ISSN.0975-5664 **www.ijcsee.org.uk** **Vol. 2 Issue 3**

Data Storage Security in Cloud Computing and Verification of Metadata by Encryption

#V.Sathiya Suntharam[1], Assoc.Prof,dept of CSE, E-Mail id : sathiya261@gmail.com
#DR.K.Venkateswara Reddy[2], Principal, E-Mail id : drkvreddy2k3@rediffmail.com
 # N .Puspalatha[3] ,Asso.professor, pushpalatha523@gmail.com
Marri Laxman Reddy Inst.of.Technology & Management,Dundigul,Hyderabad, A.P, INDIA

Abstract:-
Cloud computing is a nascent technology - and more than that, a new approach to management - that is starting to gain traction. From even the most basic outsourcing of machine builds for new application development, through the efficiency goals of using external platforms and applications delivered 'on-demand' as services, to grand notions of reengineering the enterprise data center as a private cloud, or even replacing it with a third-party cloud provider, cloud computing is present in a lot of today's grand IT dreams.Cloud Computing provides the way to share distributed resources and services that belong to different organizations or sites. Since Cloud Computing share distributed resources via network in the open environment thus it makes security problems. All types of users who require the secure transmission or storage of data in any kind of media or network. Since the data transmission on the internet or over any networks are vulnerable to the hackers attack. We are in great need of encrypting the data. I propose a method to build a trusted computing environment for Cloud Computing system by providing Secure cross platform in to Cloud Computing system. In this method some important security services including authentication, encryption and decryption and compression are provided in Cloud Computing system. The need for this software can be categorized in two categories: Encryption and Decryption, Compression.

Key words
Security, Credentials, Data Encryption, Compression,Authentication, Data Decryption, Decompression.

I. Introduction

Cloud computing is a general term for anything that involves delivering hosted services over the internet. These services are broadly divided into three categories: Infrastructure-as-a- Service (IaaS), Platform-as-a-Service (PaaS) and Software-asa- Service (SaaS). A cloud service has three distinct characteristics that differentiate it from traditional hosting. It is sold on demand, typically by the minute or the hour; it is elastic - a user can have as much or as little of a service as they want at any given time and the service is fully managed by the cloud service provider (the consumer needs nothing but a personal computer and Internet access).The advantage of cloud is cost savings. The prime disadvantage is security. Cloud computing is used by many software industries nowadays. Since the security is not provided in cloud, many companies adopt their unique security structure [3]. For eg) Amazon has its own security .structure. Introducing a new and uniform security structure for all types of cloud is the problem we are going to tackle in this paper. Since the data placed in the cloud is accessible to everyone, security is not guaranteed .I propose a method to build a trusted computing environment for Cloud Computing system by providing Secure cross platform in to Cloud Computing system. In this method some important security services including authentication, encryption and decryption and compression are provided in Cloud Computing system.

II. Characteristics

Cloud computing is cost-effective. Here, cost is greatly reduced as initial expense and recurring expenses are much lower than traditional computing. Maintenance cost is reduced as a third party maintains everything from running the cloud to storing data. Cloud is characterized by features such as platform, location and device independency, which make it easily adoptable for all sizes of businesses, in particular small and mid-sized [8]. However, owing to redundancy of computer system networks and storage system cloud may not be reliable

for data, but it scores well as far as security is concerned. In cloud computing, security is tremendously improved because of a superior technology security system, which is now easily available and affordable. Yet another important characteristic of cloud is scalability, which is achieved through server virtualization. Some of the most important five key characteristics are, [1].

A. On-demand Self Service

A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service's provider.

B. Broad Network Access

Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms.

C. Resource Pooling

The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or data center) [6]. Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.

D. Measured Service

Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service. Resource usage can be monitored, controlled, and reported providing transparency for both the provider and consumer of the utilized service [7].

E.Manageability

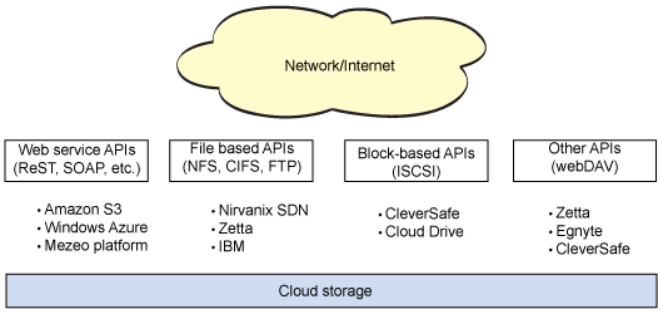
One key focus of cloud storage is cost. If a client can buy and manage storage locally compared to leasing it in the cloud, the cloud storage market disappears. But cost can be divided into two high-level categories: the cost of the physical storage ecosystem itself and the cost of managing it. The management cost is hidden but represents a long-term component of the overall cost. For this reason, cloud storage must be self-managing to a large extent. The ability to introduce new storage where the system automatically self-configures to accommodate it and the ability to find and self-heal in the presence of errors are critical. Concepts such as autonomic computing will have a key role in cloud storage architectures in the future.

F.Access method

One of the most striking differences between cloud storage and traditional storage is the means by which it's accessed (see FIG:1). Most providers implement multiple access methods, but Web service APIs are common. Many of the APIs are implemented based on REST principles, which imply an object-based scheme developed on top of HTTP (using HTTP as a transport). REST APIs are stateless and therefore simple and efficient to provide. Many cloud storage providers implement REST APIs, including Amazon Simple Storage Service (Amazon S3), Windows Azure™, and Mezeo Cloud Storage Platform. One problem with Web service APIs is that they require integration with an application to take advantage of the cloud storage. Therefore, common access methods are also used with cloud storage to provide immediate integration. For example, file-based protocols such as NFS/Common Internet File System (CIFS) or FTP are used, as are block-based protocols such as iSCSI. Cloud storage providers such as Nirvanix, Zetta, and Cleversafe provide these access methods.

Although the protocols mentioned above are the most common, other protocols are suitable for cloud storage. One of the most interesting is Web-based Distributed Authoring and Versioning (WebDAV). WebDAV is also based on HTTP and enables the Web as a readable and writable resource. Providers of WebDAV include Zetta and Cleversafe in addition to others.

Figure 1. Cloud storage access methods



You can also find solutions that support multi-protocol access. For example, IBM® Smart Business Storage Cloud enables both file-based (NFS and CIFS) and SAN-based protocols from the same storage-virtualization infrastructure.

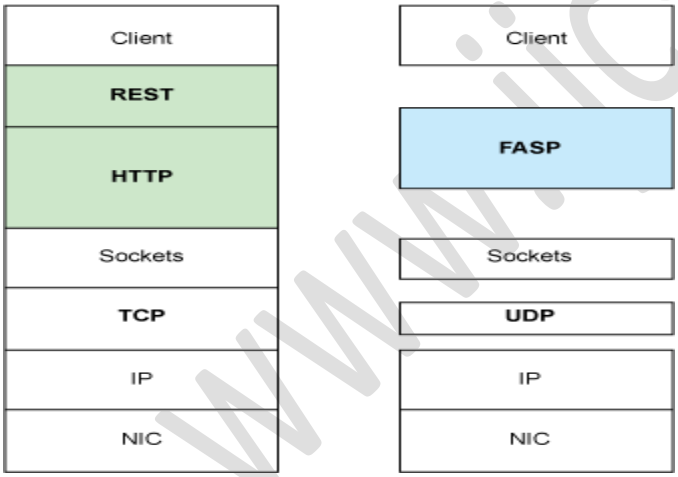
ISSN.0975-5664 **www.ijcsee.org.uk** **Vol. 2 Issue 3**

G.Performance

There are many aspects to performance, but the ability to move data between a user and a remote cloud storage provider represents the largest challenge to cloud storage. The problem, which is also the workhorse of the Internet, is TCP. TCP controls the flow of data based on packet acknowledgements from the peer endpoint. Packet loss, or late arrival, enables congestion control, which further limits performance to avoid more global networking issues. TCP is ideal for moving small amounts of data through the global Internet but is less suitable for larger data movement, with increasing round-trip time (RTT).

Amazon, through Aspera Software, solves this problem by removing TCP from the equation. A new protocol called the *Fast and Secure Protocol* (FASP™) was developed to accelerate bulk data movement in the face of large RTT and severe packet loss. The key is the use of the UDP, which is the parter transport protocol to TCP. UDP permits the host to manage congestion, pushing this aspect into the application layer protocol of FASP (see Fig.2)

Figure 2. The Fast and Secure Protocol from Aspera Software



Using standard (non-accelerated) NICs, FASP efficiently uses the bandwidth available to the application and removes the fundamental bottlenecks of conventional bulk data-transfer schemes.

H.Multi-tenancy

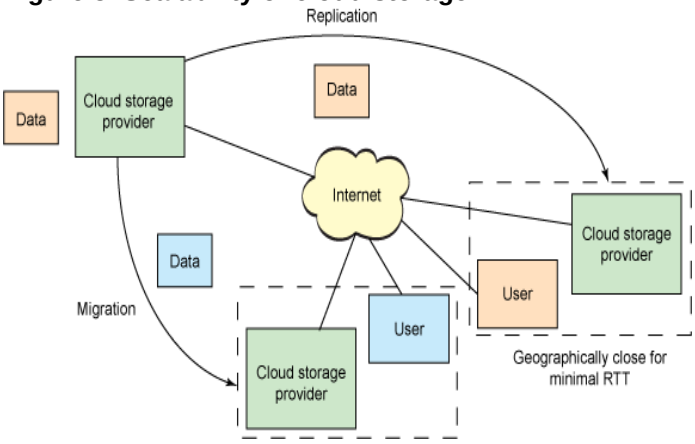
One key characteristic of cloud storage architectures is called *multi-tenancy.* This simply means that the storage is used by many users (or multiple "tenants"). Multi-tenancy applies to many layers of the cloud storage stack, from the application layer, where the storage namespace is segregated among users, to the storage layer, where physical storage can be segregated for particular users or classes of users. Multi-tenancy even applies to the networking infrastructure that connects users to storage to permit quality of service and carving bandwidth to a particular user.

I.Scalability

You can look at scalability in a number of ways, but it is the on-demand view of cloud storage that makes it most appealing. The ability to scale storage needs (both up and down) means improved cost for the user and increased complexity for the cloud storage provider.

Scalability must be provided not only for the storage itself (functionality scaling) but also the bandwidth to the storage (load scaling). Another key feature of cloud storage is geographic distribution of data (geographic scalability), allowing the data to be nearest the users over a set of cloud storage data centers (via migration). For read-only data, replication and distribution are also possible (as is done using content delivery networks). This is shown in Fig 3.

Figure 3. Scalability of cloud storage



Internally, a cloud storage infrastructure must be able to scale. Servers and storage must be capable of resizing without impact to users. As discussed in the manageability section, autonomic computing is a requirement for cloud storage architectures.

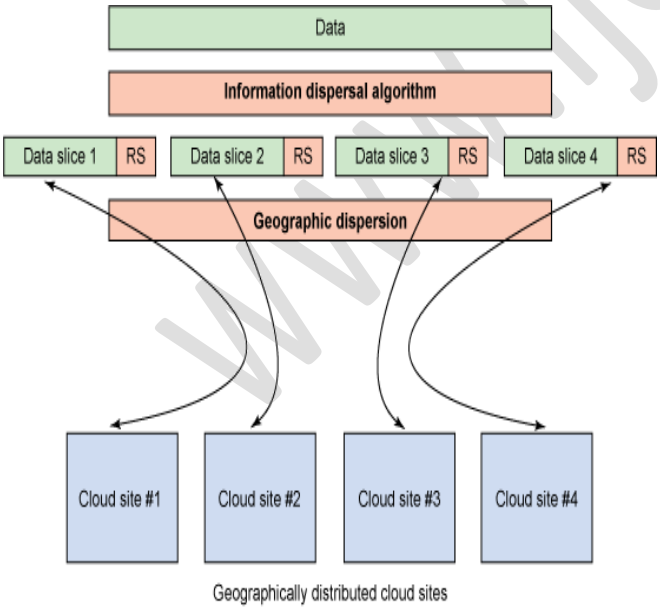
ISSN.0975-5664 **www.ijcsee.org.uk** **Vol. 2 Issue 3**

J.Availability

Once a cloud storage provider has a user's data, it must be able to provide that data back to the user upon request. Given network outages, user errors, and other circumstances, this can be difficult to provide in a reliable and deterministic way.

There are some interesting and novel schemes to address availability, such as information dispersal. Cleversafe, a company that provides private cloud storage (discussed later), uses the Information Dispersal Algorithm (IDA) to enable greater availability of data in the face of physical failures and network outages. IDA, which was first created for telecommunication systems by Michael Rabin, is an algorithm that allows data to be sliced with Reed-Solomon codes for purposes of data reconstruction in the face of missing data. Further, IDA allows you to configure the number of data slices, such that a given data object could be carved into four slices with one tolerated failure or 20 slices with eight tolerated failures. Similar to RAID, IDA permits the reconstruction of data from a subset of the original data, with some amount of overhead for error codes (dependent on the number of tolerated failures). This is shown in Fig 4.

Figure 4. Cleversafe's approach to extreme data availability



With the ability to slice data along with cauchy Reed-Solomon correction codes, the slices can then be distributed to geographically disparate sites for storage. For a number of slices (*p*) and a number of tolerated failures (*m*), the resulting overhead is *p*/(*p*-*m*). So, in the case of Fig.5 the overhead to the storage system for

p = 4 and *m* = 1 is 33%.

The downside of IDA is that it is processing intensive without hardware acceleration. Replication is another useful technique and is implemented by a variety of cloud storage providers. Although replication introduces a large amount of overhead (100%), it's simple and efficient to provide.

K.Control

A customer's ability to control and manage how his or her data is stored and the costs associated with it is important. Numerous cloud storage providers implement controls that give users greater control over their costs.

Amazon implements Reduced Redundancy Storage (RRS) to provide users with a means of minimizing overall storage costs. Data is replicated within the Amazon S3 infrastructure, but with RRS, the data is replicated fewer times with the possibility for data loss. This is ideal for data that can be recreated or that has copies that exist elsewhere. Nirvanix also provides policy-based replication to enable more granular control over how and where data is stored.

L.Efficiency

Storage efficiency is an important characteristic of cloud storage infrastructures, particularly with their focus on overall cost. The next section speaks to cost specifically, but this characteristic speaks more to the efficient use of the available resources over their cost.

To make a storage system more efficient, more data must be stored. A common solution is data reduction, whereby the source data is reduced to require less physical space. Two means to achieve this include *compression*—the reduction of data through encoding the data using a different representation—and *de-duplication*—the removal of any identical copies of data that may exist. Although both methods are useful, compression involves processing (re-encoding the data into and out of the infrastructure), where de-duplication involves calculating signatures of data to search for duplicates.

ISSN.0975-5664 **www.ijcsee.org.uk** **Vol. 2 Issue 3**

M.Cost

One of the most notable characteristics of cloud storage is the ability to reduce cost through its use. This includes the cost of purchasing storage, the cost of powering it, the cost of repairing it (when drives fail), as well as the cost of managing the storage. When viewing cloud storage from this perspective (including SLAs and increasing storage efficiency), cloud storage can be beneficial in certain use models.

An interesting peak inside a cloud storage solution is provided by a company called Backblaze). Backblaze set out to build inexpensive storage for a cloud storage offering. A Backblaze POD (shelf of storage) packs 67TB in a 4U enclosure for under US$8,000. This package consists of a 4U enclosure, a motherboard, 4GB of DRAM, four SATA controllers, 45 1.5TB SATA hard disks, and two power supplies. On the motherboard, Backblaze runs Linux® (with JFS as the file system) and GbE NICs as the front end using HTTPS and Apache Tomcat. Backblaze's software includes de-duplication, encryption, and RAID6 for data protection. Backblaze's description of their POD (which shows you in detail how to build your own) shows you the extent to which companies can cut the cost of storage, making cloud storage a viable and cost-efficient option.

N. Selection of Provider

A good service provider is the key to good service. So, it is imperative to select the right service provider. One must make sure that the provider is reliable, well-reputed for their customer service and should have a proven track record in IT- related ventures [12]. As cloud computing has taken hold, there are six major benefits that have become clear,

1. Anywhere/anytime access
It promises “universal” access to high-powered computing and storage resources for anyone with a network access device.

2. Collaboration among users
Cloud represents an environment in which users can develop software based services and from which they can deliver
them.

3. Storage as a universal service
The cloud represents a remote but scalable storage resource for users anywhere and everywhere.

4. Cost Benefits
The cloud promises to deliver computing power and services at a lower cost.

III.Literature Survey

A.Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing

The third party auditor (TPA), who has expertise and capabilities that cloud users do not have and is trusted to assess the cloud storage service security on behalf of the user upon request. Users rely on the CS for cloud data storage and maintenance [1]. They may also dynamically interact with the CS to access and update their stored data for various application purposes. The users may resort to TPA for ensuring the storage security of their outsourced data, while hoping to keep their data private from TPA. We consider the existence of a semi-trusted CS as does. Namely, in most of time it behaves properly and does not deviate from the prescribed protocol execution. However, during providing the cloud data storage based services, for their own benefits the CS might neglect to keep or deliberately delete rarely accessed data files which belong to ordinary cloud users. Moreover, the CS may decide to hide the data corruptions caused by server hacks or Byzantine failures to maintain reputation. We assume the TPA, who is in the business of auditing, is reliable and independent, and thus has no incentive to collude with either the CS or the users during the auditing process. TPA should be able to efficiently audit the cloud data storage without local copy of data and without bringing in additional on-line burden to cloud users [10].

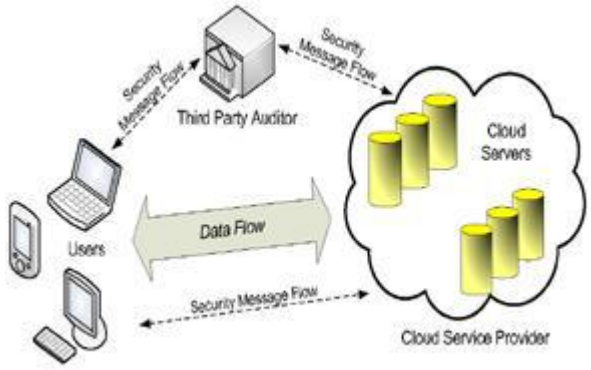


Fig. 5: The architecture of cloud data storage service
The Cloud Computing model of computing is a distributed application structure that partitions tasks or workloads between the providers of a resource or service, called Cloud servers, and service requesters, called clients. Often clients and servers.

ISSN.0975-5664 **www.ijcsee.org.uk** **Vol. 2 Issue 3**

B. Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing

The proposed scheme enables the data owner to delegate tasks of data file re-encryption and user secret key update to cloud servers without disclosing data contents or user access privilege information [2].We achieve this goal by exploiting
and uniquely combining techniques of attribute-based encryption(ABE), proxy re-encryption, and lazy reencryption.
The proposed scheme also has salient properties of user access privilege confidentiality and user secret key accountability and achieves fine graininess, scalability and data confidentiality for data access control in cloud computing. Extensive analysis shows that our proposed scheme is highly efficient and provably secures under existing security models.

1. Advantages

•Low initial capital investment
•Shorter start-up time for new services
•Lower maintenance and operation costs
•Higher utilization through virtualization
•Easier disaster recovery
In order to achieve secure, scalable and fine-grained access control on outsourced data in the cloud, the author utilize and uniquely combine the following three advanced cryptographic techniques:
• Key Policy Attribute-Based Encryption (KP-ABE).
•Proxy Re-Encryption (PRE)
•Lazy re-encryption

2. Module Description

(i). Key Policy Attribute-Based Encryption (KP-ABE)

KPABE is a public key cryptography primitive for one-to-many communications [2]. In KP-ABE, data are associated with attributes for each of which a public key component is defined. User secret key is defined to reflect the access structure so that the user is able to decrypt a cipher text if and only if the data attributes satisfy his access structure. A KP-ABE scheme is composed of four algorithms which can be defined as follows:
•Setup Attributes
•Encryption
•Secret key generation
•Decryption

(ii). Proxy Re-Encryption (PRE)

Proxy Re-Encryption (PRE) is a cryptographic primitive in which a semi-trusted proxy is able to convert a cipher text encrypted under Alice's public key into another cipher text that can be opened by Bob's private key without seeing the underlying plaintext [2].

(iii). Lazy re-encryption

The lazy re-encryption technique and allow Cloud Servers to aggregate computation tasks of multiple operations.
The operations such as [2].
• Update secret keys
• Update user attributes.

C. Toward Publicly Auditable Secure Cloud Data Storage Services

The authors propose that publicly auditable cloud data storage is able to help this nascent cloud economy become fully established. With public audit ability, a trusted entity with expertise and capabilities data owners do not possess can be delegated as an external audit party to assess the risk of outsourced data when needed. Such an auditing service not only helps save data owners' computation resources but also provides a transparent yet cost-effective method for data owners to gain trust in the cloud. The author describe approaches and system requirements that should be brought into consideration, and outline challenges that need to be resolved for such a publicly auditable secure cloud storage service to become a reality [3].

D. Online data storage using implicit security

The authors describe the use of a data partitioning scheme for implementing such security involving the roots of a Polynomial in finite field. The partitions are stored on randomly chosen servers on the network and they need to be retrieved to recreate the original data. Data reconstruction requires access to each server, login password and the knowledge of the servers on which the partitions are stored. This scheme may also be used for data security in sensor networks and internet voting protocols [4].
The authors have described an implicit security architecture suited for the application of online storage. In this scheme data is partitioned in such a way that each partition is implicitly secure and does not need to be encrypted. These partitions are stored on different servers on the network which are known only to the user. Reconstruction of the data requires access to each server and the knowledge as to which servers the data partitions are stored.
Several variations of this scheme are described, which include the implicit storage of encryption keys rather than the data, and where a subset of the partitions may be brought together to recreate the data.

E. Identity-Based Authentication for Cloud Computing

The authors propose an identity-based encryption (IBE) and decryption and identity-based signature (IBS) schemes for IBHMCC. based on the former IBE and IBS schemes, an identity- based authentication for cloud computing (IBACC) is proposed. The author presented an identity based authentication for cloud computing, based on the identitybased hierarchical model for cloud computing (IBHMCC) and corresponding encryption and signature schemes [5].

The authors proposed Identity-based Authentication Protocol. Identity-based Authentication Protocol contains sequence of steps. In step (1), the client C sends the server S a Client Hello message. The message contains a fresh random number C n, session identifier ID and C specification. In step (2), the server S responds with a ServerHello message which contains a new fresh random number S n, the session identifier ID and the cipher specification S specification The ciphertext is transmitted to as Server Key Exchange message. Then S generates a signature Sig S S [M] as the IdentityVerify message to forward to C.

Finally, The ServerHelloDone message means the step (2) is over. In step (3), C firstly verifies the signature S Sig S S with the help of S ID Being certificate-free, the authentication protocol aligned well with demands of cloud computing. Performance analysis indicated that the authentication protocol is more efficient and lightweight than SAP, especially the more lightweight user side.

F. Security Framework of Cloud Data Storage Based on Multi Agent System Architecture

The authors propose Multi- Agent System (MAS) techniques that can be beneficial in cloud computing platform to facilitate security of cloud data storage (CDS) among it [11]. MAS architecture offered eleven security attributes generated from four main security policies of correctness, integrity, confidentially and availability of users' data in the cloud.

G. Privacy-Preserving Public Auditing for Secure Cloud Storage

A Public Auditing Scheme [9]. Consists of four algorithms (KeyGen, SigGen, GenProof, VerifyProof)

1. KeyGen
key generation algorithm that is run by the user to setup the scheme

2. SigGen
used by the user to generate verification metadata, which may consist of MAC, signatures or other information used for
auditing

3. GenProof
run by the cloud server to generate a proof of data storage correctness

4. VerifyProof
run by the TPA to audit the proof from the cloud server. The author uses homomorphic authenticator technique for aggregate the data..Also uses a random mask technique achieved by a Pseudo Random Function (PRF)
(i). Homomorphic authenticator

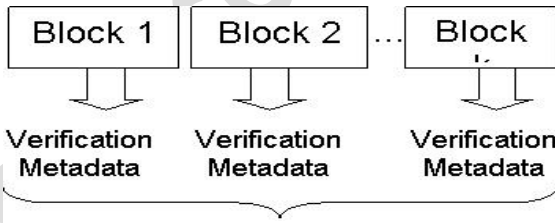


Fig. 6: A linear combination of data blocks can be verified by looking only at the aggregated authenticator [1]

IV. Existing System

To introduce an effective third party auditor (TPA) for privacy and security, the following fundamental requirements have to be met: TPA should be able to efficiently audit the cloud data storage without demanding the local copy of data, and introduce no additional on-line burden to the cloud user. The third party auditing process should bring in no new vulnerabilities towards user data privacy. They utilized and uniquely combined the public key based homomorphic authenticator with random masking to achieve the privacypreserving public cloud data auditing system, which meets all above requirements. This scheme is the first to support scalable and efficient public auditing in the Cloud Computing. In particular, this scheme achieves batch auditing where multiple delegated auditing tasks from different users can be performed simultaneously by the TPA. The security and performance is justified through concrete experiments and comparisons with the state-of-the art. In cloud service providers, for monetary reasons, reclaiming storage by discarding data that has not been or is rarely

ISSN.0975-5664 **www.ijcsee.org.uk** **Vol. 2 Issue 3**

accessed or even hiding data loss incidents so as to maintain a reputation.

In short, although outsourcing data into the cloud is economically attractive for the cost and complexity of long term large-scale data storage, it does not offer any guarantee on data integrity and availability. This problem, if not properly addressed, may impede the successful deployment of the cloud architecture. Another problem is that data stored in the cloud does not remain static [9].

V. Proposed System

The Proposed Network consists of three backup sites for recovery after disaster. The back up sites are located at remote location from the main server. If any one of the paths fails it uses alternate path working. The encrypted file will be create during back up sites and data's are compressed. The data will be decrypted during recovery operation. Proposed a cross platform integration model using secure communication via the Internet and the utilization of a key for security.

A. Data Backup Operation

Client send the data to the server which is known as Main Server. At the same time data is also back up to Multi Servers. In this method for data back up it involve with three Multi Server such as (SA 1(Server, Application), SA 2, SA 3,etc…).

B. Operation

Multi-server send the key id to our mail id.

C. Data Encryption and Compression

The data is to be encrypted and compressed in multi-server. In encryption and compression the data that has to stored in a cloud can not be stored in a text format due to security reasons so it must be transformed into an encrypted format. The data also has to be compressed for secure transmission. This method deals with the compression and encrypts the data before it is taken as back up in multi server. To encrypt the data's SHA Hash Algorithm is used for compression GZIP algorithm is used and for symmetric splitting of files SFSPL algorithm is implemented.

D. Authentication

Suppose the data is deleted in the client system. Then we authenticate the data through following procedures:
Find the key in our email id.
Give the file name and date in login form.

E. Data Decryption and Decompression

This method deals with the decompression and decrypting the data after it is taken as back up in multi server, the key is
automatically created by the server and it is send as email to the user. The data which taken as backup is stored in unrecognizable format, which cannot be open by any user. It can be readable only when it decrypt and decompress the data. If we give the key and data in the next login form, we will get the recovery of specified file.

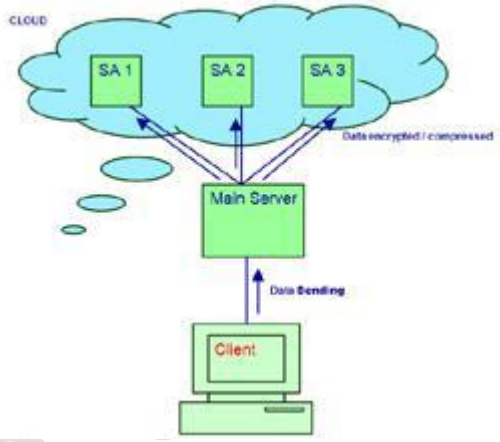


Fig.7: Data Backup

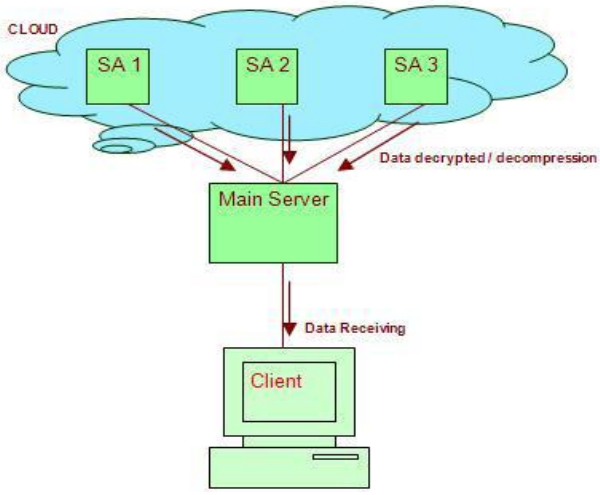


Fig.8: Data Recovery

VI. Conclusion

Authentication is necessary in Cloud Computing. After referred the papers I propose a new idea (ie) Secure Cross Platform Communication in a cloud.
Two major obstacles to this process of data sharing are providing a common storage space and secure access to the shared data. Cloud Databases are an emerging

type of non relational databases which do not follow relational algebra and are generally key-value oriented systems which are used for storing internet scale data and provide easy programmatic access. The main goal is to securely store and manage data that is not controlled by the owner of the data. The data are stored in cloud environment Cloud security here is solved by providing an credential for data in the cloud. These credential can be used to retrieve data from the cloud in a secure manner.

References

[1] Qian Wang, Cong Wang, Kui Ren, Wenjing Lou, Jin Li ,"Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing", IEEE Transactions On Parallel And Distributed Systems, Vol. 22, No. 5, 2011.

[2] Shucheng Yu., Cong Wang†, Kui Ren†, Wenjing Lou., "Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing", IEEE Communications Society for publication in the IEEE INFOCOM 2010.

[3] Qian Wang, Cong Wang, Kui Ren, Wenjing Lou, Jin Li, "Toward Publicly Auditable Secure Cloud Data Storage Services", IEEE Network, 2010.

[4] Abhishek Parakh, Subhash Kak, "Online data storage using implicit security", 2009.

[5] Hongwei Li, Yuanshun Dai, Ling Tian, Haomiao Yang, "Identity-Based Authentication for Cloud Computing", CloudCom 2009, LNCS 5931, pp. 157–166, 2009.

[6] Loud Security Alliance, "Security guidance for critical areas of focus in cloud computing", 9, [Online] Available : http:// www.cloudsecurityalliance.org.

[7] 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.

[8] Cong Wang, Qian Wang, Kui Ren, Wenjing Lou, "EnsuringData Storage Security in Cloud Computing", 2009.

[9] Cong Wang, Qian Wang, Kui Ren, Wenjing Lou, "PrivacyPreserving Public Auditing for Data Storage Security in Cloud Computing", 2010.

[10] H. Shacham, B. Waters, "Compact proofs of retrievability", in Proc. of ASIACRYPT 2008, vol. 5350, pp. 90–107,

[11] Amir Mohamed Talib, "Security Framework of Cloud Data Storage Based on Multi Agent System Architecture" ,Published by Canadian Center of Science and Education, Vol. 3, No. 4, 2010.

[12] Pardeep Kumar, Vivek Kumar Sehgal, Durg Singh Chauhan, P. K. Gupta, Manoj Diwakar, "ffective Ways of Secure, Private and Trusted Cloud Computing", IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 3, No. 2, 2011.

ABOUT AUTHORS:

1.V.SathiyaSuntharam presently working as **Associate professor** in the department of Computer Science and Engineering at Marri Laxman Reddy Institute of Technology and Management ,RR Dist,Hyderabad-43 of Andhra pradesh State ,INDIA**,** received his B.TECH. degree in Information Technology from Panimalar Engineering college , Chennai ,Madras university, INDIA, in 2004, the M.E. degree in Computer Science & Engineering from Anna University, Chennai-India in 2009, and his area of interest is data ware housing and data mining techniques, Computer networks ,Mobile computing and Cloud computing its applications.

2.K.Venkateswara Reddy Presently working as a **PRINCIPAL** at Marri Laxman Reddy Institute of Technology and Management ,RR Dist,Hyderabad-43 of Andhra pradesh State ,INDIA.He received Phd from Osmania university and he has 22 years of teaching Experience and his area of interest is data ware housing and data mining techniques, Computer networks , Mobile computing and Cloud computing its applications.