A SURVEY ON SERVICES AND SECURITY IN CLOUD COMPUTING

[1]Dr. Savita,[2]Satish Kumar

[1]Vocational Teacher,[2]Lecturer
[1]GGSSS Loharu,
[1]Haryana India

Abstract : **Cloud computing is a practical approach to experience direct cost benefits and it has the potential to transform a data center from a capital-intensive set up to a variable priced environment. Cloud computing has been envisioned as the next generation architecture of IT enterprise. Cloud computing moves the application software and data bases to the large data centers, where the management of the data and services may not be fully trustworthy. Cloud computing is a computing paradigm, where a large pool of systems are connected in private or public networks, to provide dynamically scalable infrastructure for application, data and file storage. With the advent of this technology, the cost of computation, application hosting, content storage and delivery is reduced significantly. This poses many new security challenges which have not been fully implemented. In this paper, we mainly focus on aspects for providing security for data storage in cloud, also architecture for data storage that are implemented by other service providers vendors in cloud, key points for proving security for data storage.**

Keywords: **cloud computing, cloud storage techniques, security techniques, architecture.**

I. Introduction

Cloud Computing provides us a means by which we can access the applications as utilities, over the internet. It allows us to create, configure, and customize the business applications online. Several trends are opening up the era of Cloud Computing [9], which is an Internet-based development and use of computer technology. Cloud Computing refers to manipulating, configuring, and accessing the applications online. It offers online data storage, infrastructure and application. The ever cheaper and more powerful processors, together with the software as a service (SaaS)[8] 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 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)[4] and Amazon Elastic Compute Cloud (EC2)[4] are both well-known examples. Recent downtime of Amazon's S3[4] is such an example. Benefits of Cloud storage: No need to invest any capital on storage devices, No need for technical expert to maintain the storage, backup, replication and importantly disaster management, allowing others to access your data will result with collaborative working style instead of individual work.

II. Services in cloud computing

A. SaaS:

Cloud consumers release their applications in a hosting environment, which can be accessed through networks from various clients (e.g. Web browser, PDA, etc.) by application users. Software as a Service (SaaS)[8] are probably the most popular form of cloud computing and are easy to use. SaaS uses the Web to deliver applications that are managed by a third-party vendor and whose interface is accessed on the clients' side. Most SaaS applications can be run directly from a Web browser, without any downloads or installations required. SaaS eliminates the need to install and run applications on individual computers. Cloud consumers do not have control over the cloud infrastructure that often employs multi-tenancy system architecture, namely, different cloud consumers' applications are organized in a single logical environment in the SaaS cloud to achieve economies of scale and optimization in terms of speed, security, availability, disaster recovery and maintenance. Applications: runtime, data, middleware, O/S, virtualization, servers, storage, and networking. Examples for SaaS are Gmail , Google Docs, Google Apps, Microsoft Office 365 , Google+ , face book , yahoo.

B. PaaS:

PaaS is a development platform supporting the full "Software Lifecycle" which allows cloud consumers to develop cloud services and applications (e.g. SaaS) directly on the PaaS cloud. Platform as a Service (PaaS)[8] deliver computational resources through a platform. What developers gain with PaaS is a framework they can build upon to develop or customize applications.PaaS makes the development, testing, and deployment of applications quick, simple, and cost-effective, eliminating the need to buy the underlying layers of hardware and software. This requires PaaS, in addition to supporting application hosting environment, to possess development infrastructure including programming environment, tools, configuration management, and so forth. With

PaaS, vendors still manage runtime, middleware, O/S, virtualization, servers, storage, and networking, but users manage applications and data. Examples for PaaS are AWS Elastic Beanstalk, Windows Azure, Heroku, Force.com and Google App Engine.

C. IaaS

Infrastructure as a Service (IaaS)[8] delivers computer infrastructure (such as a platform virtualization environment), storage, and networking. Cloud consumers directly use IT infrastructures (processing, storage, networks and other fundamental computing resources) provided in the IaaS cloud. Notice that this strategy is different from the multi-tenancy model, which aims to transform the application software architecture so that multiple instances (from multiple cloud consumers) can run on a single application (i.e. the same logic machine).Basically, in exchange for a rental fee, a third party allows you to install a virtual server on their IT infrastructure. Compared to SaaS,PaaS and IaaS users are responsible for managing more: applications, data, runtime, middleware, and O/S. Vendors still manage virtualization, servers, hard drives, storage, and networking. What users gain with IaaS is infrastructure on top of which they can install any required plateforms. Users are responsible for updating these if new versions are released. Examples for IaaS are Amazon EC2, Windows Azure, Rack space, Google Compute Engine.

D. Data as a Service (DaaS) The delivery of virtualized storage on demand becomes a separate Cloud service - data storage service. Notice that DaaS could be seen as a special type IaaS. The motivation is that on-premise enterprise database systems are often tied in a prohibitive upfront cost in dedicated server, software license, post-delivery services and in-house IT maintenance. DaaS allows consumers to pay for what they are actually using rather than the site license for the entire database. In addition to traditional storage interfaces such as RDBMS and file system, Examples of this kind of DaaS include Amazon S3, Google BigTable, and Apache HBase, etc.

III. Cloud Storage Models

There are models for cloud storage that allow users to maintain control over their data. Cloud storage [2] has evolved into three categories, one of which permits the merging of two categories for a cost-efficient and secure option. Public cloud storage providers, which present storage infrastructure as a leasable commodity (both in terms of long-term or short-term storage and the networking bandwidth used within the infrastructure). Finally, hybrid cloud storage permits the two models to merge, allowing policies to define which data must be maintained privately and which can be secured within public clouds (see Figure 1).

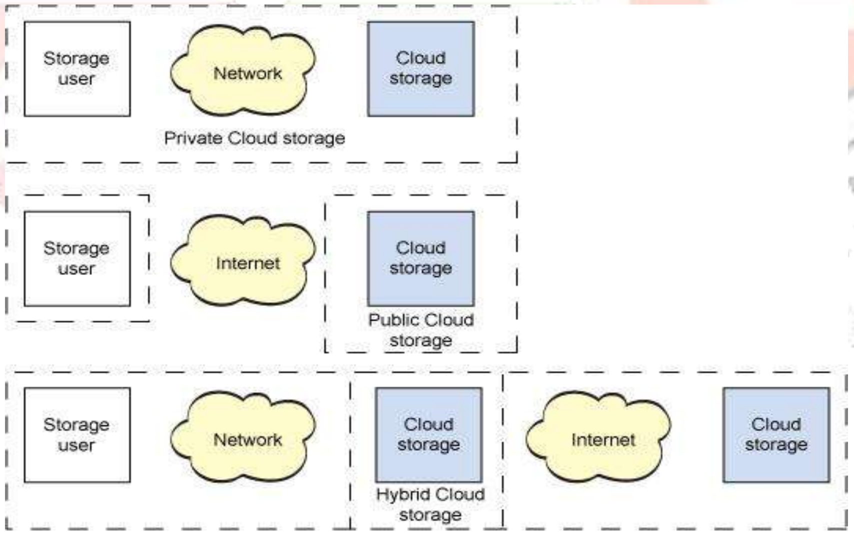

Fig 1. Cloud storage models

The cloud models are shown graphically in Figure 1. Examples of public cloud storage providers include Amazon (which offers storage as a service). Examples of private cloud storage providers include IBM[1], Para scale, and Clever safe (which build software and/or hardware for internal clouds). Finally, hybrid cloud providers include Egnyte, among others.

IV. Data Storage Security techniques in cloud computing

Various existing techniques [2] have been discussed in this paper. Cloud storage is regarded as a system of disseminated data centers that generally Utilizes virtualization technology and supplies interface for data storage.

- *Identify –Based Authentication*
  An identify based encryption (IBE) and decryption and identity based signature IBS schemes for

IBHMCC.Resourcesand services are distributed across numerous consumer. So there is a chance of various security risks. Therefore authentication of users as well as services is an important requirement for cloud security. When SSH Authentication protocol (SAP) was employed to cloud, it becomes very complex. n step (1) the client C sends the servers a client Hello message. The message contains a fresh random number Cnsession identifier ID and c specification. In step (2) the server S responds with a server Hello message which contains new fresh random number Sn.

- *Implicit Storage Security to Data in Online*
  Providing implicit storage security to data in online is more beneficial in a cloud computing. The use of a data partitioning scheme is for implementing such security involving the roots of a polynomial in finite field. In this scheme data is partitioned in such way that each portion is implicitly secure and does not to be encrypted. Several versions of this scheme are described, which include the implicit storage of encryption keys rather than the data and where a subset of the partition may be brought together to recreate the data.

- *Efficient Third Party Auditing (TPA)*
  Cloud consumers save data in cloud server so that security as well as data storage correctness is primary concern. To support third party auditing where user safely delegate in integrity checking tasks to third party auditors(TPA)[2] this scheme can almost guarantee the simultaneous localization of data error(i.e. the identification of misbehaving servers). A novel and homogeneous structure is introduced to provide security to different cloud types. To achieve data storage security, BLS (Bonch-Lynn-Sachems) algorithm is used to signing the data blocks before outsourcing data into cloud. Reed Solomon technique is used for error correction and to ensure data storage correction.

- *Public Auditing with Complete Data Dynamic Support*
  Verification of data integrity at unreliable servers is the major concern in cloud storage with public audit ability trusted entity with expertise and capabilities data owners do not posses can be delegated as an external audit party to access the risk of outsourced data when needed. To accomplish, dynamic data support, the existent proof read of PDF (or) POR scheme is improved by spoofing the basic Markel Hash tree (MHT).

- *Effective and Secure Storage Protocol*
  Current trend is users outsourcing data into service provider who have enough area for storage with lower storage cost. A secure and efficient storage protocol is proposed that guarantees the data storage confidentiality and integrity. Challenge response protocol is protocol is credential so that it will not exposes the contents of the data to outsiders. Data dynamic operations are also used keep the same security assurance and also provide relief to users from the difficult of data leakage and corruptions problems.

- *Secure and Dependable Storage Service*
  Storage service of permits consumers to the data in cloud as well as allowed to utilize the available well qualified application with no worry data storage maintained. The proposed a flexible distributed storage integrity auditing mechanism, utilizing the homomorphism token and distributed coded-data. The proposed design further support secure and efficient dynamic operation on outsource data including block modification, deletion and append.

- *Optimal cloud storage systems*
  Cloud data storage which requires no effort is acquiring more popularity for individual, enterprise and institutions data backup and synchronization. At its core, the architecture consists of these components- a data processor (DP) that processes data before it is sent to the cloud a data verifier (DV) that checks whether the data in the cloud has been tampers with, and a token generator (TG)[2] that generator token which enables the cloud storage providers to retrieve segments of consumer data.

- *Process of access and store small files with storage*
  To support services extensively, Hadoop distributed file system server reasons are examined for small file trouble of native Hadoop distributed file system. Burden on Nane Node of HADOOP distributed file system is enforced by large amount of small files, for data placement correction are not considered prefetching mechanism is not also presented. In order to overcome these small size problems, proposed an approach that these small size problem, proposed an approach. That improves the small file efficiency on Hadoop distributed file system, in a large cluster, thousands of servers both host directly attached storage and execute user application task.

- *Way of Dynamically Store Data in Cloud*
  Data storage is cloud may not be completely trustable because the clients did not have local copy of data stored in cloud. To address these issues proposed a new protocol system using the data reading protocol algorithm to check the data integrity services providers help the clients to check the data security by the proposed effective automatic data reading algorithm. A flexible distributed storage integrity auditing mechanism (FDSIAM), these mechanisms utilizes the homomorphism tokens, blocking erasure and unblocking factors and distributed erasure coded data.

- *Storage Security of Data*
  The data is secured in server based on user's choice of security method so that data is given high secure priority resources are being shared across server trouble to data security in cloud. The proposed effective and flexible distribution scheme two-way handshakes based on token management by utilizing the homomorphism token with distributed verification of erasure coded data, our scheme achieves the integration of storage correctness insurance and data error location (i.e.) the identification of misbehaving server.

- *File storage security management*
  To assure the security of stored data in cloud, presented a system which utilizes distributed scheme. Proposed system consists of a master server and a set of slave server. These are not direct commutation link between clients and slave servers in the proposed model. Clients file is stored in the form of tokens on main server and files were chunked on slave server for file recovery.

V. **Cloud Storage Architecture**

Cloud storage architectures [3] are primarily about delivery of storage on demand in a highly scalable and multi-tenant way. Generically (see Figure 2), cloud storage architectures consist of a front end that exports an API to access the storage. In traditional storage systems, this API is the SCSI protocol; but in the cloud, these protocols are evolving. There, you can find Web service front ends, file-based front ends, and even more traditional front ends (such as Internet SCSI, or iSCSI). This layer implements a variety of features, such as replication and data reduction, over the traditional data-placement algorithms (with consideration for geographic placement).

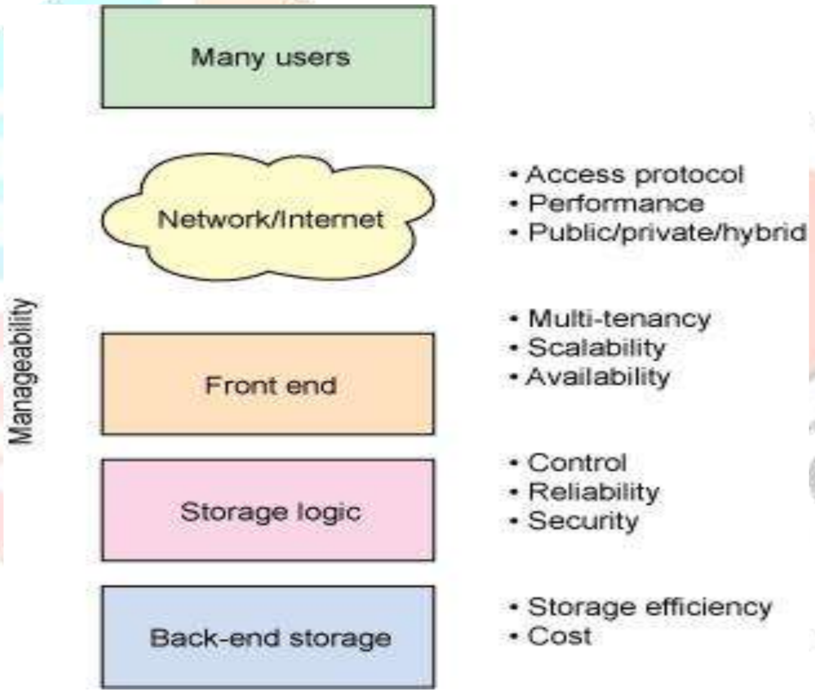

Fig 2. Cloud storage architecture

From Figure 2, you can see some of the characteristics for current cloud storage architectures [3]. Note that no characteristics are exclusive in the particular layer but serve as a guide for specific topics that addresses.

VI. **Cloud Storage API (Application Programming Interface)**

A Cloud Storage Application Programming Interface (API)[7] is a method for access to and utilization of a cloud storage system. The most common of these kinds are REST (Representational State Transfer) although there are others, which are based on SOAP (Simple Object Access Protocol). All these APIs are associated with establishing requests for service via the Internet. REST is a concept widely recognized as an approach to "quality" scalable API design. Cloud Storage is for files, which, some refer to as objects, and others call unstructured data. Think about the files stored on your PC, like pictures, spreadsheets and documents. These have an extraordinary variability, thus unstructured. The other kind of data is block or structured data. Think data base data, data that feeds transactional system that require a certain guaranteed or low-latency performance. Cloud Storage is not for this use case. Industrial Design Centre (IDC) estimates that approximately 70% of the machine stored data in the world is unstructured, and this is also the fastest growing data type. So, Cloud Storage is storage for files that is easily accessed via the Internet. This does not mean you cannot access Cloud Storage on a private network or LAN, which may also provide access to a storage cloud by other approaches, like NFS or CIFS. It does mean that the primary and preferred access is by a REST API. REST APIs are language neutral and therefore can be leveraged very easily by developers using any development language they choose. Resources within the system may be acted on through a URL. So, an API is not a "programming language", but it is the way a programming language is used to access a storage cloud. REST APIs are also about changing the state of resource through representations of those resources. Amazon S3 APIs, Eucalyptus APIs, Rack space Cloud Files APIs, Mezeo APIs, Nivanix APIs, Simple Cloud API, along with the standards proposed by the Storage Networking Industry Association (SNIA) Cloud Storage Technical Work Group, and more.

VII. **Conclusion**

Data storage in cloud is more advantageous than traditional storage because of its availability, scalability, performance, portability and its functional requirements. We mainly focused on data storage aspects that cloud service providers are following to store the data and security aspects to be provided for that data stored in cloud. We took a look on Amazon s3 [4] and third party auditing (TPA)[2] mechanisms which are used for data storage and security for data in cloud.

References

[1] http://www.ibm.com/developerworks/cloud/library/cl-cloudstorage/cl-cloudstorage-pdf.pdf

[2] T. Sivashakthi1, Dr. N Prabakaran A Survey on Storage Techniques in Cloud Computing" Volume3Issue12/IJETAE.

[3] R. Arokia Paul Rajan, S. Shanmugapriyaa "Evolution of Cloud Storage as Cloud Computing Infrastructure Service" IOSR Journal of Computer Engineering (IOSRJCE) ISSN: 2278-0661 Volume 1, Issue 1 (May-June 2012), PP 38-45

[4] Amazon.com, "Amazon Web Services (AWS)," Online at http://aws.amazon.com, 2008.

[5] http://www.business.att.com/enterprise/Service/hosting-services/cloud/storage/

[6] "Cloud Computing-Storage as Service" GurudattKulkarni, Ramesh Sutar, JayantGambhir / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 2, Issue 1, Jan-Feb 2012, pp.945-950

[7] http://searchsmbstorage.techtarget.com/feature/Understanding-cloud-storage-services-A-guide-for-beginners

[8] E.Gorelik, "Cloud Computing Models", Massachusetts Institute of Technology Cambridge, MA,2013. Available: http://web.mit.edu/smadnick/www/wp/2013-01.pdf

[9]GurudattKulkarni, Rani Waghmar, RajnikantPalwe, VidyaWaykule, HemantBankar, KudilikKoli."Cloud Storage Architecture".IEEE International conference on Telecommunication Systems, Services, and Applications(TSSA)

[10]Peter Mel, Timothy Grance,"The NIST Definition of Cloud Computing", Sept, 2011. Available: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf