CHAPTER 1

INTRODUCTION

1.1 CLOUD COMPUTING

1.1.1 Introduction to Cloud Computing

Computing as a service has seen a phenomenal growth in recent years. The primary motivation for this growth has been the promise of reduced capital and operating expenses, and the ease of dynamically scaling and deploying new services without maintaining a dedicated compute infrastructure. Hence, cloud computing has begun to rapidly transform the way organizations view their IT resources. From a scenario of a single system consisting of single operating system and single application, organizations have been moving into cloud computing, where resources are available in abundance and the user has a wide range to choose from. Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with service provider interaction or minimal management effort. Here, the end-users need not to know the details of a specific technology while hosting their application, as the service is completely managed by the Cloud Service Provider (CSP). Users can consume services at a rate that is set by their particular needs. This on-demand service can be provided any time. CSP would take care of all the necessary complex operations on behalf of the user. It would provide the complete system which allocates the required resources for execution of user applications and management of the entire system

flow. Figure 1.1, depicts the graphical representation of the architecture of cloud computing [1].

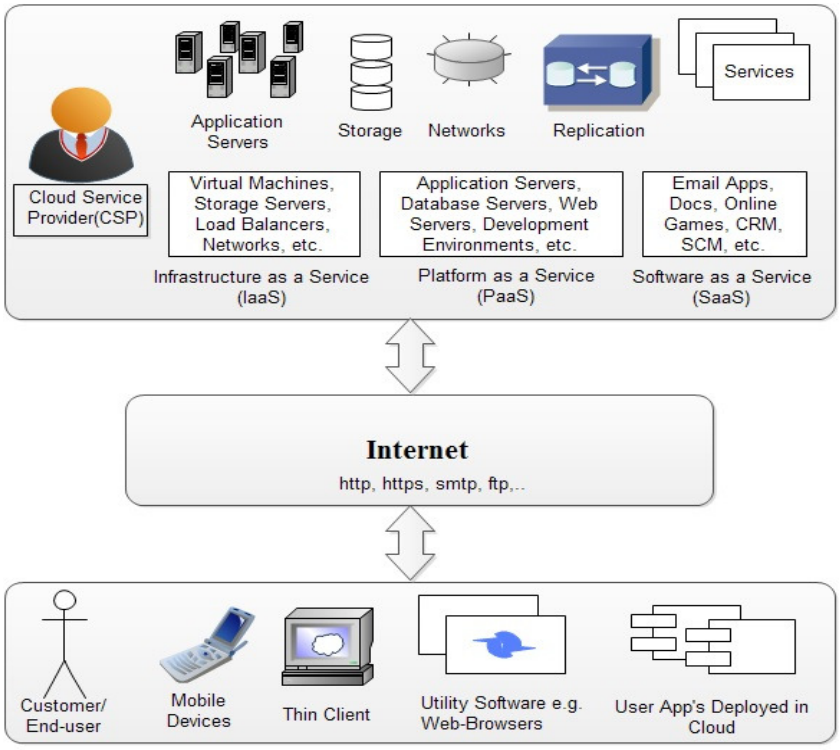

Fig. 1.1 Cloud Computing Architecture.

Additionally, this new model has gathered many proponents because of being labeled as a 'Greener Computing Alternative' [2]. Analysts say that pooling of resources and facilities can help cut significant costs for a company. In addition, this also has an extremely positive effect on the environment as an AT&T supported study posits [3]. By 2020, the group estimates, large US companies that use cloud computing can achieve annual energy savings of $12.3 billion and annual carbon reductions equivalent to 200 million barrels of oil.

Cloud vs. Grid

Cloud technology is a kind of grid computing model. It has evolved from grid computing by addressing the reliability problems and QoS (quality of service). Cloud computing provide the technologies and tools to compute intensive parallel applications with affordable prices when compared to traditional parallel computing techniques. Figure 1.2 illustrates the evolution of computing and communication technologies from 1960 to 2015.

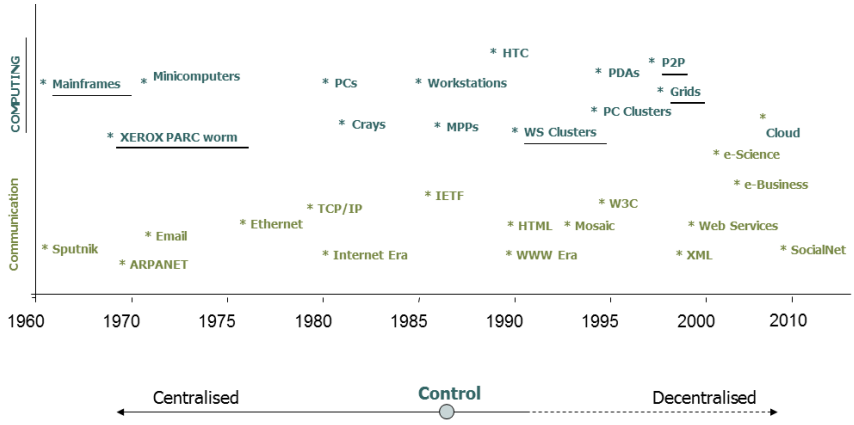

Fig. 1.2. Computing and Communication Technologies Evolution: 1960-2015.

There has been sources of confusion between grid computing and cloud computing. Clouds and grid have been sharing same visions: reduce computing cost, increase flexibility and reliability. But they differ in the following aspects.

- **Resource sharing:** Grid enhances the share of resources across organizations, whereas cloud provides the resources

based on demand of the user. There is no actual sharing due to isolation provided through virtualization.

- **Virtualization:** Grids has capability to virtualize the sum of parts into a singular wide-area resource pool. Virtualization covers both data (databases, flat files) and computing resources. In addition, cloud computing adds virtualization of hardware too.
- **Security:** Cloud Service User has unique access to its single virtualized environment, as virtualization is related to security, where Grid do not deal with end user security.
- **Coordination:** Grids need to perform the coordination of services workflow and location; whereas in clouds it is not necessary.
- **Scalability:** Grid scalability is mainly enabled by increasing the number of working nodes, whereas cloud resizes the virtualized hardware automatically.

Why Cloud Computing?

The best part of cloud computing is that it provides more flexibility than its previous counterparts. It has shown many benefits to enterprise IT world. Cost optimization among them is the frontrunner, since the principle of cloud is “pay as per use”. The other benefits are increased mobility, ease of use, utmost apt utilization of resources, portability of application, etc. This means users will be able to access information from anywhere at any time easily without wasting the underlying hardware resources ideal or unused. Due to its benefit, today’s computing technology has witnessed a vast migration of

organizations from their traditional IT infrastructure to cloud. Some of the noteworthy benefits are [Appendix A 1.1]:

- Cost Savings
- Remote Working
- Efficiency
- Flexibility
- Future Proofing
- Morale Boosting
- Resilience without Redundancy

1.1.2 Cloud Characteristics

- On Demand Self-services
- Broad Network Access
- Resource Pooling
- Rapid Elasticity
- Measured Service
- Dynamic Computing Infrastructure
- IT Service-centric Approach
- Minimally or Self-managed Platform
- Consumption-based Billing
- Multi Tenancy
- Managed Metering

Details are given in Appendix A 1.2.

1.1.3 Cloud Service Models

Figure 1.3 elucidates the cloud reference model given by Cloud Security Alliance (CSA) [4]. In general, there are three basic designs of cloud computing models as described below [Appendix A 1.3]:

- Infrastructure as a Service
- Platform as a Service
- Software as a Service

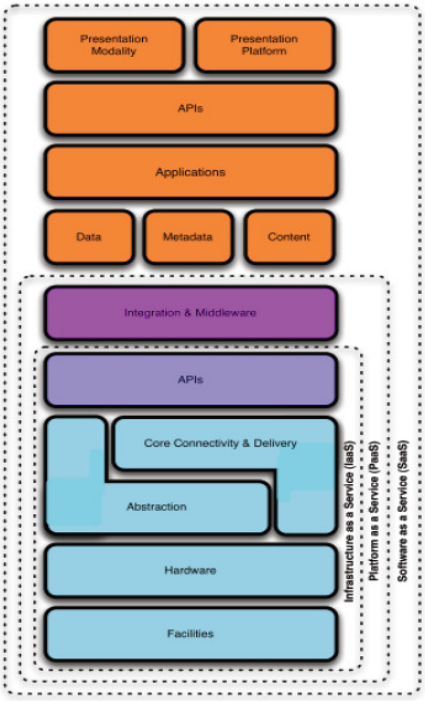

Fig. 1.3. Cloud Reference Model.

1.1.4 Cloud Deployment Models

- Public Cloud or External Cloud
- Private or Internal Cloud
- Hybrid Cloud

- Community Cloud

Details are given in Appendix A 1.4.

1.1.5 Virtualization and Hypervisor

Virtualization

Virtualization is the process of creating virtual format of resources like hardware, software, etc. In computing, it is termed as creation of virtual hardware resources, operating systems or network resources.

Virtualization is nothing but a software layer in between OS and host machine. It has a greater importance in cloud computing. By means of virtualization CSP's are able to create virtual machines in cloud computing. The applications are deployed in virtual machines so that it can be accessed from anywhere in the world in its virtualized form. The VM image is created, and when a user sends request for accessing a particular resource, the VM instance is created and access is provided. Users are allowed to access only the VM's that contains their applications or resources. Virtual machines are end point software layers and need to be protected in an efficient manner. This software layer divides the resources of the host machine among all the guest OS. The OS has no idea that it is being managed or not. The advantage of virtualization is that the CPU is shared among different OS. Multiplexing hardware resources to many OS is done by Virtualization Layer. Every OS would think that they are controlling the hardware but switching behind scenes is done by virtualization layer so that system can host many OS. With the help of Hypervisor, virtual machines are created and managed. Hypervisor is placed on top

of hardware which in turn will run multiple OS and applications in virtualized environment.

During virtualization, it is like single OS image per machine, even when there are Multiple OS running on machine. Due to the virtualization process the user will get a feeling he is working on single operating system. But actually a guest operating system will be running on the hypervisor by utilizing the underlying hardware resources of host operating system.

Different Types of Virtualization

The entire process of virtualization can be classified in to many forms based on the area and platform in which it is being applied. The following are the different formats of virtualization [Appendix A 1.5].

- Server (Hardware) Virtualization
- Client (Desktop) Virtualization
- Data Virtualization
- Application Virtualization
- Network Virtualization

Hypervisor

The concept of virtualization has become dominant over the past six years. There may be a number of issues arising regarding this virtualization and application access in its virtualized form. Most of the software vendors raised a compliant that their application is not supported in a virtual state or will not be supported if the end-user

decides to virtualize them. To accommodate the needs of the industry and operating environment, to create a more efficient infrastructure – virtualization process has been modified as a powerful platform, such that the process virtualization greatly revolves around one piece of very important software. This is called as hypervisor.

Hypervisor software is also called as Virtual Machine Monitor (VMM) or virtualization manager. The hypervisor can manage multiple instances of the same operating system on a single computer system. Hypervisor manages the system resources like the processor, memory, storage, etc. to get allocated to each operating system needs. Hypervisor makes the job easier by allowing multiple operating systems to run in a single CPU there by increasing the CPU utilization. Hypervisor takes care of the definition and management of virtual resources such that it always gives a solution for system consolidation. This software provides a convenient and efficient way to share resources amongst virtual machines which are running on top of the physical hardware. There are mainly two types of hypervisors [Appendix A 1.6].

- Type 1 Hypervisor
- Type 2 Hypervisor

1.1.6 Cloud Architecture

Cloud Architectural Models

The term cloud architecture or cloud computing architecture indicates the components and sub components which are required to implement a well-defined and efficient cloud computing set up. The architecture

consists of a front end platform, back end platform, a cloud based delivery and a network. These components also consist of sub components that together make up cloud computing architecture. The front end platform consist of fat client, thin client and mobile devices. The back end platforms include servers and storage. The architecture component network consists of an Internet or intranet [Appendix A 1.7].

- Front End Platforms
- Back End Platforms
- Cloud Based Delivery
- Cloud Networking

1.1.7 Advantages of Cloud Computing in the Current Scenario

- Cost Efficient
- Flexibility of Work Practices
- Collaboration Efficiency
- Access to Automatic Updates
- Reliability
- Scalability
- Business Continuity
- Innovation
- Multiple Users at One Time
- Customize Settings

Details are given in Appendix A 1.8.

1.2 PROBLEMS IN CLOUD COMPUTING

Cloud computing attracts users with its great elasticity and scalability of resources with an attractive tag line ‘pay-as-you-use’ at relatively low prices. Compared to the construction of their own infrastructures, customers are able to cut down on expenditure significantly by migrating computation, storage and hosting onto the cloud. Although this provides savings in terms of finance and manpower, it brings lots of new challenges and risks. Considering the influence of cloud computing with respect to its business benefits and technological transformations, the future enterprise applications are going to be completely dependent on it. It has its own benefits; nevertheless it has numerous issues and challenges [Appendix A 1.9].

- Data Integrity
- Data Theft
- Privacy Issues
- Infected Application
- Data Loss
- Data Location
- Security on Vendor Level
- Security on User Level

1.3 CLOUD SECURITY – A CURRENT SCENARIO

1.3.1 Security Scenarios

Cloud computing is a well-known technology nowadays. Companies like Amazon, Google and Microsoft are enhancing the services provided for their users. Security issue is a barrier for users to adapt into cloud systems. Cloud service providers have been concerned of the non-adequate security measures and aspects like data integrity, control, audit, confidentiality, availability should be added. Privacy acts which are in use are out of date and are not protecting the private information of user in the cloud environment since they are not applicable to three parties like cloud service user, cloud service provider, cloud provider. Privacy issue becomes worse when applications are in multiple locations. Cloud computing offers storage of data with scalable power of processing that elevated IT to newer limits with low capital expenditure. If one runs the application in public domain or beyond firewall then there arises security consciousness and concerns. In cloud computing the consumers can access resources online at any time through Internet without managing the original resources issues like physical and technical management. Cloud computing resources are scalable and dynamic. The significant difference in cloud security is enterprise control loss opposed to particular technical challenge. In cloud based application access control is important. The application of security, infrastructure and platform is under provider's control.

1.3.2 Regulations

It determines the functional requirements of security and not the technical issues. Other than technical issues in cloud computing, regulations is the harsh reality. The governments are concerned about the cloud computing for many reasons. The privacy laws are followed by many countries that prohibit the data which stores on physical machine located outside the country. The organizations are penalized for violating laws. In cloud if any organization stores sensitive data then the cloud provider should prove that it never stores data outside geographical area. Other than government agencies trade and industry groups create regulations. That regulation represents best practices. It is applicable to the applications which are running in the cloud. An application which is running on the virtual machine can access the sensitive data or not, this is not addressed by many countries. A new law is required for an organization to spend the resources which changes the application infrastructure than adding features to it.

1.3.3 Security Controls

Consumer needs all security controls which should not vary based on cloud provider that makes claims on security related issues and reassurances. For a secure system a number of controls are necessary.

- **Security Control Descriptions:**
  - **Asset Management:** To manage the hardware, network and software assets which make up the cloud infrastructure. This includes physical access of asset for audit.

  - **Cryptography (Key and Certificate Management):** Infrastructure for managing cryptographic keys are needed for a secure system. It includes employing cryptographic functions and services for information security.

- **Data Security:** The data is to be stored in encrypted format. The data of one consumer should be separated from other consumer.
- **Endpoint Security:** Consumers must secure the endpoints to the resources in the cloud. It includes restricted endpoints by device type and network protocol.
- **Event Auditing and Reporting:** Consumers must be able to access data about events happened in the cloud, especially security breaches and system failures. The access event includes the learning of past events and new events reporting. Cloud providers cause damage to their reputations when they fail in reporting events timely.
- **Identity, Roles, Access Control and Attributes:** It must be possible to define the entitlements, identity, roles and individual attributes and services in a machine-readable way and consistent in order to implement access control effectively and enforce security policy.
- **Network Security:** It must be possible to secure network traffic at the router, switch and packet level. The IP stack also should be secure.
- **Security Policies:** It must be possible to resolve, define policies and enforce policies of security in support of access control, resource allocation and other decisions in a machine readable and consistent way. The policies defining method

should be robust that licenses and SLAs can be automatically enforced.

1.3.4 Service Automation

There must be an automated way to analyze and manage control flows of security and processes in support of security audits. This includes reporting any events that violate any policies of security or agreements of customer license.

1.4 MOTIVATION FOR THIS RESEARCH WORK

In today's IT world, cloud computing has become a key factor for the technological transformation towards achieving the business goals through its extensive list of advantages. While demonstrating several advantages, cloud computing also has its potential risks and challenges on the other side.

Hence, in this research work, an attempt has been made focusing the resolution of problems involved in cloud computing, centering security issues with high priority. From the list of problems stated in section 1.2, this research work mainly focuses on the following issues:

- **Data Integrity:** When an organization deploys application(s) (i.e. application, database and other documents) onto cloud, predominantly databases will be highly affected by integrity issues. Hence, the proposed system handles this problem through log and database monitoring systems.

- **Data Theft and Data Loss:** The proposed solution is primarily based on its strong system auditor/monitor mechanism(s), and hence each and every activity performed on the host VM(s) is continuously monitored and taken into analysis in real-time. Hence, the chances of data theft and data losses can be controlled to a good extent.
- **Security on Vendor Level:** This research work is primarily designed to address the infrastructural security concerns of a cloud service provider by addressing the top three cloud computing security taxonomies [1]. Hence, the proposed security framework enhances the security features at vendor level, while bringing more confidence at user level.
- **Security on User Level:** In addition to the above fact, this research work is also focusing on real-time decision making at CSP location and updating the cloud user using a dedicated alert mechanism. Hence, the proposed solution provides a maximum confidence level and comfort factor for cloud users in deploying their application with CSP.

1.5 SUMMARY

Cloud computing is expressively leading today's IT enterprises towards achieving their business goals alongside providing utmost customer satisfaction with very lower cost with respect to infrastructure, platforms, and software perspectives. While these infrastructure-related hassles handled by a CSP, cloud service provider, organization needs to completely focus on the service to their customers. Being a user of cloud services from CSP, organizations need not have high technical potential with respect

infrastructure and platforms. Whereas, Cloud Service Users need to have expertise on the functionality provisioning/servicing based on their customer requirements. Alongside to its benefits, cloud computing is also comes with various challenges. Among all, security being a leading threat.

Hence, in this research work, an attempt has been made to influence further on to the problems mentioned in section 1.4; alongside designing a generic cloud security solution/framework.