Cloud Computing – Health Applications & Security

Jeevan Reddy
Computer Science and Engineering
Saveetha School of Engineering, Saveetha University.

Abstract— Cloud Computing is defined as a type of parallel and distributed system consisting of a collection of interconnected and virtualized computers. It is based on service-level agreements that are established between the service providers and consumers. Cloud Computing opens up many new possibilities for application developers. This paper provides an approach on how to use Cloud computing in healthcare, focusing on the implementation needs and benefits. Cloud Computing moves databases to be data centre where the management of the data and services may not be fully trustworthy and it poses many security challenges which have not been well understood. To ensure the correctness of users' data in the cloud, this paper also describes about the security criteria and strains.

Key words **:** Cloud Computing, virtualized computers, Security, virtualized computers.

I. SYSTEM DESIGN

The Cloud services should be in the form of queues. The cloud platform is a Graphical user interface which acts as the front end controller for the application. The cloud storage is the database which is used to store data entries. Even though Clouds make deployment of large scale applications easier and cheaper, the cloud also creates new issues for developers. Cloud infrastructures are distributed, applications can be

deployed in different geographic locations, and the chosen distribution impacts the performance for users who are far from the data center. Below is the overview of the cloud service providers.

Components of the service provider are :

(1) Cloud Agent
(2) Account Manager
(3) Resource Sharer
(4) Service Register
(5) Service Manager
(6) Resource Monitor

A. Cloud Agent :

Cloud Agent are the customers

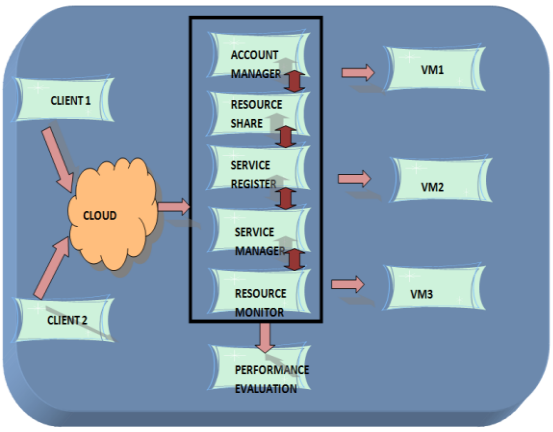

Fig. 1: Cloud Agent

who securely access information from the cloud environment. Leveraging WiFi connectivity, users can securely access corporate reports, network file systems, applications, and content from anywhere, at anytime.

B. Account Manager:

The role of the Cloud Account Manager will be to drive business results and growth by working closely with the assigned cloud partner to establish key application and operator partnerships that leads to increased revenue through the mobile cloud while leveraging the unique capabilities of the product suite.

C. Resource Sharer:

This component provides desirable execution environment based on user requirements and providing necessary disk images and required information for running the application. After deployment phase, the component helps end users to manage their appliances.

D. Service Register:

It allows providers to advertise their virtual units. The advertisement of virtual unit contains descriptions of their features, costs, and the validity time of the advertisement.

E. Service Manager:

A monitoring system is provided by this component for fairly determining to which extent a facilitating procedure taken by a user is received. The monitoring is based on the copy of signed SLA which is kept in SLA repository. Third party monitoring results can be similar to what the Cloud Status service reports. Hyperic's Cloud Status is the first service to provide an independent view into the health and performance.

F. Resource Monitor:

Administrators can drill down into detailed performance data from disk latency to network trafficto application-specific parameters

G. Performance Evaluation:

The performance of the cloud environment is being evaluated using some algorithm and the techniques specified and some optimizing techniques is also been specified in the cloud environment.

II. MODULES

(1) GUI package
(2) Remote Cloud Server Access
(3) Virtual Server Integration
(4) Multiple Operating System Integration

A. GUI Package:

The interaction between the requester and the provider takes place via GUI. It provides authentication for the requester

and acts as a service provider. The client also has to be authenticated for the cloud servers. To be an authenticated client, the client has to produce the system name, IP address and port address, and It also specifies the authentication using the username and password, It is stored in the MySQL database. The data can be accessed from the database and can perform the import operations. The unauthenticated users can't access the cloud environment.

B. Remote Cloud Server Access:

The remote Cloud Server Access can be obtained from the base remote servers which holds the main server software. The remote servers can be accessed by connecting to the servers through the server IP address and server passwords. And we can access the software from the server only by proper authentication environment.

C. Virtual Server Integration:

The virtual servers can be integrated through the remote servers. Through the virtual server integration the various software and operating systems in the cloud systems can be accessed from the servers. The virtual servers can be accessed from the VMware integrator. And using this module we can calculate the CPU and the execution time can also be calculated.

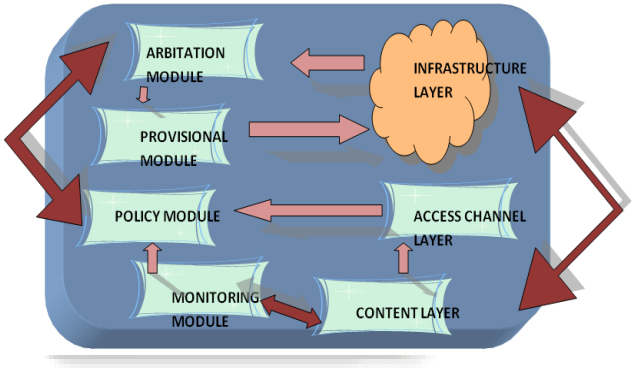

Fig. 2 : Virtual server integration

D. Multioperating System Integration:

Through our virtual servers we can access the other operating system. For e.g., if the client has Microsoft xp in their system but if they want to access Linux that is possible through our virtual server.

III. Cloud Computing and Healthcare

Cloud computing has the strength to face the demands in the health field. The feature of a good health service includes:
-Successful and judicious contact between the particulates.
The emerging cloud computing technologies provide a promising approach to for the future collaborative needs in coordinated healthcare and its services. The structure can simplify the sharing and governance of the healthcare information to better facilitated patient-centric healthcare and Verification predestined medicine.

IV. Health Architecture

The health care architecture contains three layers.

(1) Access Channel Layer
(2) Content Layer
(3) Infrastructure Layer

A. Access Channel Layer:

This is responsible for handling all the interactions between various users with the cloud based healthcare applications and provides the users with a rich interface. This layer handles the construction and presentation of the unit to the user, device handling of content, manages the session and provides the right content for the right person through personalized content.

B. Content Layer:

It mainly consists of cloud based contents, such as web file systems, database systems, web services, and so on. This layer exposes the standard interfaces and APIs of contents for higher layers.

C. Infrastructure Layer:

This acts as the resource pool of cloud based healthcare system. This infrastructure is managed by cloud computing platform. Hardware and software virtualization technologies are used to ensure the stability and reliability of the infrastructure. The health care architecture contains three modules

(1) Monitoring module
(2) Policy Module
(3) Arbitration module
(4) Provision module

1) Monitoring module:

Monitoring module keeps track of the executions of requests, the real-time configuration information , resource utilization, the health of CPU, memory, I/O.

2) Policy module:

Policy module establishes and maintains the healthcare strategies, the run-time and resource scheduling strategies. According to the data from monitoring module and the strategies of its own, policy module establishes specific solutions, and then triggers provision module.

3) Arbitration module:

Few of the Arbitration module policies are made by experts manually, requests from users are completed, and some disputes among various customers within the healthcare system are solved. Arbitration module adjusts, and improves the resource allocation and management. It also establishes usage modes for different kinds of users based on the heath conditions.

4) Provision module:

Provision module starts the execution of resource allocation solutions set by the policy module and arbitration module, and deploys resources referred to users automatically in a short time. If the request comes from a user, some related information such as IP, user name and password will be supplied.

V. How does the system work?

A local database about the patient needs to be maintained. When needed the user has to enter his/her symptoms into the cloud system. Based on this entry a notification will be sent to the patient and the appropriate doctor. Using the information obtained by the doctor, the required medication will be provided. Every step taken in response to the patient's condition will be updated in the cloud database.

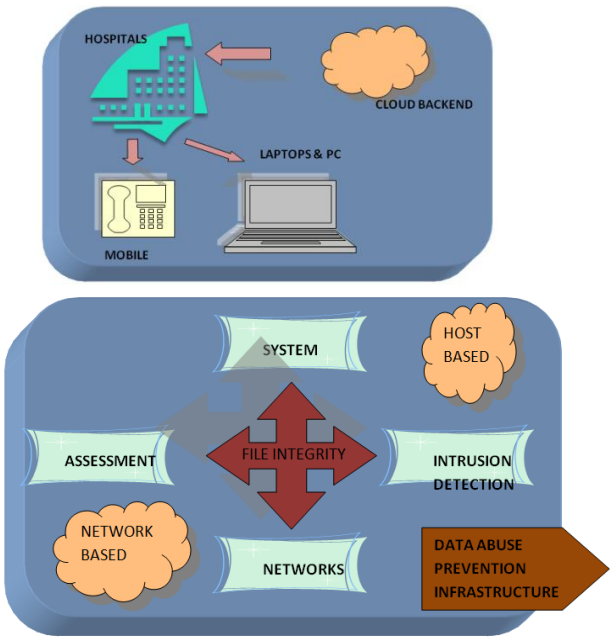

Fig. 3: Advantages of the cloud

VI. System with respect to healthcare

- Regular updates of the diagnosis will be supplied to the user through mobile methods.
- In case if medicine, home delivery can be done.
- Any kind of person can use this feature.
- The interface adapted is fully Graphical
- This system provides increased accuracy, efficiency and better communication among
- It has minimum errors
- The information is well secured.

VII. Risk compliance

Acquiescence requirements are becoming and a cloud provider who can meet these requirements and offer better fulfilment of the compliance can gain significant advantage. Compliance covers various procedures, from system logging, administrator authentication, data archiving, backups, and recovery along with server security. What is required is to develop a system that can make the cloud compliant, and that can guarantee the observance the individual customers satisfaction.

VIII. Data abuse

Data protection and data abuse prevention is traditionally handled using authorization, strong access control. By using Intrusion Detection and Data Leakage Prevention systems too the security is ensured. However, for reasons, the users of the clients must access a remote cloud using secure connections, making the use of existing systems difficult Thus, a solution that can share the traffic of the encrypted channels with the clients' IDS/DLP is highly beneficial. Depending on the type of access solutions that can record the actions of the users should be adapted. Some of the data problems in cloud computing technology are:

- Deletion/alteration of records without a backup
- unlinking a record from a larger context may make it unrecoverable,
- Loss of an encoding key result in destruction.
- Unauthorised parties may be allowed to access to sensitive data.

Data damage done by a malicious insider, such as a system administrator can be extremely rare but devastating than in a regular computing environment. Therefore, special precautions must be taken to prevent such damage. These precautions should include strong authentication and authorization, such as multifactor and 4-eyes solutions, and the rigorous recording and monitoring of the actions of the cloud administrators.

IX. A view from the network

Accessing systems across a network is a huge benefit for users sharing resources and modern Local Area Networks (LANs). Once Connected to the network the user is indulged to many activities inclusively: storage and transfer of data, and communications and remote environment working. This is in contrast to traditional standalone systems that rely on removable media devices for data transfer.

As network access is of the utmost importance to users of cloud computing losing the network is an extremely NOT desirable event.

E.G. When a communication is occurring between a customer and a business user, the loss of the network may impact business services, or directly impact the customer service satisfaction.

Addressing this issue and maintaining fully resilient network access is a difficult task for cloud providers. However it is possible for the cloud users who are external to connect to the network without been fully under the control of the cloud service provider. Therefore despite the provider having implemented and tested their incident recovery procedures, this does not preclude a network component beyond their perimeter.

X. Effective problem statement model

A. *System Model:*

Three different network entities can be identified in the given architecture:

- User:
  users, who have data to be stored in the cloudand rely on the cloud for data computation.
- Cloud Service Provider (CSP):

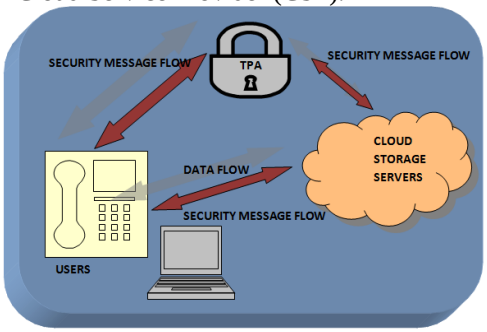

Fig. 4: Cloud Service Provider

a CSP, who has significant resources and expertise in building and managing distributed cloud storage servers.

– Third Party Auditor (TPA):

an optional TPA, who has expertise and capabilities that users may not have, is trusted to assess and expose risk of cloud storage services on behalf of the users upon request.
In cloud data storage, a user stores hisdata through a CSP into a set of cloud servers, which are running in a simultaneous, cooperated and distributed manner.
Data redundancy can be employed with technique of erasure-correcting code to further tolerate faults or server crash as user's data grows in size and importance. Thereafter, for application purposes, the user interacts with the cloud servers via CSP to access or retrieve his data. In some cases, the user may need to perform block level operations on his data. The most general forms of these operations we are considering are block update, delete, insert and append. As users no longer possess their data locally, it is of critical importance to assure users that their data are being correctly stored and maintained. In this model, we assume that the point-to point communication channels between each cloud server and the user is authenticated and reliable, which can be practice with little overhead.

B. Adversary Model:

Security threats faced by cloud data storage can come from two different sources. CSP can be self-interested, untrusted and possibly malicious. it desires to move data that has not been or is rarely accessed to a lower tier of storage. it may also attempt to hide a data loss incident. A part from this there may also exist an economically motivated adversary, who has the capability to compromise a number of cloud data storage servers in different time intervals and subsequently is able to modify or delete users' data while remaining undetected by CSPs for a certain period.

1) Weak Adversary:

The adversary is interested in corrupting the user's data files stored on individual servers. Once a server is comprised, an adversary can pollute the original data files

2) Strong Adversary:

This is the worst case scenario, in which we assume that the adversary can compromise all the storage servers so that he can intentionally modify the data files as long as they are internally consistent. In fact, this is equivalent to the case where all servers are colluding together to hide a data loss or corruption incident.

XI. Conclusion

In cloud data storage system, users store their data in the cloud and no longer possess the data locally. Thus, the correctness and availability of the data files stored on the distributed cloud servers must be guaranteed. Cloud computing infrastructure with effective detection of any unauthorized data modification and corruption allows for the stability, equilibrium, efficient resource use, and upholds cloud based healthcare system. Cloud based healthcare has been demonstrated to reduce cost and improve the quality of care for patients and hence a perfect implementation in future hospitals.

References

[1] Security in Cloud Computing Framework Based On Risk Assessments
Balakrishnan, Ramesh
[2] Ensuring Data Storage Security in Cloud Computing
Mr S.Azhad , Mr. S.Rao
[3] Computer Networks a systems Approach
Larry

