Cloud Computing Security concerns

Charu Jain*
Mtech-Research Scholar
Engineering College Bikaner
Rajasthan Technical University, Kota

Dr.SubhashPanwar**
Research Supervisor
Assistant Professor, Computer Science,
Engineering College Bikaner

Abstract

Cloud computing is aconstruction for providing computing services via the internet on demand and pay per use access to a pool of shared resources namely networks, storage, servers, services and applications, without physically acquiring them. So it saves managing cost and time for organizations. Many industries, such as banking, healthcare and education are moving towards the cloud due to the efficiency of services provided by the pay-per-use pattern based on the resources such as processing power used, transactions carried out, bandwidth consumed, data transferred, or storage space occupied etc. Cloud computing is a completely internet dependent technology where client data is stored and maintain in the data centre of a cloud provider like Google, Amazon, Salesforce.com and Microsoft etc. Limited control over the data may incur various security issues and threats which include data leakage, insecure interface, sharing of resources, data availability and inside attacks. There are various research challenges also there for adopting cloud computing such as well managed service level agreement (SLA), privacy, interoperability and reliability. This research paper outlines what cloud computing is, cloud architecture, the various cloud models, the main security risks and issues that are currently present within the cloud computing trade.This research also include the discussion about the best practices to service providers as well as enterprises hoping to leverage cloud service to improve their bottom line in this severe economic climate.

Keywords: Security Issues, Cloud Security, Cloud Architecture, Data Protection, Cloud Platform, Data Security, virtual memory.

1. Introduction

Cloud computing has become the most emergent technology now a days.It is a recently evolved computing terminology or metaphor based on usefulness and consumption of computing resources. Cloud computing includes deploying groups of remote servers and software networks that permit centralized data storage and online access to computer services or resources. It is a computing pattern, where a vast pool of systems are connected in private or public networks, to provide vigorously scalable infrastructure for application, data and file storage at low cost.

1.1 Origin of Cloud

The origin of the term *cloud computing* is imprecise. The expression *cloud* is commonly used in science to describe a large pool of objects that visually appear from a distance as a cloud and describes any set of things whose specifics are not inspected further in a given context. References to cloud computing in its modern sense appeared early as 1996, with the earliest known statement in a Compaq internal document. The commercialisation of the term can be sketched to 2006 when Amazon.com presented the Elastic Compute Cloud. EC2 started providing "Infrastructure-as-a-service" (IaaS) to the customers. Cloud computing is the result of evolution and adoption of existing technologies and models. The main objective of cloud computing is to allow users to take benefit from all of these technologies, without the need for good knowledge about or proficiency with each one of them. The cloud aims to cut costs, and helps the users focus on their staple business instead of being obstructed by IT obstacles.

1.2 The major milestones of Cloud computing

Swiftness: It recovers with users' ability to re-provision technological infrastructure resources.

Cost: Cost reductions claimed by cloud providers. A public-cloud model converts capital expenditure to operational expenditure. This supposedly lowers blocks to entry, as infrastructure is typically provided by a third party and does not need to be bought for one-time or intermittent intensive computing tasks.

Device and location independence: It enable users to access systems using a web browser irrespective of their location or what device they use (e.g., PC, mobile phone). As infrastructure is off-site (typically provided by a third-party) and retrieved via the Internet, users can connect from wherever.

Maintenance: Maintenance of cloud computing applications are easier, because they do not need to be installed on each user's computer and can be log on from dissimilar places.

Multitenancy: It permits sharing of resources and costs across a large gathering of users thus permitting for:**Centralization** of infrastructure in locations with lower costs (such as real estate, electricity, etc.), increase **peak-load capacity,** also enhance the efficiency of the system that are often only 10-20% utilized.

Productivity: It may be amplified when multiple users can work on the same data at the same time, rather than waiting for it to be saved and emailed. Period may be saved as there is no need to be re-entered the information when fields are matched, and the users do not need to install application software upgrades to their computer.

Trustworthiness: It improves with the usage of multiple redundant sites, which makes well-designed cloud computing appropriate for business continuity and disaster recovery.

Security: Security can expand due to centralization of data, increased security-based resources, etc., but concerns can persevere about loss of control over certain sensitive data, and the lack of security for stored kernels.

2. Service Models or cloud architecture: Services offered by cloud providers can be grouped into three categories.

- Software as a service(SaaS)
- Platform as a service (PaaS)
- Infrastructure as a service (IaaS).

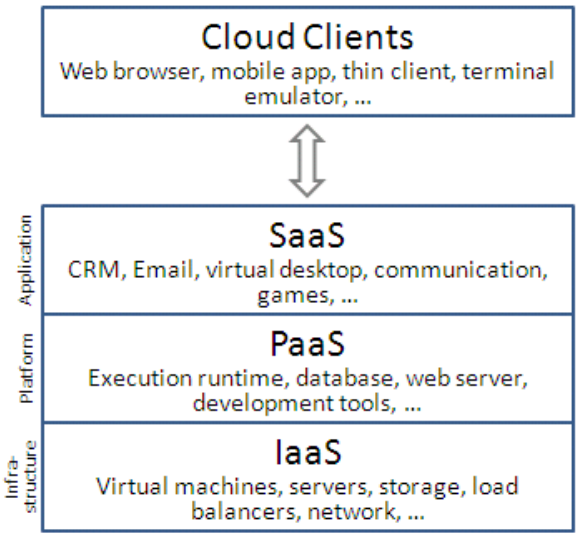

Fig.1 Cloud Architecture

Infrastructure as a service (IaaS): In the most basic cloud-service model & according to the IETF (Internet Engineering Task Force), providers of IaaS offer computers, physical or virtual machines and other

assets. It also offer additional resources such as a virtual-machine disk image library, raw block storage, and file or object storage, firewalls, load balancers, IP addresses, virtual local area networks (VLANs), and software packages. IaaS-cloud providers supply these resources on appeal from their large pools installed in data centres. For wide area connectivity, customers can use the Internet and can use carrier clouds (dedicated virtual private networks).To install their applications, cloud consumers install operating-system images and their application software on the cloud infrastructure. In this model, the cloud user covers and maintains the operating systems and the application software.

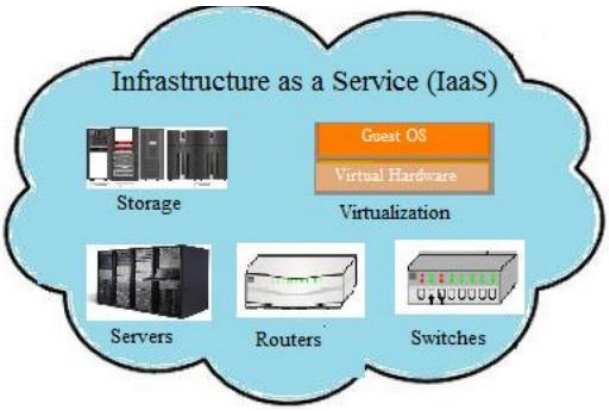

Fig. 2 Infrastructure as a service

Cloud providers typically bill IaaS services on a service computing basis: cost reflects the amount of resources allocated and consumed. Examples of IaaS service providers includes Amazon web services, Rackspace, GoGrid, BitRefinery, GoDaddy, Hosting.com, NephoScale, OpSource, ReliaCloud, SoftLayer, TerreMark etc.

Platform as a service (PaaS): Platform as a Service means delivering software design, development and testing platform over the Internet. Jack Schofield says that PaaS offers the facility of software and application development. Client can get this service from the cloud providers without the buying and maintaining the required software and hardware, so client can save the cost for their IT services. In the PaaS models, cloud providers provide a computing platform, usually including operating system, programming language execution environment, database, and web server.

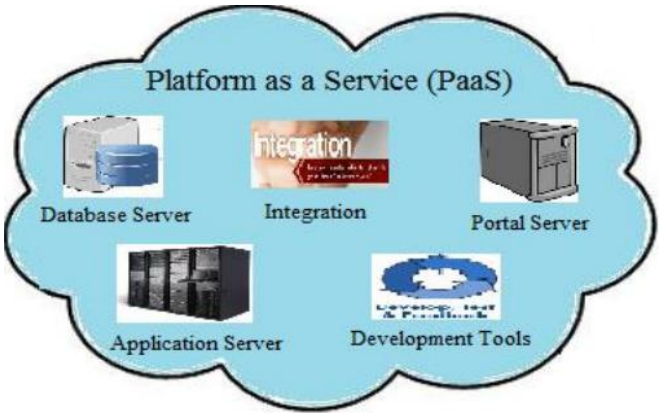

Fig.3Platform as a service

Application creators can develop and run their software solutions on a cloud platform without the cost and complexity of buying and handling the fundamental hardware and software layers. With some PaaS offers like Microsoft Azure and Google App Engine, the underlying computer and storage resources scale automatically to match application request so that the cloud consumer does not have to allocate resources physically. PaaS joins with software as a service (SaaS) and infrastructure as a service (IaaS), model of cloud computing. Examples of PaaS providers includes Windos Azure, Google AppEngine, Force.com, from salesforce, Bungee Connect, LongJump, WaveMaker, Amazon WebServices, AppScale, Engine Yard, FlexiScale, GigaSpaces, GridGain, LongJump, OS33, ThinkGrid, OutSystems etc.

Software as a service (SaaS): In software as a service (SaaS), users are providing access to application software and databases. Cloud providers manage the infrastructure and platforms that run the applications. SaaS is sometimes mentioned to as "**on-demand software**" and is usually priced on a pay-per-use basis or using a subscription fee.

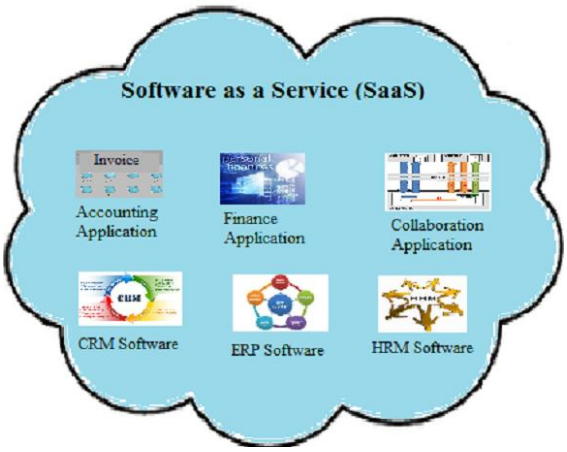

Fig.4 Software as a service

In the SaaS model, cloud suppliers install and operate application software in the cloud and cloud users access the software from cloud clients. Cloud operators do not manage the cloud infrastructure and platform where the application runs. This eliminates the necessity to install and run the application on the cloud user's own computers, which simplifies maintenance and support. Example of SaaS providers includes Sales Force CRM, Google Apps, Impel CRM, Wipro w-SaaS, Abiquo, AccelOps, Akamai, Apprenda, CloudOptix, Cloud9, CloudSwitch, NetSuite, Oracle CRM, Pardot, and SAP Business ByDesign etc.

3. Deployment model: Deployment models offered by cloud providers can be grouped into four categories:

- Public Cloud
- Private Cloud
- Community Cloud
- Hybrid Cloud

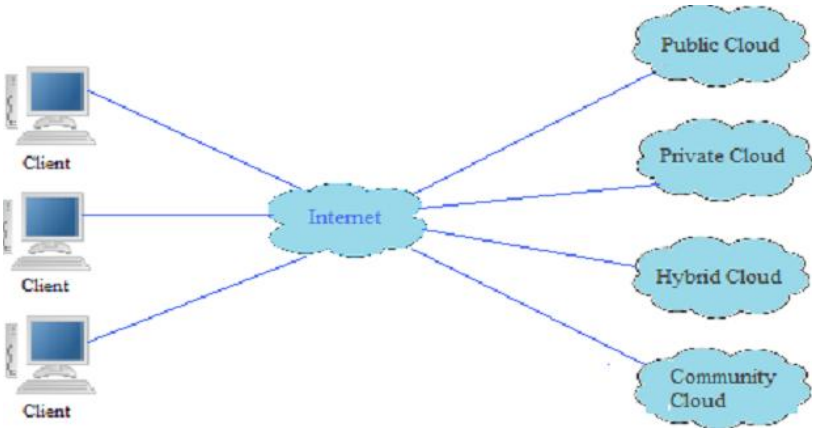

Fig.5 Cloud Deployment model

Private cloud: JitheshMoothoor, Vasvi Bhat of IBM says that private cloud is designed essentially for an association or government that needs more control over their data and applications that they can get by using a vendor hosted cloud service. Private cloud delivers control over services, security of the data and applications, these clouds are built for the use of one customer only. These clouds are generally installed behind the firewall of the association, and only the employees of that organization are allowed to access the cloud and its resources. The benefit of using private cloud encompasses more elastic and flexible cloud computing model. Using private cloud client can have more control and high security on their data and adherence to regulatory and compliance needs.

Public cloud: Public clouds are mostly hosted away from customer premises. Customer generally doesn't know the geographical location of the public cloud they are using. Public clouds are open to anyone who wants to sign up and use them. A cloud is called a "public cloud" when the services are purified over a network that is open for public use. Its services may be free or offered on a pay-per-usage model. AWS and Microsoft also offer direct connect services called "AWS Direct Connect" and "Azure ExpressRoute" respectively, such connections require customers to purchase or lease a private connection to a peering point offered by the cloud provider.

Community Cloud: A community cloud is similar to a private cloud where resources are shared by manyorganizations those have similar privacy, security, and regulatory considerations. A community cloud is managed and used by a group of many companies or government agencies that have common interest, such as specific security needs or common goals. Only the members of the community cloud are allowed to access the resource, data and applications in the cloud.

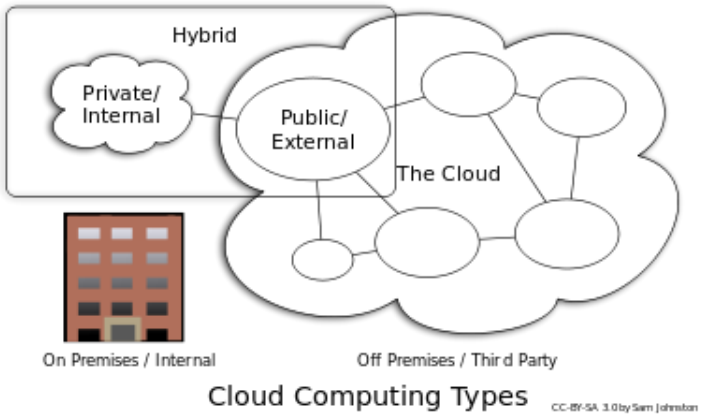

Fig.6 Cloud Computing Types

Hybrid cloud: Hybrid cloud is a composition of two or more clouds (private, community or public) that remain distinct entities but are bundled together, offering the benefits of multiple deployment models. Hybrid cloud can also mean the ability to connect association, managed and/or dedicated services with cloud resources. The hybrid cloud computing model attracts various governments and companies due to its multitenant nature, less development time and low cost. The public nature of the public cloud is the big issue for the governments and other organization, in adoption of it, because in case of the public cloud, control of the cloud remains with the vendor not with the client, which increase the security threat in public cloud adoption.

4. Security of data on Cloud: Cloudcomputing isacompletelyinternet dependenttechnology where clientdata isstoredand maintaininthe data centres of a cloudprovider like Google, Amazon, Salesforce.com and Microsoft etc. Limited.Security withincloudcomputing is an especially troublesomeissue becauseof the fact thatthe devices used toprovideservices do not related tothe users themselves. The users havenocontrolof, nor anyknowledgeof, whatcould ensuetotheirdata. Thisisa greatalarm incases when usershave valuableand delicateinformation stored in a cloud computing service. Users do not want to compromisetheir privacy socloudcomputing service providers must ensure that the customer's data is safe. To keep the data safe is gradually become challenging because as security developments are made, there always seemstobe someonetofigure out a wayto disable the securityandtake advantage of userinformation.[18]Someorganizations are now aware of the securityissues inthe cloudcomputing.The **Cloud Security Alliance** is a non-profitorganization formed topromote the use of bestpractices for providingsecurityassurance withinCloud Computing, andprovide education onthe uses of Cloud Computing tohelpsecure allother forms of computing.[18] The **Open Security Architecture (OSA)** is another organization focusing onsecurity issues. They propose the OSA pattern, whichpatternisanattempt toillustrate core cloudfunctions, the key roles for oversight and risk mitigation, collaborationacross variousinternal organizations, andthe controls thatrequire additionalemphasis. [18] Figure 7 show the high level security architecture that is given by open security architecture organization.

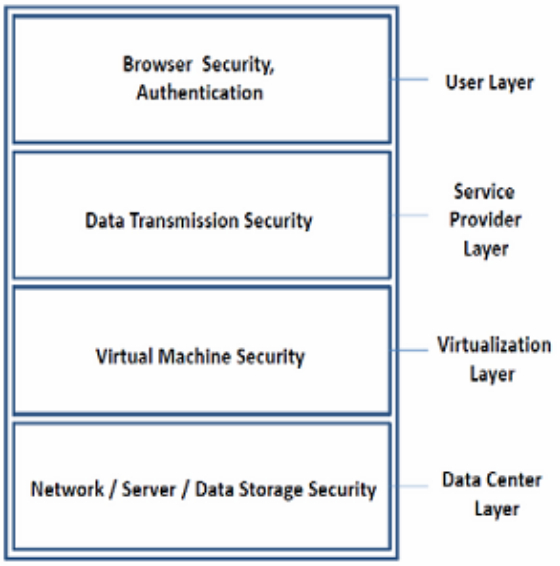

Figure 7. High Level Security Architecture

5. The key security issues that are presently annoying: Cloud computing consistsof applications, platforms, large pool of data andinfrastructure segments. Each segmentperformsdifferentoperations andoffers differentproducts for businesses and individualsaroundthe world. [18]There are countless security issues for cloud computing asitcomprehendsmany technologies including networks, database management,operating systems, virtualization, resourcescheduling, priority scheduling, transaction management, loadbalancing,concurrencycontroland memory management. Therefore,security issues for all of these systems and technologies are alsoapplicabletocloud computing technology. For example, the networkthatinterconnects the systems in a cloud should to be secure andmappingof virtual machines to the physical machines hastobe carriedout securely. Data security involves encrypting and decrypting the data as well as ensuring that appropriate policies are imposed for datasharing. There are many more security threats that are similar to other technology but the rectification policies and methods for removal of threats are different because of the change in the working of cloud computing technology.The various securityconcerns ina cloud computing environment are given below.

- Access toServers & Applications
- Data Transmission
- Virtual Machine Security
- NetworkSecurity
- Data Security
- Data Privacy
- Data Integrity
- Data Location
- Data Availability

Access to Servers &Applications: In traditional data centres, the access to data and database is in the control of the system administrator but this is not possible in case of cloud data centres. In cloud computing administrative access to all the data isconducted via Internet. So this increase exposure and risk. It is particularly important to restrictadministrative access to data andmonitor this access to maintain visibility of changes in system. So who will access and how will access is the biggest security of cloud data centres. To ensure access security of data and server some organizations uses security policies. These security policies may entitle someconsiderationswherein some ofthe employees of that organization arenot given access to certain amount of data. These security policies ensures that no unauthorized user can access the data.Many companies are storing their employee information in sometype of Lightweight Directory Access Protocol (LDAP) servers.

DataTransmission: Data transmission means communication of data from and to the users.Encryption techniques are used for datatransmission.

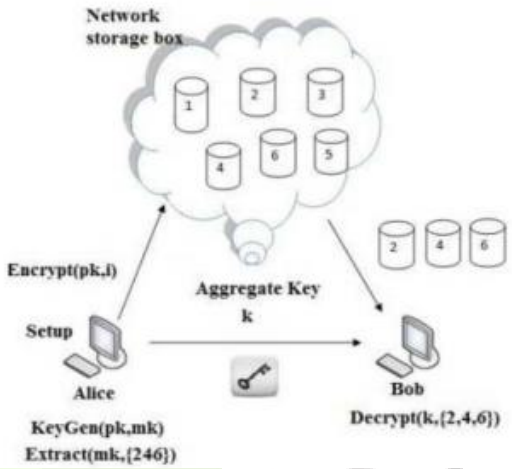

Figure 8. Key sharing mechanism for sharing data

Figure 8 shows how data can be shared from one user to anther using cryptography key sharingmechanism. To provide the protectionof dataonly goes where the customer wants it to go by using authentication and integrity and is not modifiedin transmissionSSL/TLS protocols are used here. InCloud environment mostof the dataisnotencrypted inthe processing time. In our traditional system all the data is encrypted by using cryptography techniques so data is safe. Therefore just like traditional system in cloud environment there should be some cryptography techniques that can deliver security at data transmission time. Subsequently there will be nopossibility that intruder can interruptandchangecommunications.

Virtual Machine Security: Virtualization is one of the maincomponents ofa cloud. Virtual machines are dynamic. A virtual machine is an environment of operating system or application that is installed on software, which imitates dedicated hardware. The end user has the same experience on a virtual machine as they would have on dedicated hardware. Cloud computing works on virtualization.Virtualization means to create a virtual version of a device and resource, such as a server, storage device, network or even

an operating system where the framework divides the resource into one or more execution environments.[19]The term virtualization has become a buzzword, and include the following:

- Storage virtualization: the combination of multiple network storage devices into what appears to be a single storage unit.
- Server virtualization: the partitioning a physical server into smaller virtual servers.
- Virtualization at Operating system-level: a type of server virtualization technology which works at the operating system (kernel) level.
- Network virtualization: using network resources through a logical subdivision of a single physical network.
- Application virtualization.

Itis difficult tomaintainanauditable record ofthe security stateof a virtual machine atanygiven pointintime. There are two type of virtualization FullVirtualizationand Partial Virtualization. In fullvirtualization, whole hardware architecture is replicatedvirtually. However, in partial virtualization,an operatingsystemis reformed sothatitcanbe run concurrentlywith otheroperatingsystems. VMM (Virtual Machine Monitor), is a software layer that abstracts the physical resources used bythe multiple virtual machines.[18]The VMMprovides a virtualprocessor and other virtualized versions ofsystemdevices suchas I/O devices, storage, memory, etc. The security issue with VMM is the control of administrator onhostand guestoperating systems. Current VMMs (Virtual Machine Monitor) do not offer perfectisolation.

Network Security: Cloud computing is the next generation of networking computing. Undoubtedly, one of the significant concerns in cloud computing is network security. Networks are categorizedintomanytypes like Sharedandnon-shared, public orprivate, small area or largearea networks i.e. LAN, WAN, MAN. Each of themhave a plenty full security threats todeal with. That's the reason that the problems associatedwith all these networks are also become security threats on cloud.**DNS attacks, Sniffer attacks, issue of reused IPaddress** are some of them are explained in detailsas follows. A Domain NameServer (DNS) server does the translation of a domain name to an IP address. Domain names are much easier to remember therefore the DNS servers are needed. But there are cases when having called the server by name, the userhas beenroutedtosome other evilcloud instead ofthe onehe askedforandhence the use ofDNS serverbecome a problem.Although DNS security measures are used like: **DomainNameSystemSecurityExtensions (DNSSEC)** reducestheeffects ofDNS threats but still there are cases when these securitymeasures prove incapable toeliminate the wrong path between asender and areceiver. A Sniffer (also known as network protocol analysers) is an application that capture network packets. If the network packets do not use encryption techniques to encrypt the packets, the data within the network packet can be read using a sniffer. Sniffing refers to the process used by invaders to capture network traffic using a sniffer. Once the packet is captured using a sniffer, the contents of packets can be changed. Sniffers are used by hackers to steal sensitive network information, such as passwords, account information etc. hacking of information using sniffer is called sniffer attacks. Many protocols are used to overcome these sniffers attacks. Reused IP

address issue have beena big network securityproblem. When a particular user moves from the network, the IP- address associated with him can be assigned to the new user. It is just like when an element is deleted from memory then its space is free for the use of other variable storage.This process take some time as the address should be changed from the DNS storage and Cache. Hence the processing time for changing the name from the memory and DNS server become a security problem.

Datasecurity and privacy:Data security has become a major issue in information technology. In the cloud computing atmosphere, it becomes particularly severe because the data is located in different places even in all the globe. Data security and privacy are the two main factors of user's concerns in cloud technology. Though many techniques have been investigated in both academics and industries, data security and privacy protection are becoming more important for the future development of cloud computing technology in government, industry, and business.

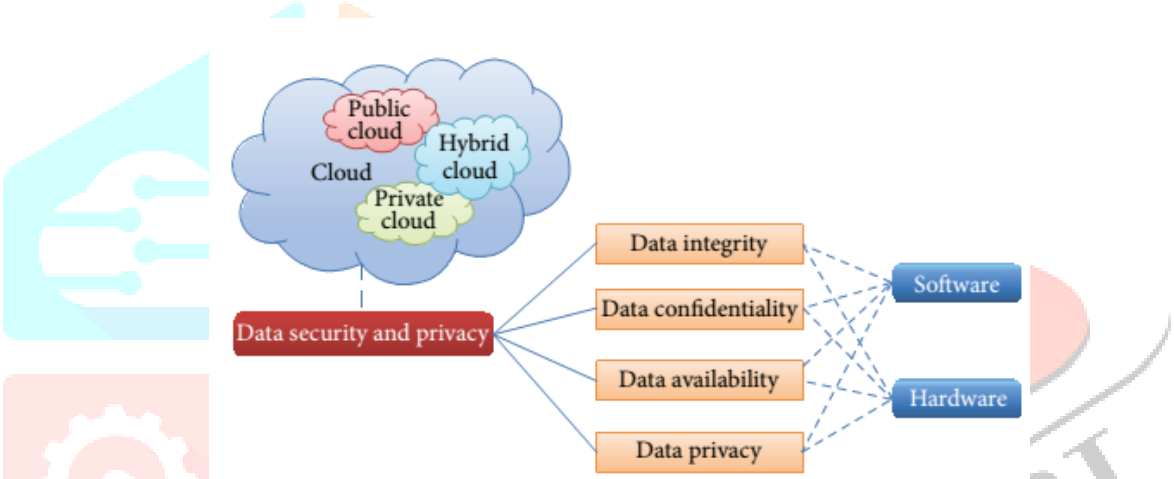

Figure 9: Organization of data security and privacy in cloud computing. [20]

Data security and privacy protection issues are relevant to both hardware and software in the cloud structural design. For data transfer in cloud the most common protocol that is used is HTTP (Hypertext transfer protocol). For security measure HTTPs and SSH (Secure Shell) is used. In cloud, privacy means when users visit the sensitive data, the cloud services can prevent potential adversary from inferring the user's behaviour by the user's visit model. Oblivious RAM (ORAM) technology is used to maintain data privacy. ORAM technology visits numerous copies of data to hide the real visiting aims of users. ORAM has been widely used in software protection and has been used in protecting the privacy in the cloud as a promising technology. [20]

DataIntegrity: Data that is stored in the cloud could suffer from the loss on transmitting to/from cloud data storage. The meaning of Data integrity is that data should be kept secure from unauthorized modification. Any modification to the data from any person should be detected. Integrity should be checked at the data level and computation level both. Data integrity could help in telling about the data loss or notifying if there is data manipulation. Dataexploitation can happen atanylevelofstorage and withanytype of media. Hence

integritymonitoring isessential incloud storage whichis critical for any data centre. Data integrity can easilyachievedina traditional standalonesystem which use asingle database. Data integrity insuchsystems is maintained using database constraints and transactions. Transactions should follow ACID (atomicity,consistency, isolationanddurability)attributes to ensure data integrity of a system. Data generated bycloud computing services are stored inthe clouds.Keeping data inthe clouds means users have no control over their data and rely on cloud operatorsto enforceaccess control. It also means that data can be saved anywhere on the cloud. User do not know that on which cloud location his/her data is stored. Means data location is also unknown to user. Consequently maintaining data integrity is somewhat hard in cloud computing technology.

DataAvailability: Data availability means when accidents such ashard disk damage, IDC fire, short circuit, data base crash and network failures occur, theamount that user's data can be used or recovered and how theusers verify their data by using any techniques. The issue of storing data over the cloud servers that are not in user's approachis a serious concern of clients because the cloud vendorsare governed by the local laws and rules to the data and therefore the cloudclients should be aware of those laws.

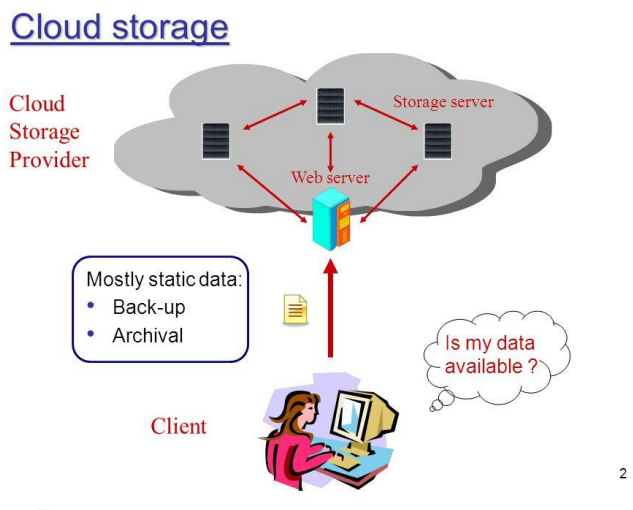

Figure 10. Process of data availability from cloud storage

Figure 10 shows that how data will make available to the end user from the cloud storage. It also shows that user is always in that worry that whether his/her data is safe or not, whether it will become available when needed or not. Furthermore, the cloudservice provider should give the surety to the cloud clients about their data security, confidentiality and integrity. The cloud service provider shouldshare all such worries with the client and build trustrelationship in this connection.There should be a transparent service between the users and cloud service provider.Data Availabilityis one of the prime concerns of liability and safetycriticalorganizations. All these security issues are vibrant and should be kept in mind while working on cloud environment.

Conclusion and Future Scope

Conclusion: One of the biggest security concerns with the cloud computing Model is the sharing of resources. Cloudservice providers needtonotifytheir customers onthe level ofsecurity that they provide ontheir cloud.Inthis research,wefirstdiscussed variousmodels of cloud computing, cloud computing architecture and then the security issues in cloudcomputing. Data securityis major issue for Cloud Computing. Cloud data can be very large, unstructured or semi structured, and typically append-only with rare updates. Cloud data management and its security is an important part in cloud computing. Since service providers typically do not have access to the physical security system of data centres, they must rely on the infrastructure provider to achieve full data security.Thereareseveral other securitychallengesincluding securityaspects ofnetwork and virtualization. This research has highlighted allthese issues of cloud computing and further focus on how the data will become more secure on cloud.

Future Scope: Because of the complexity of the cloud, it is very difficult to achieve end-to-end security. To achieve better security new security techniques need to be developed and older security techniques needed to be radically squeezed to be able to work with the clouds architecture. As the developmentof cloud computing technologyis still at anearly stage, many existing issues have not been fully addressed, while new challenges keep emerging from industry applications. Some of the challenging research issues in cloud computing are Service Level Agreements (SLA's), Cloud Data Management & Security, Data Encryption, Migration of virtual Machines, Interoperability, Access Controls, Energy Management, Multitenancy, Reliability & Availability of Service, Common Cloud Standards, Platform Management. As the enlargement of cloud computing technology is still at an early stage, we except that our work will provide a better understanding of the design challenges of cloud computing, and give a better surface for the further research in this area.

References

1. Available:http://d36cz9buwru1tt.cloudfront.net/pdf/aws-risk-and-compliance whitepaper.pdf
2. Available:http://www.ajilitee.com/wp-content/uploads/2010/07/White-Paper Ajilitee-Cloud-Computing-from-the-Ground-Up-July-20101.pdf
3. Vecchiola, X. Chu, and R. Buyya(2009) Aneka: A Software Platform for .NET-based Cloud Computing. High Speed and Large Scale Scientific Computing, pp267-295, W. Gentzsch, L. Grandinetti, G. Joubert (Eds.), ISBN: 978-1-60750-073-5, IOS Press, Amsterdam, Netherlands, 2009.
4. Cloud Computing Use case Discussion Group (2010). Cloud Computing Use Cases. Available: cloudusecases.org/Cloud_Computing_Use_Cases_Whitepaper-4_0.od
5. CPNI, (2010). Information Security Briefing: Cloud Computing. Available:http://www.cpni.gov.uk/Documents/Publications/2010/2010007-ISB_cloud_computing.pdf
6. David C. Wyld, (2010), The cloudy future of the Government IT: Cloud Computing and the Public Sector around the World. Available: http://airccse.org/journal/ijwest/papers/0101w1.pdf
7. Garg, S.K., Venugopal, S., and Buyya, R.(2008): A Meta-scheduler with Auction Based Resource Allocation for Global Grids, *Proceedings of the 14th IEEE International Conference on Parallel and Distributed Systems*, IEEE CS Press, Los Alamitos, USA, 2008.
8. IBM Sales and Distribution, Thought Leadership White Paper, (2013), Cloud computing for banking Driving business model transformation.
9. Munich, Gerald Kaefer G., (2010), Cloud Computing Architecture, Siemens, *Corporate Research and Technologies*, SATURN 2010
10. Pollan, Michael et al., The Omnivore‘s Dilemma: A Natural History of Four Meals. New York: Penguin, 2006.
11. Yigitbasi N., Iosup A., Epema D. &Ostermann S.,(2009), C-Meter: A Framework for Performance Analysis of Computing Clouds, *9th IEEE/ACM International Symposium on Cluster Computing and the Grid*, DOI 10.1109/CCGRID.2009.40
12. Manjrasoft, (2010). Aneka Dynamic Provisioning. Available: http://www.manjrasoft.com/download/2.0/AnekaDynamicProvisioning.pdf
13. wikipedia. Cloud communications. Available: http://en.wikipedia.org/wiki/Cloud_communications
14. ORACLE. Accelerating Multimedia Application Development with JSR 309 Media Server Control API. Available:
15. http://www.oracle.com/technetwork/articles/communications/ericson-jsr309-084430.html
16. IBM, (2009). IBM Delivers Down to Earth Cloud Computing. Available: http://www=03.ibm.com/innovation/us/smarterplanet/global/pdfs/Mainstream_Cloud_Computing.pdf

17. Darren Mundy and Bandi Musa, (2010). Towards a Framework for eGovernment Development in Nigeria. Electronic journal of e-government volume 8 issue 2. Available: www.ejeg.com/issue/download.html?idArticle=205
18. Rabi Prasad Padhy, ManasRanjan Patra, Suresh Chandra Satapathy, (2011). Cloud Computing: Security Issues and Research Challenges. IRACST - International Journal of Computer Science and Information Technology &Security (IJCSITS) Vol. 1, No. 2, ISSN: 2249-9555
19. https://www.webopedia.com/TERM/V/virtualization.html
20. Yunchuan Sun, Junsheng Zhang, YongpingXiong, and Guangyu Zhu (2014). Data Security and Privacy in Cloud Computing. Hindawi Publishing Corporation International Journal of Distributed Sensor Networks Volume 2014, Article ID 190903, 9 pages http://dx.doi.org/10.1155/2014/190903