A Survey on Cloud Computing Technology

Karan Singh[1] Nippun Kamboj[2]
[1,2]Department of Computer Science & Applications
[1,2]Kurukshetra University, Kurukshetra-136119

Abstract— Cloud computing evolution is the next generation architecture of IT enterprise. Cloud technique works with the application software and data bases at data centers, where the manipulations and management of data is done by cloud providers and these services may not be fully trustworthy. This occur many new security challenges which have not been fully implemented yet and this task is going on as research opportunities. Here in this paper, mainly focus on aspects for providing security for data storage in cloud, also services in cloud and architecture for data storage that are implemented by other service provider's vendors and TPAs in cloud, key points for proving security for data storage.

Key words: API, Cloud Computing, Cloud Security, Cloud Services

I. INTRODUCTION

Several trends and technology are opening up in the field of Cloud Computing, which is a computer technology based on internet services. Cloud storage is cheaper and more powerful concept. Software as a service (SaaS) model, are transforming data centers into a collection of computing service on a huge scale. Increasing these services users can now subscribe high quality services from data and software that reside on remote data centers(cloud stores).Using cloud storage services user need not to worry about hardware resources as well as maintenance. Some cloud computing vendors are Amazon Simple Storage Service (S3) and Amazon Elastic Compute Cloud (EC2). These internet based technology provide space for data storage and IT resources as per their user's need. Although, users depend on cloud service provider for the availability and integrity of data. Some benefits are added by cloud services as user need not to invest any capital on storage devices, no need for technical staff for maintain and manage the storage, backup and disaster management. Cloud computing provides group working with collaborating each other (both providers and clients) Allowing others instead of individual work while accessing data.

II. SERVICES IN CLOUD COMPUTING

Software as a Service: Software as a Service (SaaS) [1] is easy to use and most popular. SaaS service is used with help of the Web to provide applications that are provided by a third-party vendor and whose interface is accessed on the user's side. In the SaaS model, vendors provide application software. The installation, up-gradation and maintenance of application software in SaaS model handled by cloud vendors and cloud users access these resources. Support for all type of applications such as runtime, data integration, O/S, virtualization, servers, storage, and networking are all provided (see in fig. 1) by SaaS vendors therefore client not need to install these applications on their terminal. Examples for SaaS are Gmail, Google Apps, Microsoft Office 365, Google+ and Facebook.

Platform as a Service: Platform as a service (PaaS) [2] is a cloud computing model that provides applications over the Internet (see in fig. 1). In a PaaS model, a cloud provider delivers (on its own infrastructure) hardware and software tools usually those needed for application development to its users as a service. Clients need not to install hardware and software in PaaS model. Although, PaaS does not replace entire infrastructure, Instead, PaaS vendors provides some key services, such as Java development environment and tools or application hosting etc. Users usually access PaaS resources through a Web browser. Examples are Google App Engine, Appear IQ, Heroku, Amazon Web Services (AWS) Elastic Beanstalk and Mendix etc.

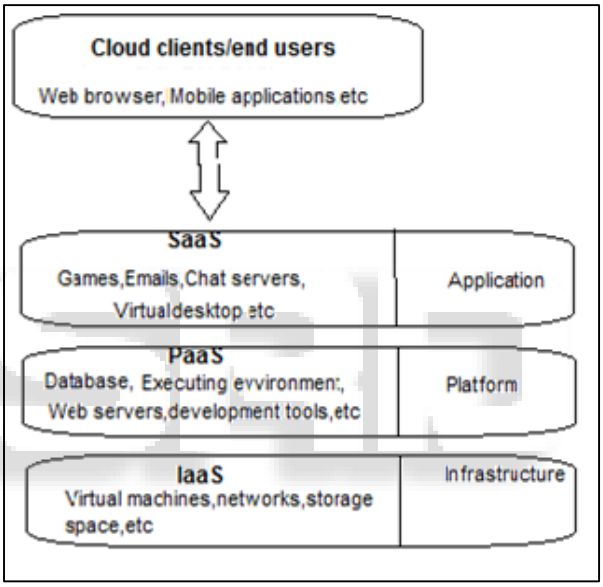

Fig. 1: Cloud Services

There are several types of PaaS models, including public, private and hybrid [3]. Public PaaS is derived from software as a service (SaaS) [4] and is situated in cloud computing between SaaS and infrastructure as a service (IaaS) [5]. A private PaaS can typically be downloaded and installed either on a company's on-premises infrastructure, or in a public cloud.

Infrastructure as a Service: Infrastructure as a Service (IaaS) model [6] provides virtualized computing resources (see in fig. 1) with the help of third party. In an IaaS model, a third-party vendor provides all the resources such as hardware, software, servers, storage to their clients by setting up virtual machine (server) on their IT infrastructure and charge as per uses basis (resource consumed). IaaS providers handle tasks including system maintenance, backup, virtual machines facility etc. Some examples of IaaS providers are Amazon Web Services (AWS), IBM Smart Cloud Enterprise, Windows Azure, Google Compute Engine, and Rackspace Open Cloud.

III. CLOUD STORAGE MODELS

The control over data is performed by cloud models [1]. Cloud storage has divided into three categories [7], public, private, hybrid cloud storage. In public cloud storage model all customers share the same infrastructure pool with limited configurations and publically sharable resources. Private cloud model built exclusively for an individual enterprise. Hybrid cloud storage merges private and public clouds (see figure no. 2).

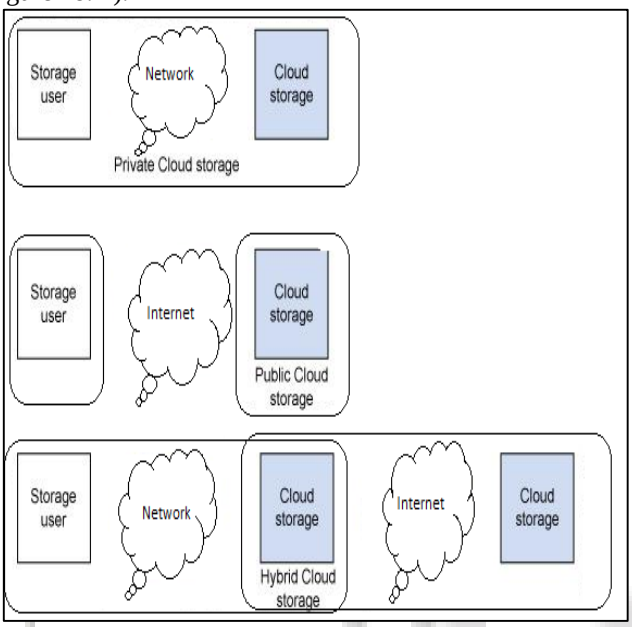

Fig. 2: Different cloud storage models

Examples of public cloud storage providers include Amazon (which offers SaaS). Examples of private cloud storage providers include IBM, Para scale, and Clever safe (which build software and/or hardware for internal clouds). Finally, hybrid cloud providers include Egnyte.

IV. CLOUD STORAGE ARCHITECTURE

Cloud storage architectures [8] [9] are primarily about delivery of storage on demand in a highly scalable and multi-tenant way. Web services, user interaction and application interfaces having user interactions are at front ends. Behind the front end is a layer of middleware that can call as storage logic (see in fig. no 3). This layer implements a variety of features, such as replication and data reduction for control and security issues.

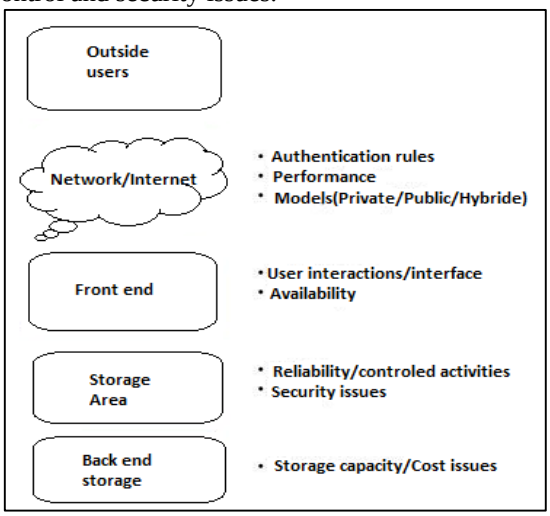

Fig. 3: Cloud Storage Architecture

At last, back end consists of physical storage, disk issues and storage capacity for data. This may be an internal protocol that implements specific features or a traditional back end to the physical disks.

V. DATA STORAGE SECURITY TECHNIQUES IN CLOUD COMPUTING

Many traditional techniques for securing the cloud [10] have been discussed here. Cloud storage uses virtualization technology and provides interface for data storage.

A. Implicit Storage Security to Data in Online transaction/activity

In cloud security implicit storage security provides some additional advantages. For using this type of data partitioning schemes involves the roots of a polynomial in finite field. Data in this method is divided in separate portions and each divided portion implicitly secure [11]. Any data portion not need to be encrypted and each data portion placed randomly on different servers on network only known to the users.

For recreation of data each server is to be accessed by user on which data portions are stored.

B. Identify –Based Authentication (IBE)

In Cloud Computing, resources and services are distributed across thousands of clients. Due to distributed type network each user and services need to be authenticated for security reasons.

While using SSL Authentication Protocol (SAP) it was becomes a tough task to implement it. Therefor to achieve the security benefits of SAP a new authentication protocol based on identity [12], using hierarchical model with corresponding signature and encryption schemes was used.

IBA protocol used sequence of steps to secure cloud. In step (1) the user 'U' sends the servers a user "Hello" message. The message contains a fresh random number 'Un', session identifier 'ID' and 'U' specification.
In step (2) the server S responds with a server "Hello" message which contains new fresh random number Sn and provides authentication to user.

C. Public Auditing with Complete Data Dynamic Support

Data integrity and verification of integrity at various unreliable and suspected servers is to be verified in cloud storage for security concern. Firstly find out the problems and potential security threats of existing works and after that prepare a refined verification scheme Public auditing system with protocol that provides provision of complete dynamic data operations [13]. The efficient data dynamics is supported by the classic Merkle Hash Tree (MHT) construction. The technique of bilinear aggregate signature is used for auditing task efficiently. In this way TPA will be able to do multiple auditing tasks at a time in multiuser setting. This scheme is efficient and provably secure.

D. Efficient Third Party Auditing (TPA)

Cloud clients save data in cloud server and their main aim is security as well as data storage correctness. Managing the outsourced data is difficult and expensive task for safely data integration and manipulation. Data owners therefore

required reliable third party auditors (TPA) [14] with safety in integrity checking tasks. 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.

E. Way of Dynamically Store Data in Cloud

Clients do not possess local copy of outsourced data stored in cloud, thus not completely reliable. To solve these issues a novel protocol is proposed using the data reading protocol algorithm to check the data integrity [15]. Cloud service providers help the clients to check the data security by using the proposed effective automatic data reading algorithm. To recover data in future, a multi-server data comparison algorithm with overall data calculation in each update before outsourcing it to server's remote access point is also provided.

F. Effective and Secure Storage Protocol

While outsourcing data, a cloud user loses control over data and new security risks such as confidentiality and integrity occur. To solve these issues a new protocol which is based on elliptic curve cryptography and sober sequence introduced [16]. This technique allows TPA to periodically confirm integrity of data at cloud without recovering original data. Cloud Server challenges a random set of blocks that generates probabilistic proof of integrity. Challenge-Response protocol exchanges small amount of data on network. This small amount of data does not carry any useful information and will not expose the contents of data to outsiders.

G. Storage Security of Data

Resources in cloud computing are being shared across internet that creates many type of data security problems in cloud. Transmitting data over internet is dangerous due to the intermediate attack. Data encryption algorithms play an important role in cloud environment while exchanging data. The proposed technique provides some security benefits [17] that are used in cloud environment. A virtual network model is created which having three data backups techniques for data recovery. These three backups located in remote location from main server. This method used

1) SHA Hash algorithm for encryption,
2) SFSPL algorithm for splitting files,
3) GZIP algorithm for compression.

Thus, a secure platform is provided for cloud computing.

H. Secure and Dependable Storage Service

Clients of cloud storage services do not worry about data storage maintenance but correctness of data is major issue. Proposed system [18] permits clients inspecting the cloud data storage. Reed-Solomon erasure correcting code technique is used, which ensures the correctness and also recognizes misbehaving server. This design also support block level dynamic operations and if users do not have sufficient resources for processing data then user can assign this task to TPA. In this way this technique provides secure remote place for data storage and supports dynamic operations like insert, update and delete.

I. Optimal Cloud Storage Systems

Cloud data storage which needs minimum effort is popular among clients for data backup and synchronization. The proposed system describes a possible architecture for a cryptographic enabled storage service. 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) that generates token which enables the cloud storage providers to retrieve segments of consumer data.

J. Process of Access And Store Small Files With Storage

Hadoop distributed file system (HDFS) is used for support internet resources and services. HDFS does not support well with many small size files and this issue to be focused in cloud. In order to overcome these small size problems, proposed an approach [19] that improves the small files efficiency on HDFS. For securely manage small files over network correlation between small files is not considered as essential task. Instead of this correlation feature file is divided into three parts as:-

Logically related small files, Structurally related small files and Independent files for structurally-related small files.

K. File Storage Security Management

Distributed framework scheme is used to ensure data security in cloud computing. This framework consists of a master-slave server policy (Master 'M' and multiple slaves 'S'). 'M' is responsible to process the client's request and at 'S' chunking operation in order to provide data backup for file recovery in future. Clients file is stored in the form of tokens on main server and files were chunked on slave servers for file recovery. Holomorphic token and merging algorithms were used to generate tokens for clients in this approach.

VI. CLOUD STORAGE APIS

Access and utilization of Cloud Storage is performed by Cloud Storage Application Programming Interface (API) [20]. For Cloud storage and for using Cloud resources REST (Representational State Transfer) and SOAP (Simple Object Access Protocol) are mostly used APIs. All these APIs are used via internet by setting up requests for services. REST having "stateless" architecture used as an approach to "quality" scalable API design. "Stateless" defines itself as everything that needed to complete the request to the storage cloud is contained in the request, and this implies that a session between the requestor and the storage cloud is no further needed. It is very important because the Internet has an undefined response time and it is generally not fast when compared to a local area network thus this concept becomes more important. Traditional file storage access methods that use NFS (network files system) or CIFS (Common Internet File System)] do not work over the Internet, because of latency. Cloud Storage is for files, which, some refer to as objects, and others call unstructured data. So, Cloud Storage is storage for files that is easily accessed via the Internet. This does not mean anyone 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 not language dependent and can be implemented in any language environment. Hence API is not a "programming language", but it is the way a programming language is used to access a storage cloud. Some examples of APIs are Amazon S3 APIs, Rack space Cloud Files APIs, Mezeo APIs, Simple Cloud API , Eucalyptus APIs etc.

VII. CONCLUSION

Data storage in cloud storage provides more advantages over traditional storage because of its scalability, performance, availability, portability and its remote functional requirements. In cloud storage focus is on data storage aspects and security aspects to be provided to their clients. Amazon s3 and third party auditing (TPA) mechanisms which are used for data storage and security for data in cloud are popular in these days.

REFERENCES

[1] V. Spoorthy, M. Mamatha, B. Santhosh Kumar "A Survey on Data Storage and Security in Cloud Computing", IJCSMC, pg. no. 306 – 313, Vol. 3, Issue 6, June 2014.
[2] Dinesh Prakash, Dr. Sunil Taneja, "Cloud Computing Survey: Architecture, Models, Performance, Storage and Technologies", IJCITE, page no 96-106, Volume-1 Issue - 7, October 2014.
[3] Mike Kavis, "Top 8 Reasons Why Enterprises Are Passing On PaaS," Forbes, September 15, 2014.
[4] Jack Schofield, "Google angles for business users with platform as a service," The Guardian, April 16, 2008.
[5] Brandon Butler, "PaaS Primer: What is platform as a service and why does it matter?" Network World, February 11, 2013.
[6] Jahnvi S. Kapadia," Survey on Various Techniques for Data Storage Security in Cloud Computing", IJSER, Volume 4, Issue 5, May-2013
[7] D. Kanchana, Dr. S. Dhandapani, "A Novel Method for Storage Security in Cloud Computing", IJESIT, Volume 2, Issue 2, March 2013.
[8] R. A. P. Rajan, S. Shanmugapriyaa "Evolution of Cloud Storage as Cloud Computing Infrastructure Service" IOSRJCE,Volume 1,Issue 1
[9] Manoj Kokane, Premkumar Jain, Poonam Sarangdhar, "Data Storage Security in Cloud Computing", IJARCCE, Vol. 2, Issue 3, March 2013.
[10] Wang C, Wang Q et al, Towards secure And dependable Storage Services in Cloud Computing , IEEE Transactions on Services Computing ,vol5(2), pp-220-232, 2012.
[11] T. Sivashakthi, Dr. N Prabakaran, "A Survey on Storage Techniques in Cloud Computing", IJETAE, Volume 3, Issue 12, December 2013.
[12] Li H, Dai Y et al. (2009), Identity-Based Authentication for Cloud Computing, M. G. Jaatun, G. Zhao, and C. Rong (Eds.): Cloud Computing, Lecture Notes in Computer Science, vol 5931, 157–166.
[13] Pradnya B. Godhankar, Deepak Gupta," Review of Cloud Storage Security and Cloud Computing Challenges", IJCSIT, Vol. 5 (1), 528-533, 2014.
[14] D. Purushothaman, Dr. Sunitha Abburu, "An Approach for Data Storage Security in Cloud Computing", IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 2, No 1, March 2012.
[15] Dinesh C (2011). Data Integrity and Dynamic Storage Way in Cloud Computing, Distributed, Parallel, and Cluster Computing.
[16] Kumar S P, Subramanian R (2011). An efficient and secure protocol for ensuring data storage security in Cloud Computing, International Journal of Computer Science Issues, vol 8(6), No 1, 261–274
[17] Sajithabanu S, Raj E G P (2011). Data Storage Security in Cloud, International Journal of Computer Science and Technology, vol. 2(4), 436–440.
[18] Amol S. Choure, S. M. Bansode, "A Comprehensive Survey on Storage Techniques in Cloud Computing", IJCA, Volume 122 – No.18, July 2015.
[19] Dong B, Zheng Q et al. (2012) An optimized approach for storing and accessing small files on cloud storage, Journal of Network and Computer Applications, 35 (6),1847–1862.
[20] CITO Research Advancing the craft of technology leadership, Enterprise-class API Patterns for Cloud & Mobile, may 2012.

