ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Using Multi Shares for Ensuring Privacy in Outsourced Cloud Storage

Billakurti Venkata Reddy
M.Tech Student,
Department of Computer Science and Engineering,
Amalapuram Institute of Management Sciences and College of Engineering.

Mohammed Alisha
Associate Professor & HOD,
Department of Computer Science and Engineering,
Amalapuram Institute of Management Sciences and College of Engineering.

ABSTRACT:

The major problem of cloud data storage is security. Many researchers have proposed their work or new algorithms to achieve security or to resolve this security problem. In this paper, we propose a new innovative idea for Privacy Preserving Public Auditing with watermarking for data Storage security in cloud computing. It supports data dynamics where the user can perform various operations on data like insert, update and delete as well as batch auditing where multiple user requests for storage correctness will be handled simultaneously which reduce communication and computing cost. Security is a considerable issue for this type of data centers. Security consist set of policies, applications and infrastructure. In this article we propose a model to overcome these issues; outsourced data are verified by trusted third party persons to ensure its integrity. This auditing was done because most of the data are outsourced. Next focused on security and performance analysis issues this was done by auditors simultaneously without over burden to the users.

Key Terms:

Cloud storage, privacy issues, third party auditors, integrity issues.

I. INTRODUCTION:

Cloud Computing is using hardware and software as computing resources to provide service through internet. Cloud computing provides various service models as platform as a service (PaaS), software as a service (SaaS), Infrastructure as a service (Iaas), storage as a service (STaaS), security as a service (SECaaS), Data as a service (DaaS) & many more. Out of this Paas, SaaS and IaaS are most popular. Cloud computing has four models as Public cloud: though which the service is available to all public use. Private cloud: Through which service is available to private enterprise or organization. Community Cloud: It allows us to share infrastructure among various organizations through which we can achieve security, compliance and jurisdiction. This can be managed internally or by a third-party and hosted internally or externally. Hybrid cloud: it is a combination of public and private cloud. Cloud computing has many advantages as: we can easily upload and download the data stored in the cloud without worrying about security. We can access the data from anywhere, any time on demand. Cost is low or pay per usage basis. Hardware and software resources are easily available without location independent. The major disadvantages of cloud computing is security.

A. Security Issues:

The security is a major issue in cloud computing. It is a sub domain of computer security, network security or else data security. The cloud computing security refers to a broad set of policies, technology & controls deployed to protect data, application & the associated infrastructure of cloud computing. Some security and privacy issues that need to be considered are as follows

1) Authentication: Only authorized user can access data in the cloud

2) Correctness of data: This is the way through which user will get the confirmation that the data stored in the cloud is secure

3) Availability: The cloud data should be easily available and accessible without any burden. The user should access the cloud data as if he is accessing local data

4) No storage Overhead and easy maintenance: User doesn't have to worry about the storage requirement & maintenance of the data on a cloud

5) No data Leakage: The user data stored on a cloud can accessed by only authorize the user or owner. So all the contents are accessible by only authorize the user.

6) No Data Loss: Provider may hide data loss on a cloud for the user to maintain their reputation.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

In cloud computing, cloud data storage contains two entities as cloud user and cloud service provider/ cloud server. Cloud user is a person who stores large amount of data on cloud server which is managed by the cloud service provider. User can upload their data on cloud without worrying about storage and maintenance. A cloud service provider will provide services to cloud user. The major issue in cloud data storage is to obtain correctness and integrity of data stored on the cloud. Cloud Service Provider (CSP) has to provide some form of mechanism through which user will get the confirmation that cloud data is secure or is stored as it is. No data loss or modification is done.Security in cloud computing can be addressed in many ways as authentication, integrity, confidentiality. Data integrity or data correctness is another security issue that needs to be considered. The proposed scheme [4] specifies that the data storage correctness can be achieved by using SMDS (Secure Model for cloud Data Storage). It specifies that the data storage correctness can be achieved in 2 ways as 1) without trusted third party 2) with trusted third party based on who does the verification.

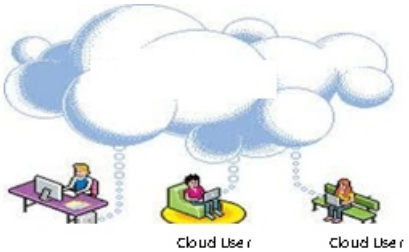


Fig 1: Cloud Architecture

It provides data confidentiality in two stages as 1) Data at rest 2) Data in transmission.
1)Data at rest: Symmetric key encryption technique (i.e. AES, TDES, and DES) are recommended which are secure but more time consuming.
2)Data in transmission: Secure Socket Layer (SSL) protocol is used for integrity verification. It uses a two different hash function such as Secure Hash Algorithm (SHA1) for digital signature and Message Digest (MD5) is a cryptographic hash function which is used to check the data integrity.

II.RELATED WORK:

The cloud data storage service contains 3 different entities as cloud user, Third party auditor & cloud server / cloud service provider. Cloud user is a person who stores large amount of data or files on a cloud server.

Cloud server is a place where we are storing cloud data and that data will be managed by the cloud service provider. Third party auditors will do the auditing on users request for storage correctness and integrity of data.The proposed system specifies that user can access the data on a cloud as if the local one without worrying about the integrity of the data. Hence, TPA is used to check the integrity of data. It supports privacy preserving public auditing. It checks the integrity of the data, storage correctness. It also supports data dynamics & batch auditing. The major benefits of storing data on a cloud is the relief of burden for storage management, universal data access with location independent & avoidance of capital expenditure on hardware, software & personal maintenance.

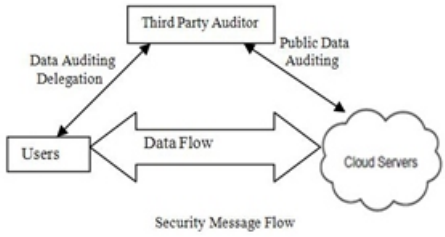


Fig 2: Architecture of Cloud Data storage service

In cloud, data is stored in a centralized form and managing this data and providing security is a difficult task. TPA can read the contents of data owner hence can modify. The reliability is increased as data is handled by TPA but data integrity is not achieved. It uses encryption technique to encrypt the contents of the file.TPA checks the integrity of the data stored on a cloud but if the TPA itself leaks the user's data. Hence the new concept comes as auditing with zero knowledge privacy where TPA will audit the users' data without seeing the contents. It uses public key based homomorphic linear authentication (HLA) [1], [2] which allows TPA to perform auditing without requesting for user data. It reduces communication & computation overhead. In this, HLA with random masking protocol is used which does not allow TPA to learn data content.

A. Goals:

•It allows TPA to audit users' data without knowing data content
•It supports batch auditing where multiple user requests for data auditing will be handled simultaneously.
•It provides security and increases performance through this system.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

B. Design Goals:

1) Public audit ability: Allows third party auditor to check data correctness without accessing local data.

2) Storage Correctness: The data stored on a cloud is as it. No data modification is done.

3) Privacy preserving: TPA can't read the users' data during the auditing phase.

4) Batch Auditing: Multiple users auditing request is handled simultaneously.

5) Light Weight: Less communication and computation overhead during the auditing phase.

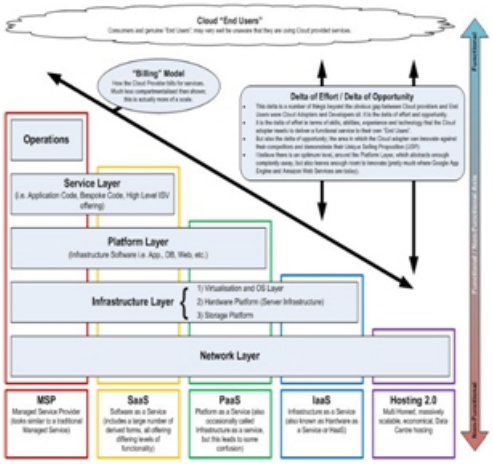
C. Batch Auditing:

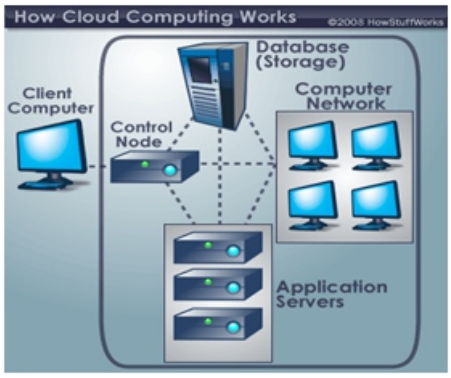
It also supports batch auditing through which efficiency is improved. It allows TPA to perform multiple auditing task simultaneously and it reduces communication and computation cost. Through this scheme, we can identify invalid response. It uses bilinear signature (BLS proposed by Boneh, Lynn and Shacham) to achieve batch auditing. System performance will be faster.

D. Data Dynamics:

It also supports data dynamics where user can frequently update the data stored on a cloud. It supports block level operation of insertion, deletion and modification. Author of [6] proposed scheme which supportSimultaneous public audability and data dynamics. It uses Merkle Hash Tree (MHT) which works only on encrypted data. It [11] uses MHT for block tag authentication.

Cloud architecture, the systems architecture of the software systems involved in the delivery of cloud computing, comprises hardware and software designed by a cloud architect who typically works for a cloud integrator. It typically involves multiple cloud other over application programming interfaces, usually web services.





Cloud architecture extends to the client, where web browsers and/or software applications access cloud applications.

Cloud storage architecture is loosely coupled, where metadata operations are centralized enabling the data nodes to scale into the hundreds, each independently delivering data to applications or user.

A typical cloud computing system:

Soon, there may be an alternative for executives like you. Instead of installing a suite of software for each computer, you'd only have to load one application. That application would allow workers to log into a Web-based service which hosts all the programs the user would need for his or her job. Remote machines owned by another company would run everything from e-mail to word processing to complex data analysis programs. It's called cloud computing, and it could change the entire computer industry. In a cloud computing system, there's a significant workload shift. Local computers no longer have to do all the heavy lifting when it comes to running applications.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

The network of computers that make up the cloud handles them instead. Hardware and software demands on the user's side decrease. The only thing the user's computer needs to be able to run is the cloud computing system's interface software, which can be as simple as a Web browser, and the cloud's network takes care of the rest. There's a good chance you've already used some form of cloud computing. If we have an e-mail account with a Web-based e-mail service like Hotmail, Yahoo! Mail or Gmail, then we've had some experience with cloud computing. Instead of running an e-mail program on our computer, we log in to a Web e-mail account remotely. The software and storage for our account doesn't exist on our computer – it's on the service's computer cloud.

» Easier for application vendors to reach new customers.
» Lowest cost way of delivering and supporting applications.
» Ability to use commodity server and storage hardware.
» Ability to drive down data center operational cots.
» Computer hardware (Dell, HP, IBM, Sun Microsystems)
» Storage (Sun Microsystems, EMC, IBM)
» Infrastructure (Cisco Systems)
» Computer software (3tera, Hadoop, IBM, RightScale)
» Operating systems (Solaris, AIX, Linux including Red Hat)

III. IMPLEMENTATION:
Proposed Approaches=:

1.Third Party Auditor
2.Cryptography
3.Cloud Computing
4.Privacy-preserving

1. Third Party Auditor:

In this module, Auditor views the all user data and verifying data .Auditor directly views all user data without key. Admin provided the permission to Auditor. After auditing data, store to the cloud.

2. Cryptography:

The art of protecting information by transforming it (encrypting it) into an unreadable format, called cipher text. Only those who possess a secret key can decipher (or decrypt) the message into plain text. Encrypted messages can sometimes be broken by cryptanalysis, also called code breaking, although modern cryptography techniques are virtually unbreakable.

3. Cloud Computing:

Cloud computing is the provision of dynamically scalable and often virtualized resources as a services over the internet Users need not have knowledge of, expertise in, or control over the technology infrastructure in the "cloud" that supports them. Cloud computing represents a major change in how we store information and run applications. Instead of hosting apps and data on an individual desktop computer, everything is hosted in the "cloud"—an assemblage of computers and servers accessed via the Internet.

Cloud computing exhibits the following key characteristics:

1. Agility improves with users' ability to re-provision technological infrastructure resources.
2. Multi tenancy enables sharing of resources and costs across a large pool of users thus allowing for:
3.Utilization and efficiency improvements for systems that are often only 10–20% utilized.
4. Reliability is improved if multiple redundant sites are used, which makes well-designed cloud computing suitable for business continuity and disaster recovery.
5. Performance is monitored and consistent and loosely coupled architectures are constructed using web services as the system interface.
6. Security could improve due to centralization of data, increased security-focused resources, etc., but concerns can persist about loss of control over certain sensitive data, and the lack of security for stored kernels. Security is often as good as or better than other traditional systems, in part because providers are able to devote resources to solving security issues that many customers cannot afford. However, the complexity of security is greatly increased when data is distributed over a wider area or greater number of devices and in multi-tenant systems that are being shared by unrelated users. In addition, user access to security audit logs may be difficult or impossible. Private cloud installations are in part motivated by users' desire to retain control over the infrastructure and avoid losing control of information security.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

7. Maintenance of cloud computing applications is easier, because they do not need to be installed on each user's computer and can be accessed from different places.

IV. SECRET SHARING ALGORITHMS:

Data stored in the cloud can be compromised or lost. So, we have to come up with a way to secure those files. We can encrypt them before storing them in the cloud, which sorts out the disclosure aspects. However, what if the data is lost due to some catastrophe befalling the cloud service provider? We could store it on more than one cloud service and encrypt it before we send it off. Each of them will have the same file. What if we use an insecure, easily guessable password to protect the 2012 45th Hawaii International Conference on System Sciences file, or the same one to protect all files? I have often thought that secret sharing algorithms could be employed to good effect in these circumstances instead.

RSA ALGORITHM:

RSA involves a public key and a private key. The public key can be known to everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted using the private key. The keys for the RSA algorithm are generated the following way:

1.Choose two distinct prime numbers p and q.
•For security purposes, the integers p and q should be chosen at random, and should be of similar bit-length.
2.Compute n = pq.
n is used as the modulus for both the public and private keys
3.Compute $\varphi(n) = (p-1)(q-1)$, where φ is Euler's totient function.
4.Choose an integer e such that $1 < e < \varphi(n)$ and greatest common divisor of $(e, \varphi(n)) = 1$; i.e., e and φ(n) are coprime. e is released as the public key exponent.
5.Determine d as: i.e., d is the multiplicative inverse of e mod φ(n).
Encryption
Encryption is the process of converting plain text into cipher text.
Decryption
Decryption is the process of converting cipher text into plain text.

V. ADVANCED ISSUES IN CLOUD COMPUTING SECURITY

In the previous section, we have discussed generic set of security concerns observed in public and hybrid clouds. We now turn our focus to some atypical cloud specific security issues. In particular, cloud does bring out a set of unique challenges like:

Abstraction:

Cloud provides an abstract set of service end-points. For a user, it is impossible to pin-point in which physical machine, storage partition (LUN), network port MAC address, switches etc. are actually involved. Thus, in event of security breach, it becomes difficult for a user to isolate a particular physical resource that has a threat or has been compromised.

Lack of execution controls:

The external cloud user does not have fine-gained control over remote execution environment. Hence the critical issues like memory management, I/O calls, access to external shared utilities and data are outside the purview of the user. Client would want to inspect the execution traces to ensure that illegal operations are not performed.

Third-party control of data:

In cloud, the storage infrastructure, and therefore, the data possession is also with the provider. So even if the cloud provider vouches for data integrity and confidentiality, the client may require verifiable proofs for the same.

Multi-party processing:

In multi-cloud scenario, one party may use part of the data which other party provides. In absence of strong encryption (as data is being processed), it becomes necessary for participating cloud computing parties to preserve privacy of respective data. Data breach is a big concern in cloud computing. A compromised server could significantly harm the users as well as cloud providers. A variety of information could be stolen. These include credit card and social security numbers, addresses, and personal messages. The U.S. now requires cloud providers to notify customers of breaches. Once notified, customers now have to worry about identify theft and fraud.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

While providers, have to deal with federal investigations, lawsuits, and bad reputation. Customer lawsuits and settlements have resulted in over $1 billion in losses to cloud providers. Cloud collaboration brings together new advances in cloud computing and collaboration that are becoming more and more necessary in firms operating in an increasingly globalised world. Cloud computing is a marketing term for technologies that provide software, data access, and storage services that do not require end-user knowledge of the physical location and configuration of the system that delivers the services. A parallel to this concept can be drawn with the electricity grid, where end-users consume power without needing to understand the component devices or infrastructure required to provide the service. Collaboration, in this case, refers to the ability of workers in a company to work together simultaneously on a particular task. In the past, most document collaboration would have to be completed face to face.

However, collaboration has become more complex, with the need to work with people all over the world in real time on a variety of different types of documents, using different devices. While growth in the collaboration sector is still growing rapidly, it has been noted that the uptake of cloud collaboration services has reached a point where it is less to do with the ability of current technology, and more to do with the reluctance of workers to collaborate in this way. A report by Erica Rugullies mapped out five reasons why workers are reluctant to collaborate more. These are: People resist sharing their knowledge. Users are most comfortable using e-mail as their primary electronic collaboration tool. People do not have incentive to change their behavior. Teams that want to or are selected to use the software do not have strong team leaders who push for more collaboration.

Senior management is not actively involved in or does not support the team collaboration initiative.As a result, many providers of cloud collaboration tools have created solutions to these problems. These include the integration of email alerts into collaboration software and the ability to see who is viewing the document at any time. All the tools a team could need are put into one piece of software so workers no longer have to rely on email based solutions. Recently, cloud collaboration has seen rapid evolution. In the past, cloud collaboration tools have been quite basic with very limited features. Newer packages are now much more document-centric in their approach to collaboration. More sophisticated tools allow users to “tag” specific areas of a document for comments which are delivered real time to those viewing the document. In some cases, the collaboration software can even be integrated into Microsoft Office, or allow users to set up video conferences. Furthermore, the trend now is for firms to employ a single software tool to solve all their collaboration needs, rather than having to rely on multiple different techniques. Single cloud collaboration providers are now replacing a complicated tangle of instant messengers, email and FTP.

Cloud collaboration today is promoted as a tool for collaboration internally between different departments within a firm, but also externally as a means for sharing documents with end-clients as receiving feedback. This makes cloud computing a very versatile tool for firms with many different applications in a business environment. The best cloud collaboration tools Use real-time commenting and messaging features to enhance speed of project delivery Leverage presence indicators to identify when others are active on documents owned by another person.

Allow users to set permissions and manage other users’ activity profiles. Allow users to set personal activity feeds and email alert profiles to keep abreast of latest activities per file or user. Allow users to collaborate and share files with users outside the company firewall.

VI.CONCLUSION:

The proposed system is suitable for providing integrity protection of customers important data. The proposed system supports data insertion, modification and deletion at the block level, and also supports public verifiability. The proposed system is proved to be secure against an untrusted server. It is also private against third party verifiers. Both theoretical analysis and experimental results demonstrate that the proposed system has very good efficiency in the aspects of communication, computation and storage costs.

Currently are still working on extending the protocol to support data level dynamics. The difficulty is that there is no clear mapping relationship between the data and the tags. In the current construction, data level dynamics can be supported by using block level dynamics. Whenever a piece of data is modified, the corresponding blocks and tags are updated. However, this can bring unnecessary computation and communication costs.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

REFERENCES:

[1]Privacy-Preserving Public Auditing for Secure Cloud Storage Cong Wang, Student Member, IEEE, Sherman S.-M. Chow, Qian Wang, Student Member, IEEE, Kui Ren, Member, IEEE, and Wenjing Lou, Member, IEEE IEEE TRANSACTIONS ON CLOUD COMPUTING YEAR 2013.

[2]Abraham, G. Chockler, I. Keidar and D. Malkhi, "Byzantine disk paxos: optimal resilience with Byzantine shared memory", Distributed Computing, 18(5), 2006, pp. 387-408.

[3]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.

[4] Kincaid, "MediaMax/TheLinkup Closes Its Doors," Online at http://www.techcrunch.com/2008/07/10/ mediamaxthelinkup-closes-its-doors/, July 2008.

[5] H. Abu-Libdeh, L. Princehouse and H.Weatherspoon, "RACS: a case for cloud storagediversity", SoCC'10:Proc. 1st ACM symposium onCloud computing, 2010, pp. 229-240.

[6]S. Wilson, "Appengine outage," Online at http://www.cio-weblog.com/50226711/appengine outage.php, June 2008.

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

[8] D. Agrawal, A. El Abbadi, F. Emekci and A.Metwally, "Database Management as a Service: Challenges and Opportunities", ICDE'09:Proc.25thIntl. Conf. on Data Engineering, 2009, pp. 1709-1716.

[9] M.A. AlZain and E. Pardede, "Using Multi Shares for Ensuring Privacy in Database-as-a-Service", 44th Hawaii Intl. Conf. on System Sciences (HICSS), 2011, pp. 1-9.

[10]A. Bessani, M. Correia, B. Quaresma, F. André and P. Sousa, "DepSky: dependable and secure storage in a cloud-of-clouds", EuroSys'11:Proc. 6thConf. On Computer systems, 2011, pp. 31-46.

[11] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson and D. Song, "Provable data possession at untrusted stores", Proc. 14th ACM Conf. on Computer and communications security,2007, pp. 598-609.

[12]K. Birman, G. Chockler and R. van Renesse,"Toward a cloud computing researchagenda", SIGACT News, 40, 2009, pp. 68-80.

[13]K.D. Bowers, A. Juels and A. Oprea, "HAIL: A high-availability and integrity layer for cloud storage", CCS'09: Proc. 16th ACM Conf. on Computer and communications security, 2009, pp.187-198.

[14]C. Cachin, R. Haas and M. Vukolic, "Dependable storage in the Intercloud", Research Report RZ, 3783, 2010.

[15]C. Cachin, I. Keidar and A. Shraer, "Trusting the cloud", ACM SIGACT News, 40, 2009, pp. 81-86.

Author Details:

Mohammed Alisha
is currently working as Associate Professor & Heading the department of Computer Science and Engineering, Amalapuram Institute of Management Sciences &College Of Engineering. He is a postgraduate in Computer Science and Engineering and had 9 years of teaching and research experience. His research interests include Spatial Data Mining, Compuer Networks, Web Mining and Data Warehousing.