Research And Challenges For Cloud Computing Security Issues

M.NAVEEN REDDY, D.SREEKANTH, V.HARSHAVARDHAN

Abstract -In this paper publisher accomplish about cloud computing architecture for providing computing service via internet is called the cloud computing and on demand pay per user access to a pool of shared resources namely networks, storage, servers, services and applications, without physically acquiring them. There are three Verities of services like.(saas, paas, iass). Business organizations, private, public organizations and also government sectors, healthcare, entertainment, educational organizational moving towards the cloud computing the main thing is cloud computing saves the cost, efficiency and it saves the time. Cloud computing totally depends on internet without having internet cloud computing is impossible to access data from the cloud. Data is organized and maintained and stored in data centers, cloud providers like, Google, Amazon, Salesforce.som and Microsoft etc. There are various research challenges also there for adopting cloud computing such as well managed service level agreement (SLA), privacy, interoperability and reliability. The major security thread is which include data leakage insecure interface, sharing of resources data maintainability and availability and inside attack or limited and it controls over the data incur. this paper analysis key researches and challenges and presents in cloud computing comprises to improve their bottom line in this service economic in this paper analysis key researches and challenges and presents in cloud computing comprises to improve their bottom line in this service economic nature.

Index Terms— Security Issues, Cloud Security, Cloud Architecture, Data Protection, Cloud Platform, Grid Computing.

1 INTRODUCTION

Cloud computing is a distributed architecture that centralizes server resources on a scalable platform so as to provide on demand computing resources and services. cloud computing is a type of Internet-based computing that provides shared computer processing resources and data to computers and other devices on demand. It is a model for enabling ubiquitous, on-demand access to a shared pool of configurable computing resources (e.g., computer networks, servers, storage, applications and services), Cloud computing relies on sharing of resources to achieve coherence and economy of scale, similar to a utility (like the electricity grid) over an electricity network. Advocates claim that cloud computing allows companies to avoid upfront infrastructure costs (e.g., purchasing servers). As well, it enables organizations to focus on their core businesses instead of spending time and money on computer infrastructure. Cloud computing and storage provides users with capabilities to store and process their data in third-party data centers Organizations use the cloud computing. Cloud computing is a computing paradigm, where a large pool of systems are connected in private or public networks, to provide dynamically scalable infrastructure for application, data and file storage. Cloud service providers (CSP's) offer cloud platforms for their customers to use and create their web services, much like internet service providers offer costumers high speed broadband to access the internet. CSPs and ISPs (Internet Service Providers) both offer services. There are typically three major offerings that sum up cloud computing services. The three are Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). In most cases, the 'layers' of cloud computing are represented as a pyramid with IaaS at the bottom, PaaS at the middle and SaaS sits at the topCloud computing providers deliver common online business applications which are accessed from servers through web browser.

- *M Naveen Reddy is currently pursuing Master of ComputerApplications on KMM Institute of PG studies in S.V University, Anhdra Pradesh, PH-7893502718. E-mail: naveenreddy15151@gmail.com*
- *D Sreekanth is currently pursuing Master of Computer Applicationson KMM Institute of PG studies in S.V University, Andhra Pradesh , PH-8790252094. E-mail: dsreekanth381@gmail.com*
- *Vemuri Harsha vardhan is currently working as Assistant Professor in KMM Institute of PG studies in S.V University, Andhra Pradesh. PH-9959974091.*
  Email: vemuriharsha@gmail.com

II. CLOUD COMPUTING BUILDING BLOCKS

❖ Different models of cloud computing

These cloud computing services can be broadly classified into three categories: 1) Software as a Service (SaaS), 2) Platform as a Service (PaaS), and 3) Infrastructure as a Service (IaaS).

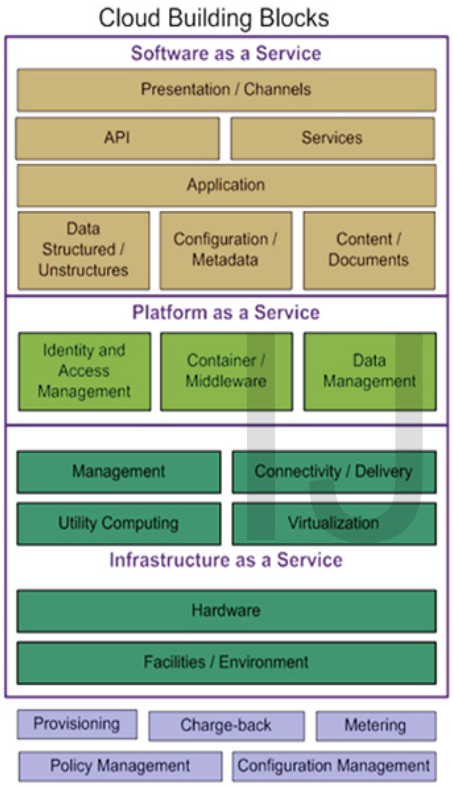
Software as a Service (SaaS): This is the cloud computing layer most people have interacted with and are likely to use in their day to day lives. Software as a service is where computing applications are accessed through the internet; this eliminates the need to download, install and run applications on local computers. In most cases, these applications are managed by a third party vendor.

A good example of SaaS is Google docs; if you don't have MS Office installed on your computer, you can use Google docs to create and edit documents. Most SaaS applications are either free to use or require some form of subscription.

Platform as a Service (PaaS): A platform is a software environment used to develop and run applications. So Platform

as a Service (PaaS) can be defined as a computing platform that enables the creation, testing and implementation of software easily and quickly without the complexities of buying and maintaining the infrastructure and additional software. Unlike SaaS which is software delivered via the internet, PaaS provides a platform for creation of applications over the internet. Another difference between PaaS and SaaS is the aspect of management. In PaaS, the vendors manage networking, storage, servers, virtualization, OS, middleware and runtime, but the end users are the ones who manage the data and applications.

A good example of a Public (IaaS) offering is Amazon Web Services Cloud computing (EC2), Amazon S3, Go Grid.



Infrastructure as a Service (IaaS): Infrastructure as a service (IaaS) refers to the sharing of hardware resources for executing services using Virtualization technology. Its main objective is to make resources such as servers, network and storage more readily accessible by applications and operating systems. Thus, it offers basic infrastructure on-demand services and using Application Programming Interface (API) for interactions with hosts, switches, and routers, and the capability of adding new equipment in a simple and transparent manner. In general, the user does not manage the underlying hardware in the cloud infrastructure, but he controls the operating systems, storage and deployed applications. Examples of IaaS includes Amazon Elastic Cloud Computing (EC2), Amazon S3, GoGrid.

There are also four different cloud deployment models namely Private cloud, Public cloud, Hybrid cloud and Community cloud. Details about the models are given below.

Private cloud: Private clouds are built exclusively for a single enterprise. They aim to address concerns on data security and offer greater control, which is typically lacking in a public cloud on-premises or off-premises. In private cloud there are no additional security regulations, legal requirements or bandwidth limitations that can be present in a public cloud environment, by using a private cloud, the cloud service providers and the clients have optimized control of the infrastructure and improved security, One of the best examples of a private cloud is Eucalyptus Systems.

Public Cloud: Public clouds are owned and operated by third parties; they deliver superior economies of scale to customers, as the infrastructure costs are spread among a mix of users, giving each individual client an attractive low-cost, "Pay-as-you-go" model. All customers share the same infrastructure pool with limited configuration, security protections, and availability variances. These are managed and supported by the cloud provider. One of the advantages of a Public cloud is that they may be larger than an enterprises cloud, thus providing the ability to scale seamlessly, on demand. Examples of a public cloud includes Microsoft Azure, Google App Engine.

Hybrid Cloud: Hybrid Clouds combine both public and private cloud models. With a Hybrid Cloud, service providers can utilize 3rd party Cloud Providers in a full or partial manner thus increasing the flexibility of computing. The Hybrid cloud environment is capable of providing on-demand, externally provisioned scale. The ability to augment a private cloud with the resources of a public cloud can be used to manage any unexpected surges in workload. An example of a Hybrid Cloud includes Amazon Web Services (AWS).

Community Cloud: Infrastructure shared by several organizations for a shared cause and may be managed by them or a third party service provider and rarely offered cloud model. These clouds are normally based on an agreement between related business organizations 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, etc.

III. CLOUD COMPUTING SECURITY ARCHITECTURE

The **Cloud Computing Architecture** is the configuration of the system that involves local and cloud resources, services, middleware and software, cloud clients and cloud storages, networks, geo-location. Note that the Cloud Computing Architecture is based on the needs of the end-user - the cloud consumer and describes how all these components are arranged and related. For documenting the Cloud Computing Architecture with a goal to facilitate the communication between stakeholders are successfully used the Cloud Computing Architecture diagrams. Each Cloud Computing Architecture diagram visually depict cloud components and relationships between them.

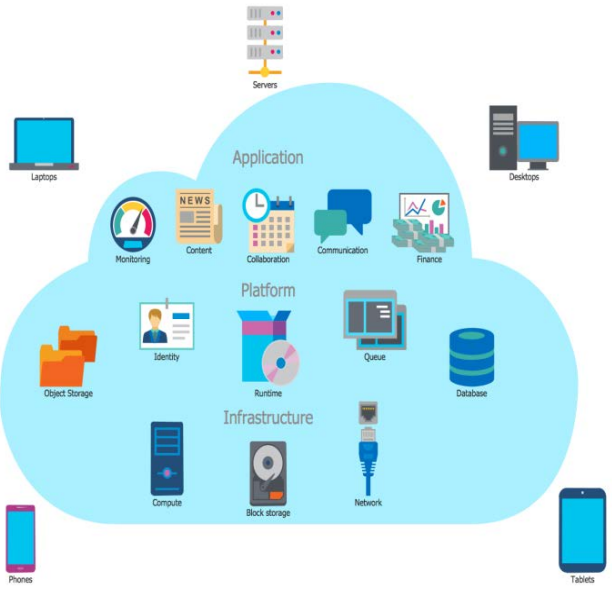
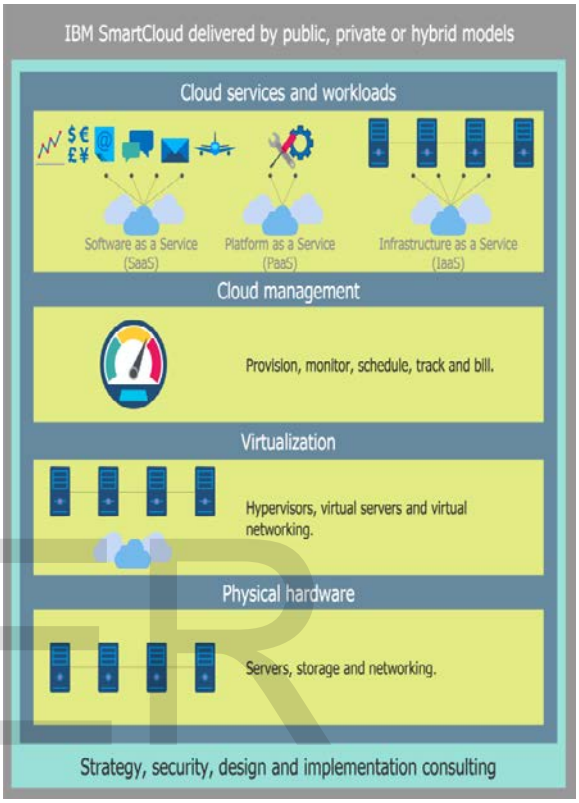


Fig-1: Cloud Computing Architecture Diagram

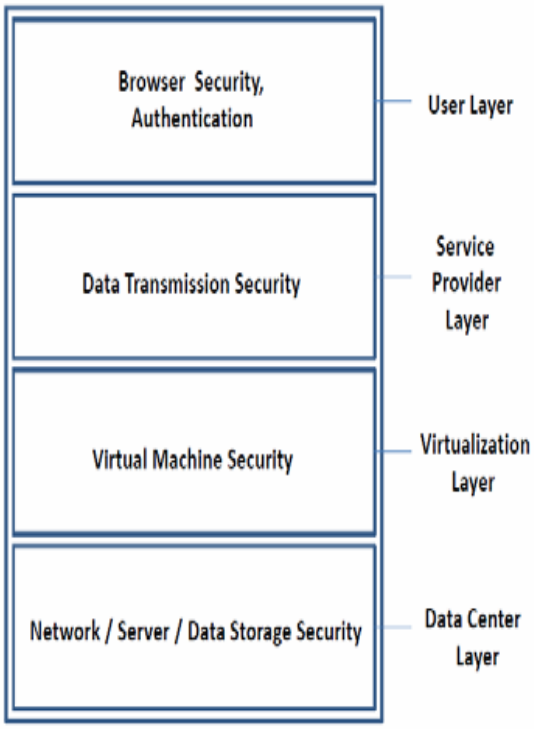
It is convenient and easy to draw various Cloud Computing Architecture diagrams in Concept Draw PRO software with help of tools of the Computer and Networks Area of Concept Draw Solution Park.

We have defined four layers based on cloud computing services categorization. The cloud computing categorization based on services as Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS). This section elaborates the four layers shown in figure and mapping the different security issues in each layer. Some of the important components of User layer are Cloud Applications, Programming, Tools and Environments. Some of the popular examples for these applications are B2B, Face Book, MySpace, Enterprise, ISV, Scientific, CDNs, Web 2.0 Interfaces, Aneka, Mashups, Map Reduce, Hadoop, Dryad , Workflows, Libraries, Scripting. Some of the security issues related to the user layer are Security as a Service, Browser Security, and Authentication as elaborated in next sections. Security within cloud computing is an especially worrisome issue because of the fact that the devices used to provide services do not belong to the users themselves. The users have no control of, nor any knowledge of, what could happen to their data. This is a great concern in cases when users have valuable and personal information stored in a cloud computing service.

Some organizations have been focusing on security issues in the cloud computing. The Cloud Security Alliance is a non-profit organization formed to promote the use of best practices for providing security assurance within Cloud Computing, and provide education on the uses of Cloud Computing to help secure all other forms of computing. The Open Security Architecture (OSA) is another organizations focusing on security issues. They propose the OSA pattern, which pattern is an attempt to illustrate core cloud functions, the key roles for oversight and risk mitigation, collaboration across various internal organizations, and the controls that require additional emphasis. System and Services Acquisition is crucial to ensure that acquisition of services is managed correctly. Contingency planning helps to ensure a clear understanding of how to respond in the event of interruptions to service delivery.



The Risk Assessment controls are important to understand the risks associated with services in a business context. National Institute of Standard and Technology (NIST), USA (http://www.nist.gov/) has initiated activities to promote standards for cloud computing. Cloud management has multiple aspects that can be standardized for interoperability. Some possible standards are Federated security (e.g., identity) across clouds, Metadata and data exchanges among clouds, Standardized outputs for monitoring, auditing, billing, reports and notification for cloud applications and services, Cloud-independent representation for policies and governance etc., showing the high level view of the cloud computing security architecture.



High Level Security Architecture of Cloud Computing

IV. KEY SECURITY ISSUES IN CLOUD COMPUTING

Cloud computing consists of applications, platforms and infrastructure segments. Each segment performs different operations and offers different products for businesses and individuals around the world. The business application includes Software as a Service (SaaS), Utility Computing, Web Services, Platform as a Service (PaaS), Managed Service Providers (MSP), Service Commerce and Internet Integration. There are numerous security issues for cloud computing as it encompasses many technologies including networks, databases, operating systems, virtualization, resource scheduling, transaction management, load balancing, concurrency control and memory management. Therefore, security issues for many of these systems and technologies are applicable to cloud computing. For example, the network that interconnects the systems in a cloud has to be secure and mapping the virtual machines to the physical machines has to be carried out securely. The given below are the various security concerns in a cloud computing environment.

- Access to Servers & Applications
- Data Transmission
- Virtual Machine Security
- Network Security
- Data Security
- Data Privacy
- Data Integrity
- Data Location
- Data Availability
- Data Segregation
- Security Policy and Compliance
- Patch management

Access to Servers & Applications: Now we are using datacenters, An administrative has access to servers are controlled and restricted to direct connections. which is not the case of cloud data centers. In cloud computing administrative access must be conducted via the Internet, increasing exposure and risk. It is extremely important to restrict administrative access to data and monitor this access to maintain visibility of changes in system control. The security policies may entitle some considerations wherein some of the employees are not given access to certain amount of data. These security policies must be adhered by the cloud to avoid intrusion of data by unauthorized users. Most companies are storing their employee information in some type of Lightweight Directory Access Protocol (LDAP) servers. In the case of SMB companies, a segment that has the highest cloud application adoption rate, Active Directory (AD) seems to be the most popular tool for managing users. With cloud application, the software is hosted outside of the corporate firewall. cloud application providers can provide delegate the authentication process to the customer's internal LDAP/AD server, so that companies can retain control over the management of users. Large enterprises, the management of user's account as the adoption of single sign on (SSO) or each employee will be dispatched some different accounts to access different systems.

Data Transmission: In the data transmission we are using encryption techniques. To provide the protection for data only goes where the customer wants it to go by using authentication and integrity and is not modified in transmission. In Cloud environment most of the data is not encrypted in the processing time. To provide the confidentiality and integrity of data-in-transmission to and from cloud provider by using access controls like authorization, authentication, auditing for using resources, and ensure the availability of the Internet-facing resources at cloud provider. Man-in-the-middle attacks is cryptographic attack is carried out when an attacker can place themselves in the communication's path between the users. Here, there is the possibility that they can interrupt and change communications.

Virtual Machine Security: Cloud is having one of the main component is Virtualization. The Virtual machines are dynamic, So it can quickly be reverted to previous instances, paused and restarted, relatively easily. Ensuring that different instances running on the same physical machine are isolated from each other is a major task of virtualization. They can also be readily cloned and seamlessly moved between physical servers. This dynamic nature and potential for VM sprawl makes it difficult to achieve and maintain consistent security. VMM (Virtual Machine Monitor), is a software layer that the physical resources used by the multiple virtual machines this is a I/O devices, storage, memory, etc. Many bugs have been found in all popular VMMs that allow escaping from Virtual machine. Virtual machine monitor should be 'root secure', meaning that no privilege within the virtualized guest environment permits interference with the host system.

Network Security: The Networks are classified into many

types, They are shared and non-shared, public or private, small area or large area networks and each of them have a number of security threats to deal with. Problems associated with the network level security comprise of DNS attacks, Sniffer attacks, issue of reused IP address, etc which are explained in details as follows.

A Domain Name Server (DNS) server performs the translation of a domain name to an IP address. But there are cases when having called the server by name, the user has been routed to some other evil cloud using IP address is not always feasible.

Data security: The cloud computing is provided to the data security. It is says to For general user, it is quite easy to find the possible storage on the side that offers the service of cloud computing. To achieve the service of cloud computing, the most common utilized communication protocol is Hypertext Transfer Protocol (HTTP). In a traditional on-premise application deployment model, the sensitive data of each enterprise continues to reside within the enterprise boundary and is subject to its physical, logical and personnel security and access control policies.

Data Privacy: In The cloud computing having data privacy is also one of the key concerns. A privacy steering committee should also be created to help make decisions related to data privacy. Data in the cloud is usually globally distributed which raises concerns about jurisdiction, data exposure and privacy. Organizations stand a risk of not complying with government policies as would be explained further while the cloud vendors who expose sensitive information risk legal liability. Virtual co-tenancy of sensitive and non-sensitive data on the same host also carries its own potential risks.

Data Integrity: Data integrity is known as the corruption can happen at any level of storage and with any type of media, So Integrity monitoring is essential in cloud storage which is critical for any data center. Most databases support ACID transactions and can preserve data integrity. Data generated by cloud computing services are kept in the clouds. Keeping data in the clouds means users may lose control of their data and rely on cloud operators to enforce access control.

Data Location: The data location is a data will be storing area. In general, cloud users are not aware of the exact location of the datacenter and also they do not have any control over the physical access mechanisms to that data. Most well-known cloud service providers have datacenters around the globe. For example, in many EU and South America countries, certain types of data cannot leave the country because of potentially sensitive information. In this system are multiple database and several applications.

Data Availability: Data availability is one of the prime concerns of mission and safety critical organizations. When keeping data at remote systems owned by others, data owners may suffer from system failures of the service provider. If the Cloud goes out of operation, data will become unavailable as the data depends on a single service provider. This involves making architectural changes at the application and infrastructural levels to add scalability and high availability. At the same time, an appropriate action plan for business continuity (BC) and disaster recovery (DR) needs to be considered for any unplanned emergencies.

Data Segregation: The cloud largely data can be shared together from one to another customer. Encryption cannot be assumed as the single solution for data segregation problems. In some situations, customers may not want to encrypt data because there may be a case when encryption accident can destroy the data. Make sure that encryption is available at all stages, and that these encryption schemes were designed and tested by experienced professionals.

Security Policy and Compliance: This services are provides to external security certifications. The Enterprises are experiencing significant pressure to comply with a wide range of regulations and standards such as PCI, HIPAA, and GLBA in addition to auditing practices such as SAS70 and ISO. Enterprises need to prove compliance with security standards, regardless of the location of the systems required to be in scope of regulation. An organization implements the Audit and compliance to the internal and external processes that may fallow the requirements classification with which it must stand and the requirements are customer contracts, laws and regulations, driven by business objectives, internal corporate policies and check or monitor all such policies, procedures, and processes are without fail.

Securing Data-Storage: Data protection is the most important security issue in Cloud computing. In the service provider's data center, protecting data privacy and managing compliance are critical by using encrypting and managing encryption keys of data in transfer to the cloud. Encryption keys share securely between Consumer and the cloud service provider and encryption of mobile media is an important and often overlooked need. The cloud-wide data classification will govern how that data is encrypted, who has access and archived, and how technologies are used to prevent data loss. At the cloud provider, Self-encrypting provides automated encryption with performance or minimal cost impact.

Patch Management: The self-service nature of cloud computing may create confusion for patch management efforts. Once an enterprises subscribes to a cloud computing resource—for example by creating a Web server from templates offered by the cloud computing service provider—the patch management for that server is no longer in the hands of the cloud computing vendor, but is now the responsibility of the subscriber.

V. RESEARCH CHALLENGES IN CLOUD COMPUTING

Cloud Computing research addresses the challenges of meeting the requirements of next generation private, public and hybrid cloud computing architectures; and the challenges of allowing applications and development platforms to take advantage of the benefits of cloud computing.

In the list of challenges in full potential of cloud computing. I organized the challenges in the following six different categories.

- Service Level Agreements (SLA's)
- Cloud Data Management & Security
- Data Encryption

- Interoperability
- Access Controls
- Energy Management
- Server Consolidation
- Reliability & Availability of Service
- Common Cloud Standards

Service Level Agreements (SLA's): The Cloud is administrated by service level agreements. It's the multiple instances of the application to be replicated on if you need arises. A big challenge for the Cloud customers is to evaluate SLAs of Cloud vendors. Most vendors create SLAs to make a defensive shield against legal action, while offering minimal assurances to customers. So, there are some important issues, e.g., data protection, outages, and price structures. The specification of SLAs will better reflect the customers' needs if they address the required issues at the right time.

Cloud Data Management: Cloud data is a very large and unstructured or semi-structured, and typically append-only with rare updates Cloud data management an important research topic in cloud computing. do not access physical security system of data centers, they must rely on the infrastructure provider to achieve full data security. Even for a virtual private cloud, the service provider can only specify the security setting remotely, without knowing whether it is fully implemented. And Software frameworks such as MapReduce and its various implementations such as Hadoop are designed for distributed processing of data-intensive tasks, these frameworks typically operate on Internet-scale file systems such as GFS and HDFS. These file systems are different from traditional distributed file systems in their storage structure, access pattern and application programming interface.

Data Encryption: Encryption is known as a key technology for data security. We can understand data in motion and data at rest encryption. Remember, security can range from simple (easy to manage, low cost and quite frankly, not very secure) all the way to highly secure (very complex, expensive to manage, and quite limiting in terms of access). You and the provider of your Cloud computing solution have many decisions and options to consider. Once the object arrives at the cloud, it is decrypted, and stored. These are options, understand your cloud computing solution and make your decisions based on desired levels of security.

Interoperability: The interoperability is a ability of two or more systems work together in order to exchange information and use that exchanged information. The lack of integration between these networks makes it difficult for organizations to combine their IT systems in the cloud and realize productivity gains and cost savings. To overcome this challenge, industry standards must be developed to help cloud service providers design interoperable platforms and enable data portability. Organizations need to automatically provision services, there is a need to have cloud interoperability.

Access Controls: In the access control we are having Authentication and identity management. What level of enforcement of password strength and change frequency does the service provider invoke? What is the recovery methodology for password and account name? How are passwords delivered to users upon a change? What about logs and the ability to audit access? This is not all that different from how you secure your internal systems and data, and it works the same way, if you use strong passwords, changed frequently, with typical IT security processes, you will protect that element of access.

Energy Resource Management: Energy Resource Management is describe to the Significant saving in the energy of a cloud data center without sacrificing SLA are an excellent economic incentive for data center operators and would also make a significant contribution to greater environmental sustainability. Energy-aware job scheduling and server consolidation are two other ways to reduce power consumption by turning off unused machines. Recent research has also begun to study energy-efficient network protocols and infrastructures. A key challenge in all the above methods is to achieve a good trade-off between energy savings and application performance. In the research started to investigate coordinated solutions for performance and power management in a dynamic cloud environment. The Global Energy Management Center (GEMC) can help companies monitor energy consumption patterns from multiple sources. This capabilities of the cloud computing.

Server consolidation: Server consolidation is achieved to the increased resource utilization and reduction in power and cooling requirements. Now being expanded into the cloud. Server consolidation is an effective approach to maximize resource utilization while minimizing energy consumption in a cloud computing environment. The problem of optimally consolidating servers in a data center is often formulated as a variant of the vector bin-packing problem, which is an NP-hard optimization problem. Additionally, dependencies among VMs, such as communication requirements, have also been considered recently. system must quickly react to resource congestions when they occur.

Reliability & Availability of Service: In the challenge of reliability comes into the picture, when a cloud provider delivers on-demand software as a service. The software needs to have a reliability quality factor so that users can access it under any network conditions. There are a few cases identified due to the unreliability of on-demand software. To avoid such problems, providers are turning to technologies such as Google Gears, Adobe AIR, and Curl, which allow cloud based applications to run locally. Considering the use of software such as 3D gaming applications and video conferencing systems, reliability is still a challenge to achieve for an IT solution that is based on cloud computing .

Common Cloud Standards: It is described to Security based accreditation for Cloud Computing would cover three main areas which are technology, personnel and operations. Technical standards are likely to be driven by organizations, such as, Jericho Forum1 before being ratified

by established bodies, e.g., ISO2 (International Standard Organization). there are some workable solutions such as tweaking the ISO 27001 and using it as the default measurement standard within the framework of the SAS 704. Currently, one of the main problems is that there are many fragmented activities going in the direction of Cloud accreditation, but a common body for the coordination of those activities is missing. The creation of a unified accreditation body to certify the Cloud services would also be a big challenge.

Conclusion and Feature work : The cloud computing model is the sharing of resources and one of the biggest security worries. This is a still struggling in its infancy for implimantaion of a large-sized enterprise. IT challenges are spearcheding the challenges. Cloud service providers need to inform their customers on the level of security that they provide on their cloud. In this paper, we first discussed various models of cloud computing, security issues and research challenges in cloud computing. Data security is major issue for Cloud Computing. There are several other security challenges including security aspects of network and virtualization. This paper has highlighted all these issues of cloud computing. In cloud computing holds some strong promises it's a highly available to dynamically allocate resources. we hope our work will provide a better understanding of the design challenges of cloud computing, and this way of further research in this area.

REFERENCES

[1]Gartner Inc:Gartner identifies the Top 10 strategic technologies for 2011.http://www.garther.com.

[2] R. L Grossman, "The Case for Cloud Computing".

[3] B. R. Kandukuri, R. Paturi V, A. Rakshit, "Cloud Security Issues".

[4] Meiko Jensen, Jorg Schwenk, Nils Gruschka, Luigi Lo Iacon, "On technical Security Issues in Cloud Computing".

[5] Aman Bakshi, Yogesh B. Dujodwala, "Securing cloud from DDoS Attacks using Intrusion Detection System in Virtual Machine".

[6] B. R. Kandukuri, R. V. Paturi and A. Rakshit, "Cloud Security Issues".

[7] R. Gellman, "Privacy in the clouds: Risks to privacy and confidentiality from cloud computing". The World Privacy Forum,2009.http://www.worldprivacyforum.org/pdf/WPF_Cloud_Privacy_Report.pdf.

[8] L.J. Zhang and Qun Zhou, "CCOA: Cloud Computing Open Architecture".

[9] Tim Mather, Subra Kumaraswamy, Shahed Latif, Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance, O' Reilly Media, USA, 2009.

[11] Cong Wang, Qian Wang, Kui Ren, and Wenjing Lou, "Ensuring Data Storage Security in Cloud Computing."

[12] S. Subashini, V. Kavitha, "A survey on security issues in service delivery models of cloud computing".

[13] V. Krishna Reddy, B. Thirumal Rao, Dr. L.S.S. Reddy, P.Sai Kiran "Research Issues in Cloud Computing ".