International Journal of Application or Innovation in Engineering & Management (IJAIEM)
Web Site: www.ijaiem.org Email: editor@ijaiem.org
Volume 6, Issue 4, April 2017 **ISSN 2319 - 4847**

Data Protection in Cloud Computing

Shabnam Kumari[1], Princy[2] and Reema[3]

[1,3]A.P., Department of CSE, Sat Kabir Institute of Technology & Management, Bahadurgarh

[2]Mtech scholar, Department of CSE, Sat Kabir Institute of Technology & Management, Bahadurgarh

ABSTRACT

Cloud Computing has been envisioned as the next generation architecture of IT Enterprise. In contrast to traditional solutions, where the IT services are under proper physical, logical and personnel controls, Cloud Computing moves the application software and databases to the large data centers, where the management of the data and services may not be fully trustworthy. This unique attribute, however, poses many new security challenges which have not been well understood. In this article, we focus on cloud data storage security, which has always been an important aspect of quality of service. To ensure the correctness of users' data in the cloud, we propose an effective and flexible distributed scheme with two salient features, opposing to its predecessors. By utilizing the homomorphic token with distributed verification of erasure-coded data, our scheme achieves the integration of storage correctness insurance and data error localization, i.e., the identification of misbehaving server(s). Unlike most prior works, the new scheme further supports secure and efficient dynamic operations on data blocks, including: data update, delete and append. Extensive security and performance analysis shows that the proposed scheme is highly efficient and resilient against Byzantine failure, malicious data modification attack, and even server colluding attacks.

Keywords: Cloud Computing, Byzantine failure, server colluding attacks.

1. INTRODUCTION

Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). The name comes from the use of a cloud-shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams. Cloud computing entrusts remote services with a user's data, software and computation.

There are many types of public cloud computing:[1]

- Infrastructure as a service (IaaS)
- Platform as a service (PaaS)
- Software as a service (SaaS)
- Network as a service (NaaS)
- Storage as a service (STaaS)
- Security as a service (SECaaS)
- Data as a service (DaaS)
- Database as a service (DBaaS)
- Test environment as a service.
- Desktop virtualization.
- API as a service (APIaaS)
- Backend as a service (BaaS)

In the business model using software as a service, users are provided access to application software and databases. The cloud providers manage the infrastructure and platforms on which the applications run. SaaS is sometimes referred to as "on-demand software" and is usually priced on a pay-per-use basis. SaaS providers generally price applications using a subscription fee.

Proponents claim that the SaaS allows a business the potential to reduce IT operational costs by outsourcing hardware and software maintenance and support to the cloud provider. This enables the business to reallocate IT operations costs away from hardware/software spending and personnel expenses, towards meeting other IT goals. In addition, with applications hosted centrally, updates can be released without the need for users to install new software. One drawback of SaaS is that the users' data are stored on the cloud provider's server. As a result, there could be unauthorized access to the data. End users access cloud-based applications through a web browser or a light-weight desktop or mobile app while the business software and user's data are stored on servers at a remote location. Proponents claim that cloud computing allows enterprises to get their applications up and running faster, with improved manageability and less maintenance, and enables IT to more rapidly adjust resources to meet fluctuating and unpredictable business demand.[2][3]

Cloud computing relies on sharing of resources to achieve coherence and economies of scale similar to a utility (like the electricity grid) over a network.[4] At the foundation of cloud computing is the broader concept of converged infrastructure and shared services.

.

Figure 1.1:- cloud computing.

2. ARCHITECTURE OF CLOUD COMPUTING

Cloud Computing architecture comprises of many cloud components, each of them are loosely coupled. We can broadly divide the cloud architecture into two parts:

a) Front End
b) Back End

Each of the ends is connected through a network, usually via Internet. The following diagram shows the graphical view of cloud computing architecture:

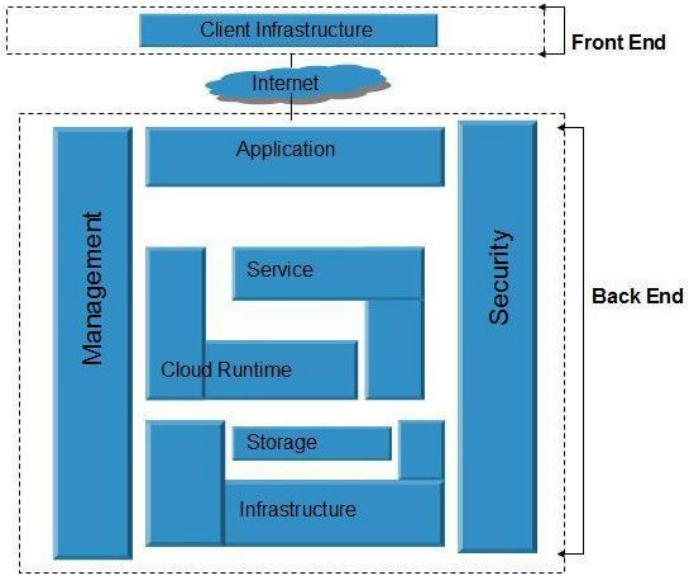

Figure 2.1:- Architecture of cloud computing

2.1. Front end

Front End refers to the client part of cloud computing system. It consists of interfaces and applications that are required to access the cloud computing platforms, e.g., Web Browser.

2.2. Back end

Back End refers to the cloud itself. It consists of all the resources required to provide cloud computing services. It comprises of huge **data storage, virtual machines, security mechanism, services, deployment models, servers**, etc.
Important Points:-

- It is the responsibility of the back end to provide built-in security mechanism, traffic control and protocols.
- The server employs certain protocols, known as middleware, helps the connected devices to communicate with each other.

3. CLOUD COMPUTING MANAGEMENT

It is the responsibility of cloud provider to manage resources and their performance. Management may include several aspects of cloud computing such as **load balancing, performance, storage and backups, capacity, deployment** , etc. Management is required to access full functionality of resources in the cloud.

3.1. Cloud Management Tasks

Cloud Management involves a number of tasks to be performed by the cloud provider to ensure efficient use of cloud resources. Here, we will discuss some of these tasks:

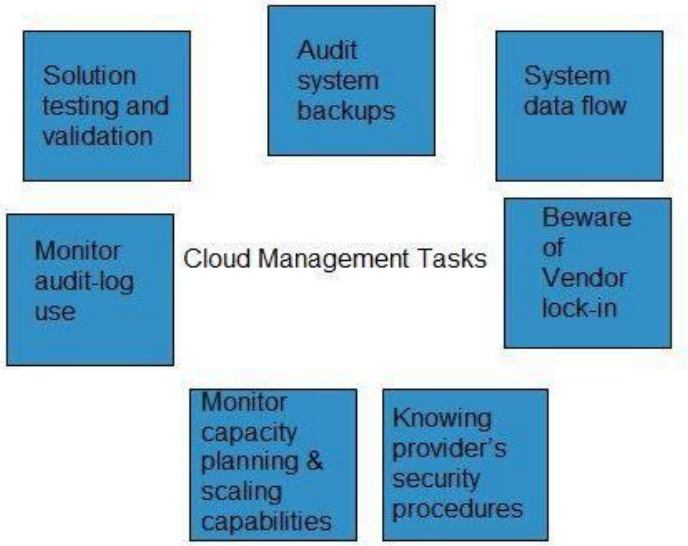

Figure 3.1:- Cloud management tasks

3.1.1. Audit System Backups

It is required to timely audit the backups to ensure you can successfully restore randomly selected files of different users. Backups can be performed in following ways:

a) Backing up files by the company, from on-site computers to the disks that reside within the cloud.

b) Backing up files by the cloud provider.

It is necessary to know if cloud provider has encrypted the data, who has access to that data and if the backup is taken at different locations, you must know where.

3.1.2. System's Data Flow

The managers should develop a diagram describing a detailed process flow. This process flow will describe the movement of company's data throughout the cloud solution.

3.1.3. Beware Of Vendor Lock-In

The managers must know the procedure to exit from services of a particular cloud provider. There must exist procedures, enabling the managers to export company's data to a file and importing it to another provider.

3.1.4. Knowing Provider's Security Procedures

The managers should know the security plans of the provider for different services:

- Multitenant use
- E-commerce processing
- Employee screening
- Encryption policy

3.1.5. Monitor Capacity Planning And Scaling Capabilities

The managers should know the capacity planning in order to ensure whether the cloud provider will meet the future capacity requirement for his business or not. It is also required to manage scaling capabilities in order to ensure services can be scaled up or down as per the user need.

3.1.6. Monitor Audit-Log Use

In order to identify the errors in the system, managers must audit the logs on a regular basis.

3.1.7. Solution Testing And Validation

It is necessary to test the solutions provided by the provider in order to validate that it gives the correct result and is error-free. This is necessary for a system to be robust and reliable

4. CLOUD COMPUTING DATA STORAGE

Cloud Storage is a service that allows to save data on offsite storage system managed by third-party and is made accessible by a **web services API**.

4.1. Storage Devices

Storage devices can be broadly classified into two categories:

a) Block Storage Devices

Block Storage Devices offer raw storage to the clients. This raw storage can be partitioned to create volumes.

b) File Storage Devices

File Storage Devices offers storage to clients in form of files, maintaining its own file system. This storage is in the form of Network Attached Storage (NAS).

4.2. Cloud Storage Classes

Cloud Storage can be broadly classified into two categories:

a) Unmanaged Cloud Storage

Unmanaged Cloud Storage means that the storage is preconfigured for the consumer. The consumer cannot format nor the consumer can install own file system or change drive properties.

b) Managed Cloud Storage

Managed Cloud Storage offers online storage space on demand. Managed cloud storage system presents what appears to the user to be a raw disk that the user can partition and format.

4.3. Creating Cloud Storage System

The cloud storage system stores multiple copies of data on multiple servers and in multiple locations. If one system fails, then it only requires changing the pointer to stored object's location. To aggregate storage assets into cloud storage systems, the cloud provider can use storage virtualization software, **StorageGRID**. It creates a virtualization layer that fetches storage from different storage devices into a single management system. It can also manage data from **CIFS** and **NFS** file system over the Internet.

4.4. Challenges

Storing the data in cloud is not that simple task. Apart from its flexibility and convenience, it also has several challenges faced by the consumers. The consumers require ability to:

- Provision additional storage on demand.
- Know and restrict the physical location of the stored data.
- Verify how data was erased?
- Have access to a documented process for surely disposing of data storage hardware.
- Administrator access control over data.

5. CLOUD COMPUTING SECURITY

Security in cloud computing is a major concern. Data in cloud should be stored in encrypted form. To restrict client from direct accessing the shared data, proxy and brokerage services should be employed.

5.1. Security Planning

Before deploying a particular resource to cloud, one should need to analyze several attributes about the resource such as:

a) Select which resources he is going to move to cloud and analyze its sensitivity to risk.

b) Consider cloud service models such as **IaaS, PaaS**, and **SaaS**. These models require consumer to be responsible for security at different levels of service.

c) Consider which cloud type such as **public, private, community** or **hybrid**.

d) Understand the cloud service provider's system that how data is transferred, where it is stored and how to move data into and out of cloud.

Mainly the risk in cloud deployment depends upon the service models and cloud types.

5.2. Understanding Security of Cloud

5.2.1. Security Boundaries

A particular service model defines the boundary between the responsibilities of service provider and consumer. **Cloud Security Alliance (CSA)** stack model defines the boundaries between each service model and shows how different functional units relate to each other. The following diagram shows the **CSA stack model:**

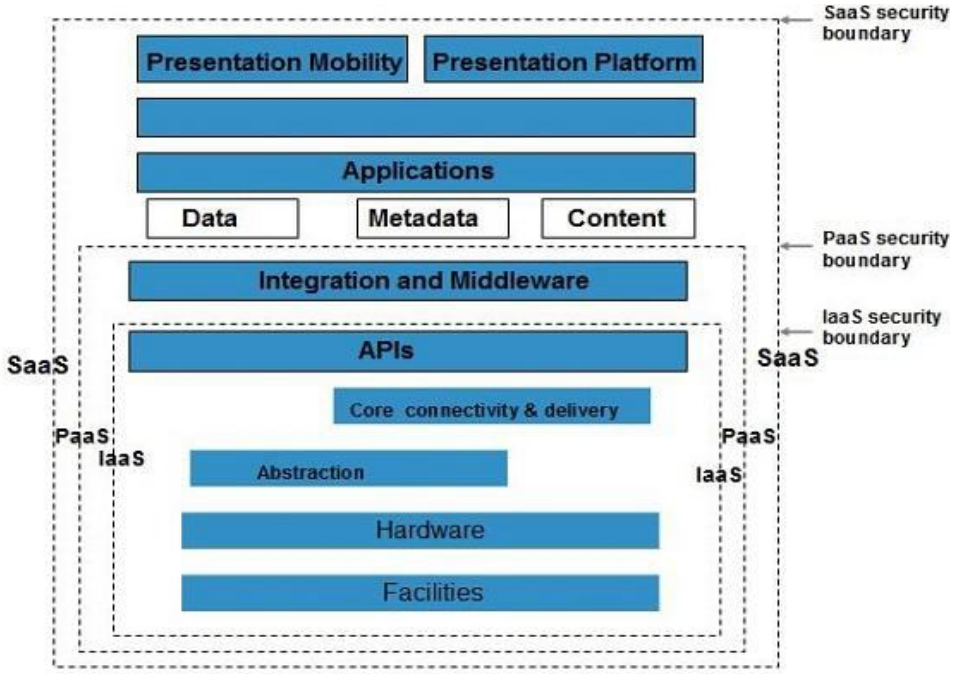

Figure 5.1:- CSA stack model

Key Points To CSA Model:

- IaaS is the most basic level of service with PaaS and SaaS next two above levels of service.
- Moving upwards each of the service inherits capabilities and security concerns of the model beneath.
- IaaS provides the infrastructure, PaaS provides platform development environment and SaaS provides operating environment.
- IaaS has the least level of integrated functionalities and integrated security while SaaS has the most.
- This model describes the security boundaries at which cloud service provider's responsibility ends and the consumer's responsibilities begin.
- Any security mechanism below the security boundary must be built into the system and above should me maintained by the consumer.
- Although each service model has security mechanism but security needs also depends upon where these services are located, in private, public, hybrid or community cloud.

5.3. Understanding Data Security

Since all the data is transferred using Internet, data security is of major concern in cloud. Here are key mechanisms for protecting data mechanisms listed below:

- Access Control
- Auditing
- Authentication
- Authorization
- All of the service models should incorporate security mechanism operating in all above-mentioned areas.

5.4. Isolated Access To Data

Since data stored in cloud can be accessed from anywhere, therefore to protect the data, we must have a mechanism to isolate data from direct client access. **Brokered Cloud Storage Access** is one of the approaches for isolating storage in cloud. In this approach, two services are created:

- A broker with full access to storage but no access to client.
- A proxy with no access to storage but access to both client and broker.

5.5. Working Of Brokered Cloud Storage Access System

When the client issue request to access data:

- The client data request goes to proxy's external service interface.
- The proxy forwards the request to the broker.
- The broker requests the data from cloud storage system.
- The cloud storage system returns the data to the broker.
- The broker returns the data to proxy.
- Finally the proxy sends the data to the client.

All of the above steps are shown in the following diagram:

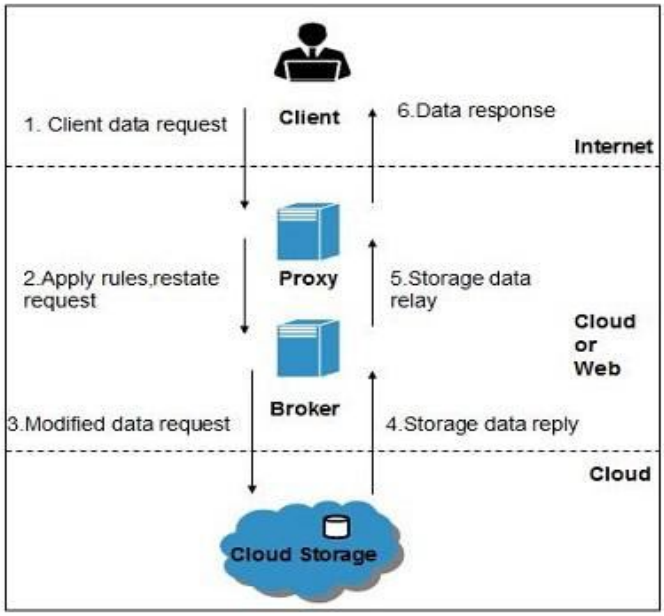

Figure 5.2:-Steps for request to access data

6. Cloud Computing Operation And Challenges

Cloud Computing operation refers to delivering superior cloud service. Today, cloud computing operations have become very popular and widely employed by many of the organizations just because it allows performing all business operations over the Internet. These operations can be performed using a web application or mobile based applications. There are a number of operations that are performed in cloud; some of them are shown in the following diagram:

Figure 6.1:-Cloud computing operations

6.1. Managing Cloud Operations

There are several ways to manage day-to-day cloud operations, as shown in the following diagram:-

- Always employ right tools and resources to perform any function in the cloud.
- Things should be done at right time and at right cost.
- Selecting an appropriate resource is mandatory for operation management.
- The process should be standardized and automated to avoid repetitive tasks.
- Using efficient process will eliminate the waste and redundancy.
- One should maintain the quality of service to avoid re-work later.

6.2 Cloud Computing Challenges

Cloud Computing, an emergence technology, has placed many challenges in different aspects. Some of these are shown in the following diagram:

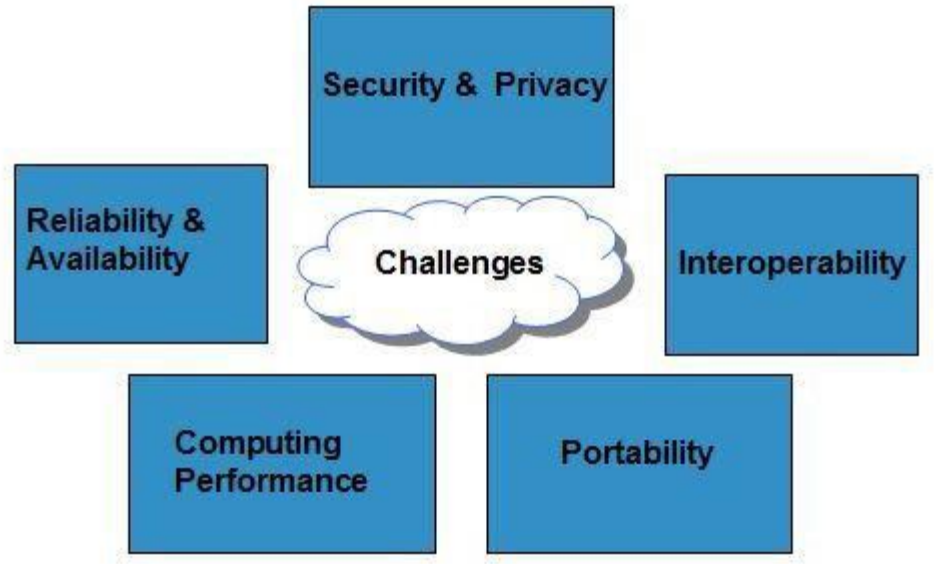

Figure 6.2 :- Cloud computing challenges

6.2.1 Security & Privacy
Security and Privacy of information is the biggest challenge to cloud computing. Security and privacy issues can be overcome by employing encryption, security hardware and security applications.

6.2.2 Portability
This is another challenge to cloud computing that applications should easily be migrated from one cloud provider to another. There should not be vendor lock-in. However, it is not yet made possible because each of the cloud provider uses different standard languages for their platforms.

6.2.3 Interoperability
Application on one platform should be able to incorporate services from other platform. It is made possible via web services. But writing such web services is very complex.

6.2.4 Computing Performance
To deliver data intensive applications on cloud requires high network bandwidth, which results in high cost. If done at low bandwidth, then it does not meet the required computing performance of cloud application.

6.2.5 Reliability And Availability
It is necessary for cloud systems to be reliable and robust because most of the businesses are now becoming dependent on services provided by third-party.

7. CONCLUSION

This Web Application provides facility to conduct online examination worldwide. It saves time as it allows number of students to give the exam at a time and displays the results as the test gets over, so no need to wait for the result. Administrator has a privilege to create, modify and delete the test papers and its particular questions. User can register, login and give the test with his specific id, and can see the results as well.

REFERENCES

[1] Angaye, C. C. (November, 2012). Cloud Computing Will Transform the Nigerian Economy:Thisday. Retrieved 20th February, 2015 from http://www.thisdaylive.com/articles/cloud-computing-will-transform-the-nigerianeconomy/129287/

[2] Armbrust, M., Fox, A. Griffith, R., Joseph, A., Katz, R., Konwinski, A., Lee, G., Patterson, D.,Rabkin, A., Stoica, and Zaharia, M. (2009). Above the Clouds: A Berkeley View of Cloud Computing, 2009.

[3] Burton, H. (2014). 'Cloud computing - Separating fact from fiction'. The Guardian, 2014.Retrieved 10th January ,2015 from http://www.theguardian.com/medianetwork/partner-zone-microsoft/cloud-computingseparating-fact.

[4] Buyya, R., Yeo, C. S., Venugopal, S., Broberg, J. and Brandic, I. (2009). "Cloud Computing and Emerging IT Platforms: Vision, Hype, and Reality for Delivering Computing as the 5th Utility," Future Generation Computer Systems (25)6.

[5] Cisco (2013). The Cloud in Africa: Reality Check. Retrieved December 15th, 2014 from http://www.cisco.com/web/ZA/press/2013/112813.html.CompTIA (August, 2013). Trends in Cloud Computing: Full Report, August 2013. Retrieved 17th March, 2015 from www.comptia.org
[6] Heiser, J. and Nicolett, M. (2008). Assessing the Security Risks of Cloud Computing. Gartner.Hinchcliffe, D. (5th June, 2009). Eight ways that Cloud Computing will Change Businesses,Retrieved March 13th, 2015 from http://www.zdnet.com/blog/hinchcliffe/eight-waysthat-Cloud-computing-will-changebusiness/488
[7] International Data Corporation (IDC) (2012). White Paper: Cloud Computing's Role in JobCreation, 2012. Retrieved 9th February, 2015 from http://people.uwec.edu/HiltonTS/ITConf2012/NetApp2012Paper.pdf
[8] Jinzy, Z. (2010). Cloud Computing Technologies and Applications, Handbook of Cloud Computing, 2010, retrieved 6th March, 2015 from http://www.springer.com/978-1-4419-6523-3
[9] Kim, W. (2009). Cloud Computing: Today and Tomorrow. Journal of Object Technology. 8(1):p. 65-72.

BOOKS:
[1] Core Servlets and JSP – vol1- Hall & Brown (2nd Edition).
[2] Core Java 2 Volume 1 - Fundamentals Cay S. Horstmann, Gary Cornell
[3] Core Java 2 Volume 2 - Advanced Features Cay S. Horstmann, Gary Cornell.
[4] Complete Reference for J2EE 5th Edition.
[5] By Google.com.

AUTHOR

Princy, received the B.Tech degree in Computer Science & Engineering from Tek chand maan College of Engineering, Sonepat affiliated to DCRUST University, Sonepat (Haryana) and pursuing M.Tech (2015 to 2017 batch) from Sat Kabir Institute of Technology and Management (SKITM), Bahadurgarh affiliated to Maharshi Dayanand University, Rohtak (Haryana). Currently I am doing research on data protection in cloud computing.

Shabnam Kumari, received the B.Tech degree in Computer Science & Engineering from Maharaja Surajmal Institute of Technology (MSIT), affiliated to Guru Gobind Singh Indraprastha University, New Delhi and M.Tech degree in Computer Science & Engineering from PDM college of Engineering, affiliated to Maharshi Dayanand University, Rohtak (Haryana) in 2011 and 2013 batch respectively. She is presently working in Sat Kabir Institute of Technology and Management (SKITM), Bahadurgarh, Haryana, India with 3.5 yrs teaching experience. She has 20+ publications in international journal and 5 publications in conferences. She is having membership of two international journals. She possesses rich experience of research and guided 15+ dissertations of M.tech.