Cloud Computing Models and Security Challenges
Saurabh Sindhu¹, Divya Sindhu²
Lecturer¹,²
Department of Computer Science
CRM Jat College, Hisar, Haryana, India

Abstract:
Cloud computing allows individuals and businesses to use software and hardware that are managed by third parties at remote locations. Cloud computing provides a platform with an enhanced and efficient way to store data in the cloud server with different range of capabilities and applications. Different cloud computing models allow access to information and computer resources from anywhere that a network connection is available. Cloud services include online file storage, social networking sites, webmail and online business applications. It provides a shared pool of configurable computing resources, including data storage space, networks, computer processing power and specialized corporate and user applications with minimal management effort or service provider interaction. Cloud computing has now become a highly demanded service or utility due to the advantages of high computing power, cheap cost of services, high performance, scalability, accessibility as well as availability. However, security of data has been a major and challenging aspect in the internet and network applications because the data is located in different places all over the world. The advantages of cloud computing will have low creditability if security is not robust and convenient. It could ultimately result in higher costs and potential loss of business. This paper describes different service and deployment models involved in cloud computing architecture along with security issues related to cloud computing.

Keywords: Cloud computing, Service models, Deployment models, Virtualization, Internet, Data security

I. INTRODUCTION
Cloud computing is one of the recently emerged technology that allows users to access infrastructure, storage, software and deployment environment [1]. IT cost reductions are achieved by offloading data and computations to cloud computing. Since the concept of cloud computing was proposed in 2006, cloud computing has been considered as the technology that probably drives the next-generation Internet revolution. The first generation cloud mainly focused on aggregating large-scale IT resources into a single cloud provider and providing users with well-managed, auto-provisioned resources and services, while increasing IT resource utilization through service consolidation. It offers improved scalability, elasticity, business agility, faster startup time, reduced management costs and just-in-time availability of resources. Cloud computing provides an easy way of accessing one’s personal file or data and use application without installing it on machines by just having Internet access. The server and the email management software is installed on the cloud and managed by service providers. Cloud services available today vary from data storage and processing to software provision, addressing requirements for high availability and on-demand commitment-free provision of services. The resource sharing at various levels results in various cloud offerings such as infrastructure cloud (e.g., hardware, IT infrastructure management), software cloud (e.g., SaaS focusing on middleware as a service or traditional CRM as a service), application cloud (e.g., Application as a Service, UML modeling tools as a service, social network as a service) and business cloud (e.g., business process as a service). Thus, cloud computing is based on several service models such as SaaS, PaaS, DbaaS, IaaS and many more. This cloud computing approach eliminates the client server and grid computing. Now a days, different companies, industries, corporations and organizations prefer cloud computing instead of investing high amount of money for acquiring the servers and professional staff for maintaining this server. In cloud computing, the companies just take services from the cloud service providers as per the requirement of companies [2]. It is a style of computing in which dynamically scalable and often virtualization resources are provided as a service over the internet. Cloud computing can be termed as a new paradigm for dynamic provisioning computer services supported by data centers that usually employ virtual machine (VM) technology for consolidation. With the globalization of the economy, the cross-border trade of commodities and services is continuously expanding, leading to the increasing interdependence of world economies. The economic globalization calls for globalized cloud services being provisioned in a geo-distributed manner at high availability and low cost. Therefore, a cloud vendor has to deploy data centers across all over the world. This is similar to the way used in early airline companies to expand their services by adding flight courses to a destination country to provide globalized flight courses. However, many cloud-enabled world businesses usually demand a burst of computation that exceeds the remaining computing capacity of a single cloud. Cloud Computing has widely been adopted by the industries or organizations though there are many existing issues like load balancing, virtual machine consolidation, energy management, etc. which have not been fully implemented. Central to these issues is the issue of load balancing that is required to distribute the excess dynamic local workload equally to all the nodes in the whole cloud to achieve a high user satisfaction [3]. Cloud vendors are experiencing appreciable growth rates in their business. Now-a-
days, Yahoo, Gmail, Amazon Rackspace, Google, Microsoft, VMware, iCloud, Drop Box etc. are good cloud service providers. Data storage and management is one of the most fundamental services offered by cloud providers [4]. Therefore, data security has become a challenging issue of data communications recently and is the main aspect of secure data transmission over unreliable network [5, 6]. Different systems are at risk in lack of data security, which include financial systems, utilities and industrial equipment, aviation, consumer devices, large corporations, automobiles, government official work and internet. As crackers troubled away at networks and computer systems, there is a need to protect that data against unauthorized access, alternation or interchanging [7, 8]. The cloud provider must ensure that their infrastructure is secure and their clients’ data and applications are protected, while the user must take measures to fortify their application and use strong passwords and authentication measures. The customers using a particular cloud, can access the resources provided by a cloud provider, according to the Service Level Agreement (SLA) given by the same cloud provider. Thus, security is considered as one of the most critical features for computer network due to sensitivity and importance of data stored.

II. ESSENTIAL CHARACTERISTICS OF CLOUD COMPUTING

Most cloud computing services are accessed through a web browser like Microsoft Internet Explorer, Microsoft Edge, Mozilla Firefox or Google Chrome. Certain cloud services could be used via a dedicated mobile app or through a browser on a smartphone or tablet. Therefore, cloud services don't require users to have sophisticated computers that can run specialized software. In a cloud-based computing infrastructure, the resources are normally in someone else's premise or network and accessed remotely by the cloud users [9, 10]. The users 'rent' it for the time they use the infrastructure [11]. Processing is done remotely implying the fact that the data and other elements from a person need to be transmitted to the cloud infrastructure or server for processing; and the output is returned upon completion of required processing. In some cases, it might be required or at least possible for a person to store data on remote cloud servers. A cloud-based constituent relationship management (CRM) database system is an alternative to running a donor database in your office. The essential characteristics of the cloud computing is as follows:

(i) On-demand self service: The end user can easily access various computing capabilities, such as server time and network storage, as needed without service provider in each service.

(ii) Broad network access: The end user’s over the network can access various standard mechanisms through various thin and thick client platforms such as mobiles, laptops, desktops and workstations.

(iii) Resource pooling: The service provider can provide various services and resources such as storage, processing, memory and network bandwidth using a multi-tenant model.

(iv) Rapid elasticity: Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.

(v) Measured service: Cloud computing provide, control and optimize resource by leveraging a measure at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth and active user accounts). Resources can be monitored, controlled and reported transparency for both the provider and consumer of the utilized service.

III. CLOUD COMPUTING INFRASTRUCTURE: SERVICE MODELS

Cloud service deals with web-fronted applications by using various languages java, php etc. Cloud infrastructure provides user the remote infrastructures and the web fronted application are further connected to the database i.e. cloud storage [12]. The cloud computing field is commonly categorized into four main layers. These layers vary slightly from one source to the next but they can generally be summarized as infrastructure as a service, platform as a service, software as a service and data as a service (Fig. 1).

(i) Infrastructure as a Service (IaaS)
IaaS is the foundation or bottom layer of cloud computing. It includes services like storage, backup and security. This model allows user to rent processing, storage, networks and other resources. The user can deploy a new user as a guest OS and applications. The user does not manage the complete cloud infrastructure but has the control over OS, storage, deployed applications and various network components. Some providers are Amazon EC2, GoGrid etc. IaaS users utilizes remote infrastructure, allows users to run any applications they want on cloud hardware of their own choice. While the advent of IaaS opened new territory for businesses to better manage IT hardware costs, it put developers in a challenging situation. Developers are now responsible for more of the operational work during development and test. They have to develop skills to provision, configure, manage and update hardware resources that they would have never needed in a traditional model. Amazon Web Services includes database, storage, virtual private server and support services that are available on demand by the user. Many SaaS applications rely on Amazon Web Services or other IaaS providers. Cloud-based Voice over Internet Protocol (VoIP) telephone service is another example of IaaS. Other examples are private cloud, dedicated hosting and hybrid hosting.

(ii) Platform as a Service (PaaS)
This model provides the user to deploy user built applications onto the cloud infrastructure that are built using programming languages and software tools supported by the provider. The user does not manage underlying cloud infrastructure. Platform as a Service provides platform to users to work on web application or software. It allows users to create own cloud applications using supplier-specific tools and language. The vendors of PaaS services provide a certain framework and a basic set of functions that customers can customize and use to develop their own applications. The capability provided to the consumer is to

http://ijesc.org/
deploy onto the cloud infrastructure consumer-created or acquired applications using programming languages, libraries, services and tools supported by the provider. The consumer does not control the underlying cloud infrastructure including network, servers, operating systems or storage but has control over the deployed applications and possibly configuration settings for the application-hosting environment. Examples of PaaS services include Google App Engine, Force.com from Salesforce and Microsoft Azure. In a PaaS environment, the service provider not only is responsible for provisioning and managing the lower level infrastructure resources, but also for providing a fully managed application development and deployment platform. PaaS provides the developers with the appropriate flavors of operating systems, databases, middleware, software tools and managed services, usually in a multi-tenant environment. The biggest added value of PaaS is that developers are completely abstracted from the lower-level details of the environment and they can fully focus on rapid development and deployment without any worry about things like scalability, security and more that are fully managed by PaaS. In Platform as a Service, the organizations or industries have to decide at which applications are most appropriate for maintenance on the cloud. It will obviously differ from organization to organization, taking care of the critical key missions or tasks to maintain on the cloud. For instance, a company that develops software for healthcare providers is going to have different needs than a financial advisor. But even within the same industry, different organizations/sections will get different things out of the cloud.

(iii) Software as a Service (SaaS)
It is browser initiated application software over thousands of cloud customers. In cloud, the customer need not invest in servers or software licensing. SaaS basically means any Internet-based software or service that you rent, usually on a per-user, per-month basis. It is the most common type of cloud service that small offices use. Web based application are those applications that are built using web languages like php, java, .net, etc. This model of cloud allows one to run existing online applications. The example is Google Docs. Some SaaS applications are highly customizable and we may even need a consultant to help set them up, but they generally don't require specialized knowledge for day-to-day operation and maintenance. In SaaS, an application is hosted by a service provider and then accessed via the World Wide Web by a client. Examples of SaaS include Microsoft Office 365, Google Apps, Salesforce and workstreams etc.

(iv) Data as a Service (DaaS)
The delivery of virtualized storage on demand becomes a separate Cloud service - data storage service and it 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 (relational data base management system) and file systems, some DaaS offerings provide table-style abstractions that are designed to scale out to store and retrieve a huge amount of data within a very compressed timeframe, often too large, too expensive or too slow for most commercial RDBMS to cope with. Examples of this kind of DaaS include Amazon S3, Google BigTable and Apache HBase etc.

Figure 1. the different layers of cloud computing. Cloud service provides software as a service, platform as a service, infrastructure as a service and data as a service

IV. CLOUD INFRASTRUCTURE: DEPLOYMENT MODELS

There are seven different types of cloud deployment models (Fig. 2) and the details of these various types of deployment models are given as follows:

(i) Public Cloud
The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed and operated by a business, academic or government organization or some combination of them. It exists on the premises of the cloud provider. A cloud infrastructure is managed by a third party and is provided to many customers, and which is beyond the firewall of the company. The infrastructure provided can be used by more than one enterprise at the same time and the resources can be provisioned by users dynamically. The cloud providers are responsible for the management, provisioning, installation and maintenance of the cloud. The cloud providers solely manage and host these clouds. The under usage of the resources are eliminated and the customers only pay for the resources they use. As the consumers have very less control over the infrastructure, processes require powerful security and regulatory compliance which are always not a good fit for public clouds. In this model, there are no restrictions applied on the access and authorization, and authentication techniques cannot
be used. Public cloud providers such as Google or Amazon offer an access control to their clients. Other examples of a public cloud include Microsoft Azure, Google App Engine.

(ii) **Private Cloud**
The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, rented, managed and operated by the organization itself or somebody not from the organization that is the third party, or some combination of them and it may exist on-premises or off-premises. When compared to the public cloud, it is more expensive and secure. Security regulations, legal requirements or bandwidth limitations are there in private cloud. There is control of the infrastructure and improved security at the end of cloud service providers and the clients have optimized the user's access and the networks used are restricted. One of the best examples of a private cloud is Eucalyptus Systems. This cloud system i.e., Eucalyptus is a third-party middleware. The middleware, as an overlay, invokes the implementation even more complicated. An example of a hybrid cloud includes Amazon Web Services.

(iii) **Hybrid Cloud**
The cloud infrastructure is a combination of two or more distinct cloud infrastructures (private, community or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability among the composing clouds e.g., cloud bursting for load balancing between clouds. It is a combination of two or more cloud deployment models, linked in such a way that data transfer takes place between the two different clouds without affecting each other. These clouds would typically be generated by the enterprise and responsibilities for management would be split amongst the enterprise and the cloud provider. In this model, a company can outline the goals and needs of services [14]. A well-constructed hybrid cloud can be useful for providing secure services such as receiving customer payments as well as those that are secondary to the business such as employee payroll processing. The major flaw in the hybrid cloud is the difficulty in creating and governing such a solution effectively. Services from different sources must be obtained and provisioned as if they originated from a single location and interactions between private and public components can make the implementation even more complicated. An example of a hybrid cloud includes Amazon Web Services.

(iv) **Community Cloud**
The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy and compliance considerations). It may be owned, managed and operated by one or more of the organizations in the community, a third party, or some combination of them and it may exist on premises or off premises. Infrastructure is shared by several organizations for a shared cause. These clouds are based normally on an agreement between business organizations which are related such as banking or educational organizations. A cloud environment operating according to this model may exist locally or remotely. An example of a community cloud includes Facebook.

(v) **JointCloud**
JointCloud is a recent key project funded by China’s Ministry of Science and Technology as a part of the National Key Program for Cloud Computing and Big Data, which borrows the ideas from airline alliances and aims at empowering the cooperation among multiple cloud vendors to provide cross-cloud services via software definition [15]. Prior efforts like SuperCloud and InterCloud focus on the fusion of cloud services, usually via a third-party middleware. The middleware, as an overlay, invokes different clouds and provides a uniform interface to end users. The clouds are actually unaware of the cooperation with other clouds. Different from existing multicloud models, JointCloud pays more attention to the direct collaboration among different clouds. It defines a series of rules and provides common services to enable collaboration among clouds. In JointCloud, clouds are independent while cooperating closely with one another. Just like global airline alliances Sky team and Star Alliance, there are many independent member airlines, and they work with one

---

**Figure 2. Diagrammatic representation of different cloud deployment models**

---

http://ijesc.org/
another closely. There are two different parts in the JointCloud architecture: the JointCloud collaboration environment (JCCE) and the peer collaboration mechanism (PCM). JCCE contains several block chain based services for enabling the cooperation among independent clouds. Based on JCCE, clouds can cooperate with one another, as long as these clouds implement a software-defined mechanism (named PCM) and provide related APIs.

(vi) Virtual Cloud
With the development of cloud computing, more and more users prefer to run their applications on clouds such as big data processing, high-performance computing and deep learning. However, users’ requirements cannot be directly satisfied by current cloud computing service model. IaaS (Infrastructure as a Service) cloud only provides users with resources such as servers, storages and networking. Users need to accomplish the environment installation with a complex configuration. In PaaS (Platform as a Service) cloud, users are provided with a cloud platform in which they can develop, manage and deliver limited applications, but they usually cannot customize the run time environment easily. Virtual cloud for special purposes is a service of JointCloud, which aims to provide end users with a specific cloud working environment upon several clouds just like grid computing [16], which is the collection of computer resources from multiple locations to reach a common goal. A cloud working environment has users’ readily available customized software stacks, configurations and computing resources. Users can develop, test and run tasks in their working environment online through a web browser. Such a working environment is built upon a customized virtual cloud, which provides the most suitable resources from underlying clouds for the working environment. This environment could span multiple clouds seamlessly and could help applications scale out to temporarily use new resources from outside parties to deal with peak load problems. Virtual cloud is designed to provide users with cheap, flexible and easy-to-manage working environment, which is supported by virtual clusters in cloud environment, to run their own tasks. The deployment of working environment is much easier than physical clusters because of the virtual cloud’s package mechanism [17]. Virtual cloud can wrap users’ working environment into a small package, which can be deployed upon multiple clouds and the package can be shared with other users so that newcomers with little cluster deployment experience can directly select a proper package and deploy it to their own working environment in minutes or even seconds. Then they can work on it just like on a well-configured physical cluster. On the other hand, virtual cloud has a powerful and easy-to-use web interface; thus users can conveniently manage their working environment, process tasks and view results through a web browser. Virtual cloud could automatically build, manage, migrate and optimize a working environment based on users’ requirement, by using software definition technology, making infrastructure transparent to users and scheduling resources to make a tradeoff between the quality and the cost.

(vii) Multi Cloud
Multi-Cloud denotes the usage of multiple and independent clouds by a client or a service [18]. It does not imply interconnection and sharing between clouds. The clients or their software representatives are responsible for managing resource provisioning. The selection of the best fitted place to deploy a cloud application is a complex technical issue in a Multi-Cloud that requires the introduction of a cloud resource management layer based on vendor-independent brokers and semi-automated tools (including knowledge-based selection methods for cloud services). Such a resource management system should be able to hide the complexity of service selection procedures and to control the life-cycle of the resources and services allocated to a certain application.

V. VIRTUALIZATION OF RESOURCES IN THE CLOUD
Virtualization is the creation of a virtual (rather than actual) version of something, such as an operating system, a storage device, an application or network resources [19]. From an enterprise perspective, virtualization offers data center consolidation and improved IT operational efficiency.

Today, enterprises have deployed virtualization technology within data centers in various forms, including OS virtualization (VMware, Xen), storage virtualization (NAS, SAN), database virtualization and application or software virtualization (Apache Tomcat, JBoss, Oracle App Server, Web Sphere). IaaS providers including Amazon (EC2) and Sun Cloud employ OS virtualization, which enables customers to run instances of various operating system flavors in a public cloud. In addition to OS and storage virtualization, Saas and PaaS service providers are known to have implemented software and database resources. For example, Salesforce.com is known to have virtualized both the software and the database stack. There are five most common reasons to virtualize resources [20].

- **Sharing**: When a resource is too big for a single user, it is best to divide it into multiple virtual pieces, as is the case with today’s multi-core processors. Each processor can run multiple virtual machines (VMs) and each machine can be used by a different user. The same applies to high-speed links and large-capacity disks.

- **Isolation**: Multiple users sharing a resource may not trust each other, so it is important to provide isolation among users. Users using one virtual component should not be able to monitor the activities or interfere with the activities of other users. This may apply even if different users belong to the same organization since different departments of the organization (e.g., finance and engineering) may have data that is confidential to the department.

- **Aggregation**: If the resource is too small, it is possible to construct a large virtual resource that behaves like a large resource. This is the case with storage, where a large number of inexpensive unreliable disks can be used to make up large reliable storage.

- **Dynamics**: Often resource requirements change fast due to user mobility and a way to reallocate the resource quickly is required. This is easier with virtual resources than with physical resources.

- **Ease of management**: The most important reason for virtualization is the ease of management. Virtual devices are
VI. ISSUES IN CLOUD COMPUTING

More and more information on individuals and companies is placed in the cloud. Concerns are beginning to grow about safety and security of the cloud environment [21]. Issues of cloud computing can be summarized as follows:

(i) Privacy: Cloud computing utilizes the virtual computing technology and users’ personal data may be scattered in various virtual data centers rather than stay in the same physical location. Users may leak hidden information when they access cloud computing services. Attackers can analyze the critical task depending on the computing task submitted by the users.

(ii) Reliability: The cloud servers also experience downtimes and slowdowns as our local server.

(iii) Legal issues: Worries stick with safety measures and confidentiality of individual all the way through legislative levels.

(iv) Compliance: Numerous regulations pertain to the storage. Use of data requires regular reporting and audit trails. In addition to the requirements to which customers are subject, the data centers maintained by cloud providers may also be subject to compliance requirements.

(v) Freedom: Cloud computing does not allow users to physically possess the storage of the data, leaving the data storage and control in the hands of cloud providers.

VII. SECURITY ISSUES IN CLOUD COMPUTING

Security of cloud is considered to be the most critical point and the location of the data is a major issue in the security of cloud computing. Cloud users personal data security is thus a concern in a cloud computing environment [22, 23]. The strategic policies of the cloud service provider are of highest significance [24] as the technical security solely is not adequate to address the problem. Trust is another issue which is raised for the security concerns to use cloud service [25] because it is directly related to the authenticity and credibility of cloud computing environment. The attacks on the computer networks and the data in transit equally applies to cloud based services such as phishing, eavesdropping, sniffing and other similar attacks. DDoS (Distributed Denial of Service) attack is one common yet major attack for cloud computing infrastructure [26]. The security of the virtual machine will define the integrity and level of security of a cloud environment to greater extent. Thus, security concern involves some type of risk in the cloud computing infrastructure and it may lead to security vulnerabilities situation eventually. Any security tools or any other kind of software that are used in a cloud environment might have loopholes in security, which would pose the security risks in the infrastructure of cloud itself. Data security covers a variety of computer networks, both public and private, that are used in everyday jobs conducting transactions and communications among organizations, enterprises and other types of institutions, businesses, government agencies and individuals [27]. Storing of data on remote cloud servers gives the following three sensitive states that are of particular concern within the operational context of cloud computing: (i) the transmission of personal sensitive data to the cloud server, (ii) the transmission of data from the cloud server to clients’ computers and (iii) the storage of clients’ personal data in cloud servers which are remote server not owned by the clients. All the above three states of cloud computing are severely prone to security breach that makes the research and investigation within the security aspects of cloud computing practice. Data storage and security has become a challenging issue of cloud computing recently and therefore, security is considered as one of the most critical features for computer network due to sensitivity and importance of data stored [28]. Data security involves many areas including secure communication channel, strong data encryption technique and trusted third party to maintain the database [29]. As crackers troubled away at networks and computer systems, there is a need to protect that data against unauthorized access, alternation or interchanging [30]. The cloud provider must ensure that their infrastructure is secure and their clients’ data and applications are protected, while the user must take measures to fortify their application and use strong passwords and authentication measures. The conventional methods of encryption are employed to maintain the data security [31]. Network security starts with authenticating the user, commonly with a username and a password, this is sometimes termed one-factor authentication. With two factor authentication, a security token or ‘dongle’, an ATM card or a mobile phone is used [32, 33]. With three-factor authentication, a fingerprint or retinal scan is used. Once authenticated, firewall forces access policies such as what services are allowed to be accessed by the network users. An anomaly based intrusion detection system may also monitor the network and traffic for suspicious content or behaviour and other anomalies to protect resources, e.g. from denial of service attacks or an employee accessing files at strange times. Due to the multi-tenancy arrangement of cloud services, the security challenge is much more difficult. Although, there are many security and privacy frameworks being developed and implemented, none offers a complete security and privacy solution. The initial reaction of the community to the security issues of cloud computing was that these could be resolved using existing techniques inherited from conventional IT systems or even distributed systems that are the ancestors of cloud computing environments [34]. Given the number of systems now dependent on cloud implementations, including the rapidly evolving Internet of Things (IoT) and Big Data, this is rather concerning. Legislative and regulatory bodies have taken notice of the adverse impact of security and privacy breaches on companies, individuals and society as a whole, and these agencies are proposing to levy higher punitive fines on companies who suffer such breaches. Accountability from all the users involved in cloud ecosystems is often aided by service level agreements. The cloud service provider should take a robust attitude to vetting all staff, but this level of rigor may not apply to sub-contractors. The threat environment is often not well understood by companies, sometimes resulting in a far less robust approach to the risks involved. Even though cloud computing has found versatile ground as an economic model and is attracting a lot of investment; many are still reluctant to use cloud services because
of several security, privacy and trust issues that have emerged. Hence, a need to re-consider security, privacy and trust concerns in the context of the cloud computing paradigm arises.

VIII. CONCLUSION

Cloud computing provides a platform with an enhanced and efficient way to store data in the cloud server. Cloud computing is a compilation of existing technologies packaged within a new infrastructure and it refers to the sustained storage and sharing of data over the internet. Recently, cloud computing has received increasing interest from various industry professionals and enterprises. Enterprise businesses are moving their IT services, applications and infrastructure to cloud-based architecture. Big businesses and even smaller operations use specific cloud computing services to make different processes like supply-chain management, inventory handling and customer relationships. Cloud computing allows the other users to store the data privately as per their requirements. However, the security threats embedded in cloud computing approach are directly proportional to its offered advantages. Every person who accesses the internet does not use the applications of cloud properly. Thus, the threats to the cloud computing and its security creates the doubt in user’s mind to use and rely upon the services being provided. Therefore, security issues in cloud computing are crucial on the basis of sociological and technological viewpoints. Recently, new security techniques are being developed to reduce the risks in cloud computing. But, still there are many more hindrances and computational problems that might occur in the coming future. More work has to be done to support cloud computing and for understanding the challenges regarding security issues in cloud.

IX. REFERENCES


