Byzantine Fault Tolerance Based Security Challenges For The Privacy Preserving Public Cloud

D. GANESAN*, K.KARTHIKA**
* II ME, CSE,EASA College of Engineering and Technology, Anna University, Chennai.
** Assistant professor, CSE, EASA College of Engineering and Technology, Anna University, Chennai.

Abstract— Cloud computing make it possible to store large amounts of data. To monitoring User an entity whose data to be stores in the cloud and relies on the cloud for data storage and computation, server is an entity which manages by cloud service provider to provide data storage service and has significant storage space and computation resources and third party is 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. Our proposed work cloud computing architecture for analysis is cloud data storage a user stores his data through a CSP into set of cloud servers which are running in a simultaneous cooperated and distributed. Data redundancy can be employed with technique of erasure correcting code to further tolerate faults. Comparative study represents the security issues in cloud computing architecture that have the best efficiency or the best learning.

Index Terms— Cloud Computing, Cloud Computing Architecture, Intruder, Security Issues, SaaS, PaaS and IaaS.

I. INTRODUCTION

Cloud computing has a future information technology architecture for enterprises, on-demand self-service, ubiquitous network access, location independent resource pooling, rapid resource elasticity, usage-based pricing and transference of risk [2]. As a disruptive technology with profound implications, Cloud Computing is transforming the very nature of how businesses use information technology. One fundamental aspect of this paradigm shifting is that data is being centralized or outsourced to the Cloud. From users' perspective, including both individuals and IT enterprises, storing data remotely to the cloud in a flexible on-demand manner brings appealing benefits: relief of the burden for storage management, universal data access with independent geographical locations, and avoidance of capital expenditure on hardware, software, and personnel maintenances, etc [2]. While Cloud Computing makes these advantages more appealing than ever, it also brings new and challenging security threats towards users' outsourced data. Since cloud service providers (CSP) are separate administrative entities, data outsourcing is actually relinquishing user's ultimate control over the fate of their data. As a result, the correctness of the data in the cloud is being put at risk due to the following reasons. First of all, although the infrastructures under the cloud are much more powerful and reliable than personal computing devices, they are still facing the broad range of both internal and external threats for data integrity. Examples of outages and security breaches of noteworthy cloud services appear from time to time [4]. Secondly, there do exist various [6] motivations for CSP to behave unfaithfully towards the cloud users regarding the status of their outsourced data. For example, CSP might reclaim storage for monetary reasons by discarding data that has not been or is rarely accessed, or even hide data loss incidents so as to maintain a reputation [3]. In short, although outsourcing data to the cloud is economically attractive for long-term large-scale data storage, it does not immediately offer any guarantee on data integrity and availability. This problem, if not properly addressed, may impede the successful deployment of the cloud architecture. Moving data into the cloud offers great convenience to users since they don't have to care about the complexities of direct hardware management. The pioneer of Cloud Computing vendors, Amazon Simple Storage Service (S3) and Amazon Elastic Compute Cloud (EC2) [1] are both well-known examples. While these internet-based online services do provide huge amounts of storage space and customizable computing resources, this computing platform shift, however, is eliminating the responsibility of local machines for data maintenance at the same time. As a result, users are at the mercy of their cloud service providers for the availability and integrity of their data. Recent downtime of Amazon's S3 is such an example [2]. From the perspective of data security, which has always been an important aspect of quality of service, Cloud Computing inevitably 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. Therefore, verification of correct data storage in the cloud must be conducted without explicit knowledge of the whole data. Considering various kinds of data for each user stored in the cloud and the demand of long term continuous assurance of their data safety, the problem of verifying correctness of data storage in the cloud becomes even more challenging. Secondly, Cloud Computing is not just a third party data warehouse. The data stored in the cloud may be frequently updated by the users, include insertion, deletion, modification, appending, reordering, etc. To ensure storage correctness under dynamic data update is hence of paramount importance. However, this dynamic feature also makes traditional integrity

insurance techniques futile and entails new solutions. Last but not the least, the deployment of Cloud Computing is powered by data centers running in a simultaneous, cooperated and distributed manner. Individual user's data is redundantly stored in multiple physical locations to further reduce the data integrity threats. Therefore, distributed protocols for storage correctness assurance will be of most importance in achieving a robust and secure cloud data storage system in the real world. The assurances of cloud data integrity and availability and enforce the quality of cloud storage service, efficient methods that enable on-demand data correctness verification on behalf of cloud users have to be designed. However, the fact that users no longer have physical possession of data in the cloud prohibits the direct adoption of traditional cryptographic primitives for the purpose of data integrity protection. Hence, the verification of cloud storage correctness must be conducted without explicit knowledge of the whole data files. Meanwhile, cloud storage is not just a third party data warehouse. The data stored in the cloud may not only be accessed but also be frequently updated by the users, including insertion, deletion, modification, appending, etc. Thus, it is also imperative to support the integration of this dynamic feature into the cloud storage correctness assurance, which makes the system design even more challenging. Last but not the least, the deployment of Cloud Computing is powered by data centers running in a simultaneous, cooperated and distributed manner However, such important area remains in the survey.

II. LITERATURE REVIEW

A. Issues on Cloud Computing:

The survey of major cloud service providers to investigate the security mechanisms to overcome the security issues discussed in this paper. We consider ten major cloud service providers. These providers provide their services in all major areas of cloud computing, including SaaS, PaaS and IaaS. List shows the list of service providers that we studied in this survey. In order to analyze the complete state of art of security in cloud computing, the survey needs to be more exhaustive. However, due to the fact that the scope of our work is not just to explore the state of art but to look at the major factors that affect security in cloud computing. Therefore we have intentionally not considered other cloud service providers in this survey. In list 2, we present the results of the survey that depicts the current state of security mechanisms. Information given in table 2 is based on the information available online at the official websites of these providers.

- IaaS Service Provides is a Amazon EC2 Amazon S3 GoGrid
- PaaS Service Provides Google Application Engine Microsoft Azure Services, Elastic Map Reduce
- SaaS service provides Sales force Google Docs

Security Issues on Cloud Computing Password Recovery 90% are using standard methods like other common services while 10% are using sophisticated techniques. Encryption 40% are using standard SSL encryption while 20% are using encryption mechanism but at an extra cost 40% are using advance methods like HTTPS access Data Location 70% have their data centers located in more than one country while 10% are located at a single location 20% are not open about this issue. Cloud computing is a model for information and services using exiting methods, it uses the internet infrastructure to allow communication between client side and server side applications. Cloud clients service providers provides exist between that offers cloud platforms for their customers to use and create their own web services. When making decisions to adopt cloud services privacy or security has always been a major deal with these issues the cloud provider must build up sufficient controls to provide such level of security than the organization would have if the cloud were not used. The major security challenge is that the owner of the data has no control on their data processing. Due to involvement of many technologies including networks, databases, operating systems, resource scheduling, transaction management, concurrency control and memory management [3],various security issues arises in cloud computing. Top seven security threats to cloud computing discovered by "Cloud Security Alliance" (CSA) are [4]:

- Abuse and Nefarious Use of Cloud Computing
- Insecure Application Programming Interfaces
- Malicious Insiders.
- Shared Technology Vulnerabilities
- Data Loss / Leakage
- Account, Service & Traffic Hijacking.
- Unknown Risk Profile

B. Survey in Existing System

It described a formal "proof of retrievability" (POR) model for ensuring the remote data integrity. Their scheme combines spot-checking and error correcting code to ensure both possession and retrievability of files on archive service systems. Shacham et al. [16] built on this model and constructed a random linear function based homomorphism authenticator which enables unlimited number of challenges and requires less communication overhead due to its usage of relatively small size of BLS signature. Bowers et al. [17] proposed an improved framework for POR protocols that generalizes both Juels and Shacham's work. Later in their subsequent work, Bowers et al. [20] extended POR model to distributed systems. However, all these schemes are focusing on static data. The effectiveness of their schemes rests primarily on the preprocessing steps that the user conducts before outsourcing the data file F. Any change to the contents of F, even few bits, must propagate through the error-correcting code and the corresponding random shuffling process, thus introducing significant computation and communication complexity. Recently, Dodis et al. [19] gave theoretical studies on generalized framework for different variants of existing POR work. Ateniese et al. [10] defined the "provable data possession" (PDP) model for ensuring possession of file on untrusted storages. Their scheme utilized public key based homomorphism tags for auditing the data file. However, the pre- computation of the tags imposes heavy computation overhead that can be expensive for an entire file. In their subsequent work, Ateniese et al. [13] described a PDP scheme that uses only symmetric key based cryptography. This method has lower-

overhead than their previous scheme and allows for block updates, deletions and appends to the stored file, which has also been supported in our work. However, their scheme focuses on single server scenario and does not provide data availability guarantee against server failures, leaving both the distributed scenario and data error recovery issue unexplored. The incremental cryptography work done by Bellare et al. [33] also provides a set of cryptographic building blocks such as hash, MAC, and signature functions that may be employed for storage integrity verification while supporting dynamic operations on data. However, this branch of work falls into the traditional data integrity protection mechanism, where local copy of data has to be maintained for the verification. It is not yet clear how the work can be adapted to cloud storage scenario where users no longer have the data at local sites but still need to ensure the storage correctness efficiently in the cloud.

III. PROBLEM DEFINTION

Cloud computing architecture contains different entities user, server, third for cloud storage service architecture. User an entity whose data to be stores and relies on the cloud for storage, server is an entity which manages by cloud service provider to provide data storage service has significant storage space and computing resources and third party is an optional Third Party Auditor 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.

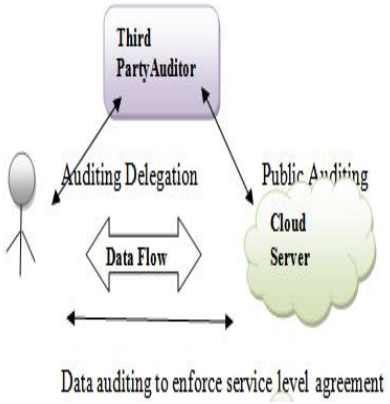

Fig 1.Data Auditing Diagram

Cloud data storage a user stores his data through a CSP into set of cloud servers which are running in a simultaneous cooperated and distributed. Data redundancy can be employed with technique of erasure correcting code to further tolerate faults or server crash as users data grows in size. For application purposes user interacts with the cloud servers via CSP to extract his data. As users no longer possess their data locally, it is of critical importance to ensure users that their data are being correctly stored and maintained. That is, users should be equipped with security means so that they can make continuous correctness assurance (to enforce cloud storage service-level agreement) 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 online, they can delegate the data auditing tasks to an optional trusted TPA of their respective choices. However, to securely introduce such a TPA, any possible leakage of user's outsourced data towards TPA through the auditing protocol should be prohibited.

A. Security Issues in Cloud Storage

Cloud service providers operate complex systems, have sophisticated processes and expert personnel for maintaining their systems which small enterprises may not have access, as result there are several direct and indirect security for cloud users. Data Centralization in a cloud environment the service provider takes care of storage issues and small business need not spend a lot of money on physical storage devices also cloud based storage providers a way to centralize the data faster and potentially cheaper, particular useful for small businesses which cannot spend additional money on security professionals to monitor the data. Incident Response like IaaS providers can put up a dedicated forensic server that can be used on demand basis. Whenever a security violation takes place the server can be brought online. Forensic image verification time in some cloud storage implementations expose a cryptographic check sum or hash Logging in a traditional computing paradigm by and large logging is often an afterthought, in general insufficient disk space is allocated that makes logging either nonexistent or minimal.

B. Aware of Security Threats in Cloud Computing

It was introduced by Cloud Security Alliance are given below A. Abuse of Cloud Computing: Abuse use of cloud computing is the top threat identified by the CSA. A simple example of this is the use of botnets to spread spam and malware. Attackers can infiltrate a public cloud, for example, and find a way to upload malware to thousands of computers and use the power of the cloud infrastructure to attack other machines.

Suggested remedies by the CSA to lessen this threat:

- Stricter initial registration and validation Processes.
- Enhanced credit card fraud monitoring and coordination.
- Comprehensive introspection of customer network traffic.
- Monitoring public blacklists for one's own Network blocks.

C. Programming Interfaces Insecurity

As software interfaces or APIs are what customers use to interact with cloud services, those must have extremely secure authentication, access control, encryption and activity monitoring mechanisms - especially when third parties start to build on them.

Suggested remedies by CSA to lessen this threat:

- Analyze the security model of cloud provider interfaces.
- Ensure strong authentication and access controls are implemented in concert with encrypted transmission.
- Understand the dependency chain associated with the API.

D. Malicious Intruders:

The malicious insider threat is one that gains in importance as many providers still don't reveal how they hire people, how they grant them access to assets or how they monitor them. Transparency is, in this case, vital to a secure cloud offering, along with compliance reporting and breach notification.

Suggested remedies by CSA to lessen this threat:

- Enforce strict supply chain management and conduct a comprehensive supplier assessment.
- Specify human resource requirements as part of legal contracts.
- Require transparency into overall information security and management practices, as well as compliance reporting.
- Determine security breach notification processes.

IV. COMPARATIVE STUDY

In contrast to traditional solutions, where the IT services are under proper physical, logical and personnel controls, 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 trustworthy. This unique attribute, however, poses many new security challenges which have not been well understood. No user data privacy Security risks towards the correctness of the data in cloud compare to existing environment on cloud data storage security, which has always been an important aspect of quality of service. To ensure the correctness of users' data in the cloud, we propose an effective and flexible distributed scheme with two salient features, opposing to its predecessors. 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., the identification of misbehaving server(s). Unlike most prior works, the new scheme further supports secure and efficient dynamic operations on data blocks, including: data update, delete and append and an effective and flexible distributed scheme with explicit dynamic data support to ensure the correctness of users' data in the cloud. Cloud Computing is not just a third party data warehouse. The data stored in the cloud may be frequently updated by the users, including insertion, deletion, modification, appending, etc. To ensure storage correctness under dynamic data update is hence of paramount importance. However, this dynamic feature also makes traditional integrity insurance techniques futile and entails new solutions.

A. Analysis Work System Model

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.

1. File Retrieval and Error Recovery

Since our layout of file matrix is systematic, the user can reconstruct the original file by downloading the data vectors from the first m servers, assuming that they return the correct response values. Notice that our verification scheme is based on random spot-checking, so the storage correctness assurance is a probabilistic one. We can guarantee the successful file retrieval with high probability. On the other hand, whenever the data corruption is detected, the comparison of pre-computed tokens and received response values can guarantee the identification of misbehaving server(s).

2. Third Party Auditing

In case the user does not have the time, feasibility or resources to perform the storage correctness verification, he can optionally delegate this task to an independent third party auditor, making the cloud storage publicly verifiable. However, as pointed out by the recent work, to securely introduce an effective TPA, the auditing process should bring in no new vulnerabilities towards user data privacy. Namely, TPA should not learn user's data content through the delegated data auditing.

3. Cloud Operations

Update Operation

In cloud data storage, sometimes the user may need to modify some data block(s) stored in the cloud, we refer this operation as data update. In other words, for all the unused tokens, the user needs to exclude every occurrence of the old data block and replace it with the new one.

Delete Operation

Sometimes, after being stored in the cloud, certain data blocks may need to be deleted. The delete operation we are considering is a general one, in which user replaces the data block with zero or some special reserved data symbol. From this point of view, the delete operation is actually a special case of the data update operation, where the original data blocks can be replaced with zeros or some predetermined special blocks.

Append Operation

In some cases, the user may want to increase the size of his stored data by adding blocks at the end of the data file, which we refer as data append. We anticipate that the most frequent append operation in cloud data storage is bulk append, in which the user needs to upload a large number of blocks (not a single block) at one time.

V. CONCLUSION

In this paper a general cloud computing architecture uses the find the secure data storage analyze for the objects in different data for security issues Cloud data storage a user stores his data through a CSP into set of cloud servers which are running in a simultaneous cooperated and distributed. Data redundancy can be employed with technique of erasure correcting code to further tolerate faults or server crash as users data grows in size. Our future direction is to implement a novel explanation mechanism for the problem of having high false intruders can also be resolved by one such approach that uses a high rate of accuracy in the case of any business method with human- understandable can also improve the efficiency for secure storage analyzing the complex dataset.

VI. REFERENCES

[1] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "Above the clouds: A Berkeley view of

cloud computing," University of California, Berkeley, Tech. Rep. UCB-EECS-2009-28, Feb 2009.

[2] 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.

[3] 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.

[4] M. Arrington, "Gmail disaster: Reports of mass email deletions," Online at http://www.techcrunch.com/2006/12/28/gmail-disaster reports-of-mass-email-deletions/, December 2006.

[5] J. Kincaid, "Media ax/The Linkup Closes Its Doors," Onlineat http://www.techcrunch.com/2008/07/10/ media-maxthelinkup-closes-its-doors/, July 2008.

[6] B. Krebs, "Payment Processor Breach May Be Largest Ever," Online at http://voices.washingtonpost.com/securityfix/2009/01/payment processor breach may b.html, Jan. 2009.

[7] Open Security Architecture http://www.opensecurityarchitecture.org/

[8] Steve Bennett Mans Bhuller, Robert Covington. Oracle White Paper in Enterprise Architecture – Architectural Strategies for Cloud Computing. August 2009. DOI= http://www.oracle.com/technology/architect/entarch/pdf/architectural_strategies_for_cloud_computing.pdf

[9] Security Guidance for Critical Areas of Focus in Cloud Computing,April2009.DOI=http://www.cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

[10] Towards Secure and Dependable Storage Services in Cloud Computing Cong Wand Student Memebet IEEE Qian Wang Kui Ran Ning Cao Student Members IEEE and Wenjing Lou Senior Member.

Author 1

Ganesan D, received B.E degree in 2011 from Anna University of Technology, Coimbatore, India. Currently pursuing M.E degree in Computer Science and Engineering in EASA college of Engineering and Technology. Coimbatore.

Author 2

Karthika K, Received B.E (CSE) degree in 2010 from Anna University Chennai India .Received M.E(CSE) degree in Karpagam University, India. Currently Working as Assistant Professor in EASA college of Engineering and Technology.coimbatore.