physical areas to further lessen the information honesty dangers. In this manner, appropriated conventions for capacity accuracy affirmation will be of most essentialness in attaining a vigorous and secure cloud information stockpiling framework in this present reality. Notwithstanding, such vital region stays to be completely investigated in the writing

II. EXISTING SYSTEM

From the viewpoint of data security, which has dependably been an essential part of nature of administration, Cloud Computing inexorably postures new testing security dangers for number of reasons.

1 . Firstly, accepted cryptographic primitives with the end goal of data security insurance can not be straightforwardly embraced because of the clients' misfortune control of data under Cloud Computing. Thusly, check of right data stockpiling in the cloud must be directed without express learning of the entire data. Recognizing different sorts of data

for every client put away in the cloud and the interest of long haul constant confirmation of their data wellbeing, the issue of confirming accuracy of data stockpiling in the cloud gets considerably all the more testing.

2 . Besides, Cloud Computing is not only an outsider data warehouse. The data put away in the cloud may be oftentimes redesigned by the clients, including insertion, erasure, change, attaching, reordering, and so forth. To guarantee stockpiling rightness under dynamic data redesign is subsequently of vital essentialness.

These procedures, while could be suitable to guarantee the capacity accuracy without having clients having data, can not address all the security dangers in cloud data storage, since they are all concentrating on single server situation and the majority of them don't think about dynamic data operations. As an integral methodology, scientists have likewise proposed conveyed conventions for guaranteeing stockpiling accuracy crosswise over different servers or companions. Once more, none of these dispersed plans is mindful of element data operations. Therefore, their appropriateness in cloud data storage could be definitely restricted.

III. PROPOSED SYSTEM

In this paper, we propose a viable and adaptable dispersed plan with unequivocal element data backing to guarantee the effectiveness of clients' data in the cloud. We depend on eradication revising code in the document conveyance planning to give redundancies and certification the data dependability. This development radically lessens the communication and storage overhead as contrasted with the conventional replication-based record dispersion strategies. By using the homomorphic token with appropriated check of eradication coded data, our plan accomplishes the capacity effectiveness protection and also data slip limitation: at whatever point data defilement has been identified throughout the stockpiling rightness confirmation, our plan can just about assurance the concurrent restriction of data mistakes, i.e., the distinguishing proof of the getting out of hand server(s).

1. Compared to many of its predecessors, which only provide binary results about the storage state across the distributed servers, the challenge-response protocol in our work further provides the localization of data error.
2. Unlike most prior works for ensuring remote data integrity, the new scheme supports secure and efficient dynamic operations on data blocks, including: update, delete and append.
3. Extensive 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.

A. Main Module

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.In the server side, it checks the client name and its password for security process. If it is satisfied and then received the queries from the client and search the corresponding files in the database. Finally, find that file and send to the client. If the server finds the intruder means, it set the alternative Path to those intruder.

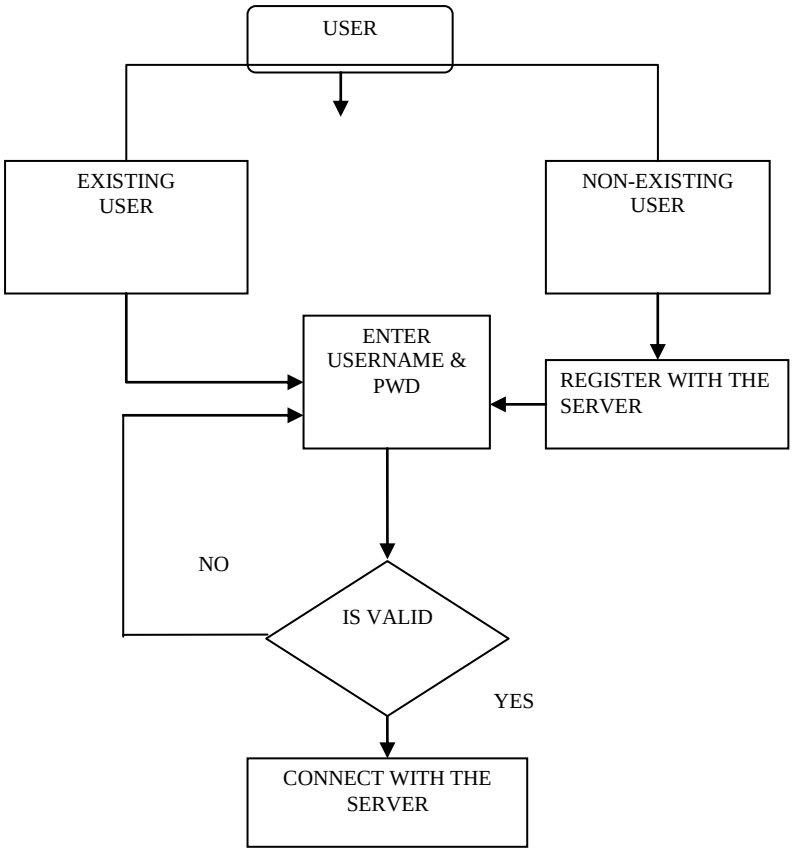


Fig 1: Architecture of the system

2) *System Module:* Representative network architecture for cloud data storage is illustrated in Figure 1. Three different network entities can be identified as follows:

• User:

Users, who have data to be stored in the cloud and rely on the cloud for data computation, consist of both individual consumers and organizations.

• Cloud Service Provider (CSP):

A CSP, who has significant resources and expertise in building and managing distributed cloud storage servers, owns and operates live Cloud Computing systems,.

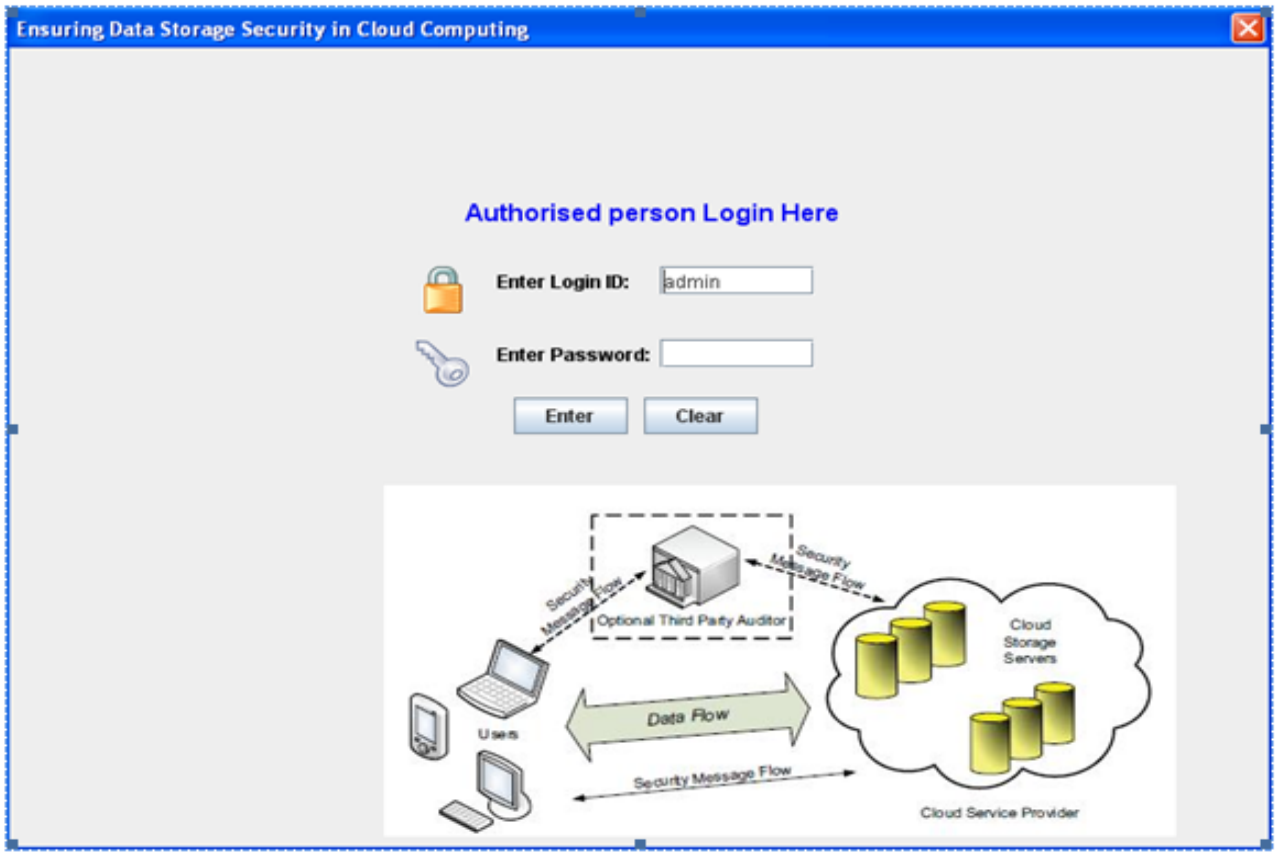
• Third Party Auditor (TPA):

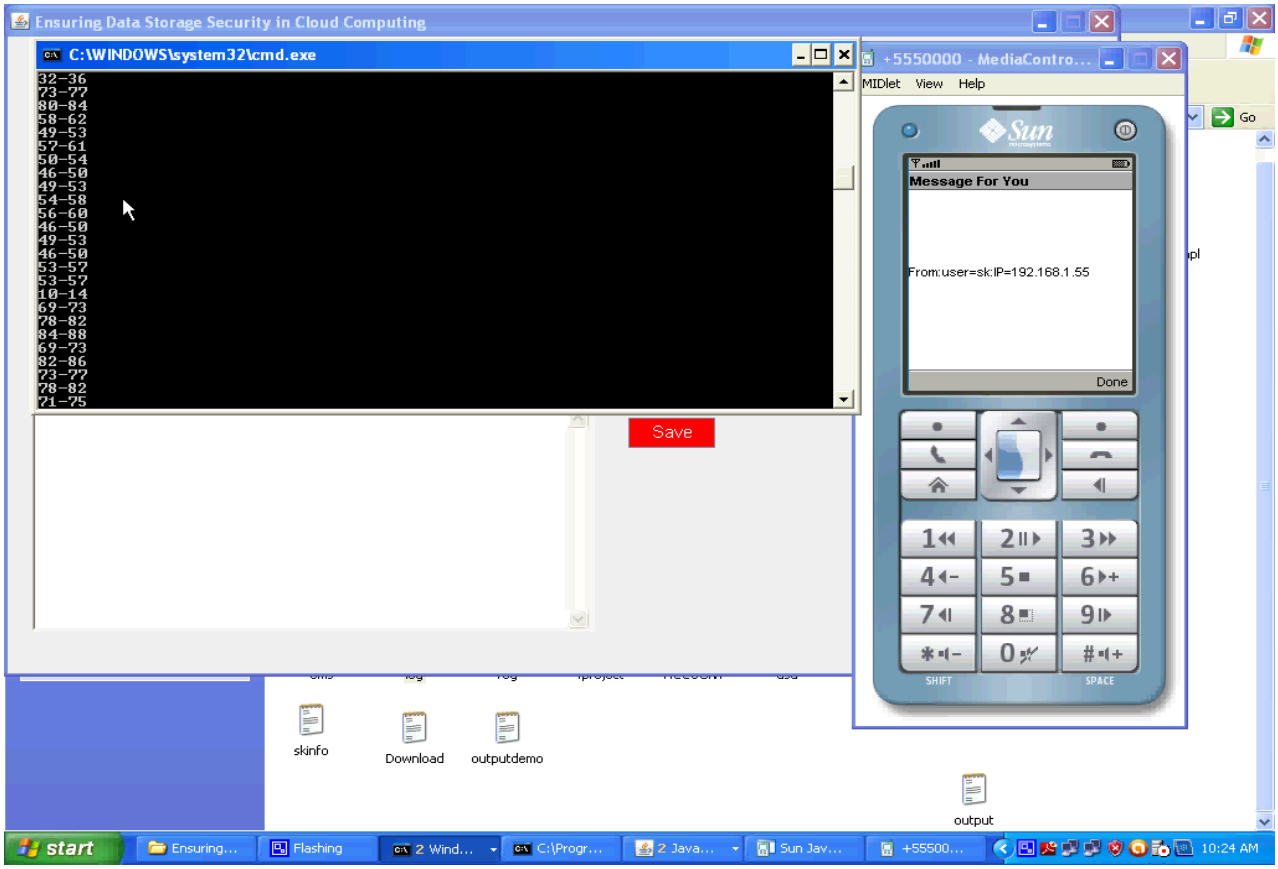
An optional TPA, who has expertise and capabilities that users may not have, is trusted to assess and expose risk of cloud storage services on behalf of the users upon request

3) *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 those 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. In our model, we assume that the point-to-point communication channels between each cloud server and the user is authenticated and reliable, which can be achieved in practice with little overhead.

4) *Cloud Authentication Server:* The Authentication Server (AS) functions as any AS would with a few additional behaviors 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.

Cloud Server Login

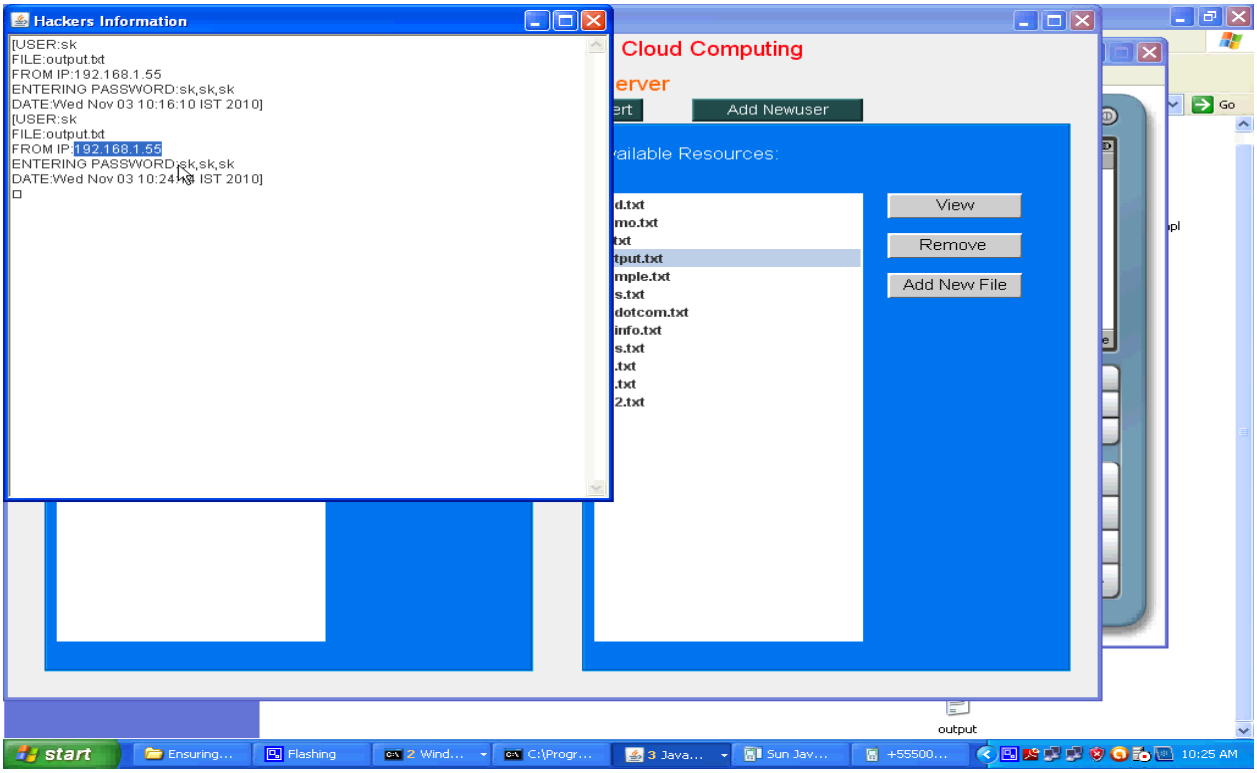




5) Unauthorized Data Modification and Corruption Module:

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.

IV. SCREEN SHOTS



V. CONCLUSIONS

The problem of data security is investigated 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. By utilizing the homomorphic token with distributed verification of erasure coded data, our scheme achieves the integration of storage correctness insurance and data error localization, i.e., at whatever point data defilement has been located throughout the stockpiling rightness check over the disseminated servers, we can just about insurance the concurrent distinguishing proof of the getting out of hand server(s). Through point by point security and execution examination, we demonstrate that our plan is exceptionally productive and flexible to Byzantine failure, malicious data change assault, and much server conniving ambushes

REFERENCES

[1] Amazon.com, "Amazon Web Services (AWS)," Online at http://aws. amazon.com, 2008.
[2] Athttp://www.pcworld.com/businesscenter/article/142549/amazo s 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] 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/.
[5] 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.
[6] 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.
[7] T. S. J. Schwarz and E. L. Miller, "Store, Forget, and Check: UsingAlgebraic Signatures to Check Remotely Administered Storage," Proc.

