Ind Jour Math & Comp Sc. Jhs. Vol. I - II, 2013 Pg 34-51

Assessing the risk associated with cloud computing

Dr. U.S Pandey, Anjali jain
Associate Professor, School of Open Learning Delhi University, Delhi
Mewar university, Gangrar, Chittorgarh(Rajasthan)
Email:uspandey1@gmail.com, Email:anjalijain81@gmail.com
Recceived on 3/2/2013

ABSTRACT : Today Cloud Computing is quite possibly the most discussed concept in Information Technology (IT).As a coin has two sides, so as cloud computing, on the one side it is viewed as a utility like telephone and electricity which provides enormous cheaper and easier business opportunities to even middle size businessman, Using cloud computing, consumers can safe cost of hardware deployment, software licenses and system maintenance and on the other side of this coin there are threats which make people think before moving into cloud.

In this paper we firstly look at cloud computing definitions, how cloud computing model is different from the traditional one. Then we will discuss the pros and cons of cloud computing, after that its architecture is briefly explained. Cloud computing models-private, public, community and hybrid, as well as cloud service modes will also be discussed. People are having several misconceptions or myths related to Cloud computing so there is a glimpse of that also. And lastly we'll examine the security challenges of cloud computing – isolating data in multi-tenant environments, controlling data movement and several others. It is important to consider all such issues before a person decide either to move or not to move his systems, applications, and/or data to the "Cloud".

INTRODUCTION

Cloud computing infrastructures are next generation platforms that can provide tremendous value to companies of any size. They can help companies achieve more efficient use of their IT hardware and software investments and provide a means to accelerate the adoption of innovations. Cloud computing increases profitability by improving resource utilization. Costs are driven down by delivering appropriate resources only for those resources are needed. Cloud computing has enabled teams and organizations to streamline lengthy procurement processes.

Cloud computing is a technology where shared resources, software and information are provided to computers and other devices on-demand over the internet. Cloud computing is a style of computing that characterizes a model in which providers deliver a variety of IT-enabled capabilities to consumers. Cloud-based services can be exploited in a variety of ways to develop an application or a solution. Using cloud resources does not eliminate the costs of IT solutions, but does re-arrange some and reduce others. In addition, consuming cloud services enterprises will increasingly act as cloud providers and deliver application, information or business process services to customers and business partners.

The term "cloud computing" has been hotly contested, drawing both derision and praise from different sectors of the I.T. community. At its core, the term refers to the outsourcing of data centres and application services to a remote provider under a pay-as-you-go contract. This 'metered' approach lowers costs and reduces complexity, simultaneously allowing the business to consume additional services "on-demand".

According to NIST(The National Institute of Standards and Technology) Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interactions.

Cloud computing is an evolving paradigm. In IT circles, the word "cloud" is associated with low-cost, OpEx-only, on-demand, limitless and elastic computing resources delivered as a utility.

Web-based email services from Google and Yahoo, Salesforce.com, instant messaging and voice-over-IP services from AOL, Google, Skype, Vonage and others are all cloud-computing services.

Cloud computing allows customers to scale vertically and horizontally, and based on the demands of

their users, it ensures there are enough resources at any given time. If a traffic spike occurs, it's easy to add more capacity. After the traffic trails off, it's just as easy to reduce capacity. And if additional components are added, you simply adjust capacity as needed.

"Cloud" computing is different than "regular" hosting.

"Cloud computing is also different from traditional hosting because it doesn't lock customers into expensive contracts that are based on calculating resources to meet their peak demands. Every month, whether all the resources are utilized or not, a customer will always have to pay for the contracted resources with regular hosting. That monthly cost translates directly into wasted operating expenses."

Traditional web hosting assumes that customers pay for a fixed amount of storage space and a fixed amount of bandwidth. But the traffic too many websites varies, and storage and bandwidth needs fluctuate over time.

For those websites, cloud computing, or cloud hosting, could save them money, as they would pay only for the actual monthly storage and bandwidth usage, and not for excess, unused capacity.

A cloud computing architecture consists of a front end and a back end. They connect to each other through a network, usually the Internet. The front end is the side the computer user, or client sees. The back end is the "cloud" section of the system.

Cloud computing does two things amazingly well," says Mark Lobel, a principal in PricewaterhouseCoopers' Advisory Services group. "It speeds up time-to-market and it lowers costs. Fundamentally, you're using the technology a lot more efficiently than you would in an in-sourced environment. In a virtualized cloud environment, you're using servers at a high level of potential utilization. The service providers make the hardware work up to its specification. If they're getting more out of every processor, they need less hardware, and that costs less money."

ADVANTAGES OF CLOUD COMPUTING

- Reduced setup costs can be considered as a major advantage for cloud computing, since the costs involved in setting up a data centre are not very high.
- In addition to the IT industry, even small scale businesses can adopt this environment (model).
- Considering cloud computing from the aspect of power management, it serves as a virtual server which is easier to implement in comparison to physical servers.
- Hardware management failure can also be localized and rectified with relative ease.
- Various data centres are spread throughout the country and thus it makes easy for the businesses to use preferred sites.
- The assessment of data can be done any time and is highly beneficial for the IT industry in reducing workloads.
- The cloud computing environments are easily scalable.
- Backup recovery is very easy in Infrastructure as a Service (IaaS) Providers, hence there is efficient incident response whenever data needs to be recovered.

DISADVANTAGES OF CLOUD COMPUTING

- A major disadvantage in cloud computing is that it is under the maintenance and supervision of a third party. Hence the confidentiality and security measures are less secured.
- In cloud environments the data is not specifically segregated. It is distributed throughout the cloud network and causes problems when specific data needs to be segregated.
- Another major drawback is the dependence on network connectivity. Network failures can result in loss to the company by causing extensive time delays.
- The Service Lease Agreements (SLA) are the agreements made with the service providers controlling varied equipment in the cloud network. These agreements should be carefully verified before entering into a contract of service.
- The quality of service is a key determining factor in the efficiency of a cloud network. A reliable service provider providing desired quality of service may be difficult to source and the process set-up could turn out to be time consuming.

CLOUD COMPUTING ARCHITECTURE

A cloud computing system is divided into two sections: the **front end** and the **back end**. They connect to each other through a network, usually the Internet. The front end is the side the computer user, or client, sees. The back end is the "cloud" section of the system.

Front end cloud computing architecture The front end of the cloud computing system comprises of the client's devices (or it may be a computer network) and some applications are needed for accessing the cloud computing system. All the cloud computing systems do not give the

same interface to users. Web services like electronic mail programs use some existing web browsers such as Firefox, Microsoft's internet explorer or Apple's Safari. Other types of systems have some unique applications which provide network access to its clients.

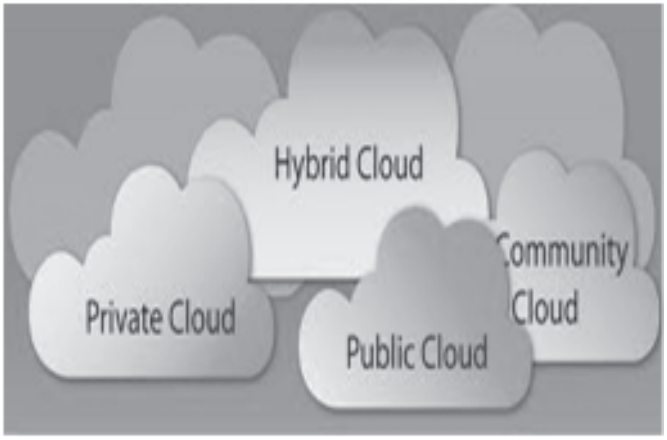
Back end cloud computing architecture Back end refers to some physical peripherals. In cloud computing, the back end is cloud itself which may encompass various computer machines, data storage systems and servers. Groups of these clouds make a whole cloud computing system.

MYTH

There are certain misconceptions related to cloud computing and these are:-

1. The public cloud is the most inexpensive way to procure IT services.
2. Virtualization is the only way to reach the cloud.
3. Critical applications do not belong in the cloud.
4. All cloud security requirements are created equally.
5. There is only one way to do cloud computing.
6. Cloud computing should satisfy all the requirements specified: scalability, on demand, pay per use, resilience, multitenancy, and workload migration.
7. Cloud computing is useful only if you are outsourcing your IT functions to an external service provider.
8. Cloud computing requires you to expose your data to the outside world.
9. Converged networks are essential to cloud computing.

CLOUD DEPOYMENT MODELS



- ❑ **Private Cloud**
- ❑ **Public Cloud**
- ❑ **Community Cloud**
- ❑ **Hybrid Cloud**

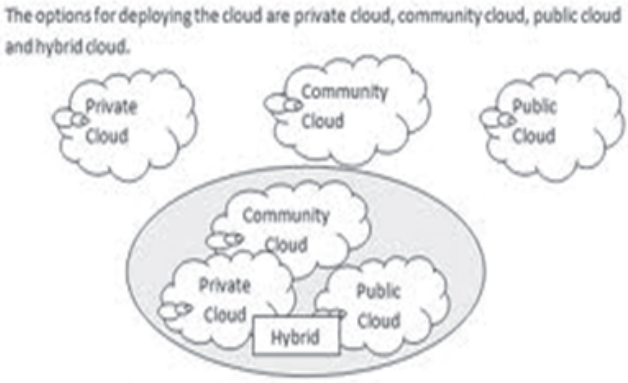


Figure 1 Cloud Deployment Options

PRIVATE CLOUD -According to NIST" private cloud is the cloud infrastructure, provisioned for exclusive use by a single organization comprising multiple consumers. It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises". It is also known as" internal cloud computing". Private cloud computing is said to be the next generation of virtualization. The cloud infrastructure is operated solely for an organization. It is created to deploy within the in-house business environment protected by the firewall settings. It may be managed by the organization or a third party and may exist on premise or off premise. Coughlin said that if a business is really serious about its data security, then they should choose a private cloud. Private cloud model is said to be one of the most reliable and secure cloud model because only single business entity has a full control over the cloud server and the access is given to only the authorized parties involved in managing the cloud. Private cloud may exist off premises and can be managed by a third party. Thus, two private cloud scenarios exist, as follows:

On-site Private Cloud

- ❑ Applies to private clouds implemented at a customer's premises. On-site private cloud mitigates this security risk by restricting the number of possible attackers as all the clients are typically the members of one subscriber organization.

Outsourced Private Cloud

- ❑ Applies to private clouds where the server side is outsourced to a hosting company.

Examples of Private Cloud:

- ❖ Eucalyptus
- ❖ Ubuntu Enterprise Cloud - UEC (powered by Eucalyptus)

- ❖ Amazon VPC (Virtual Private Cloud)
- ❖ VMware Cloud Infrastructure Suite
- ❖ Microsoft ECI data center.

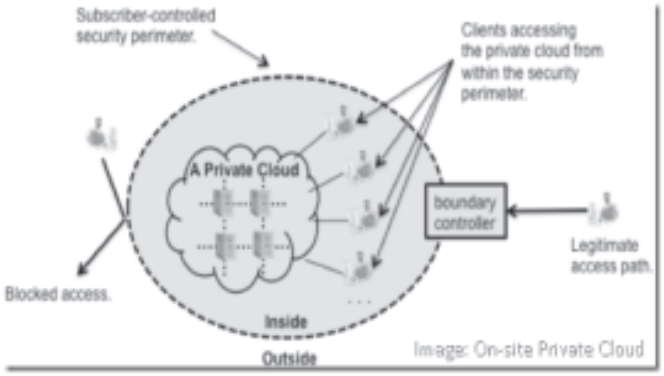


IMAGE: ON-SITE PRIVATE CLOUD

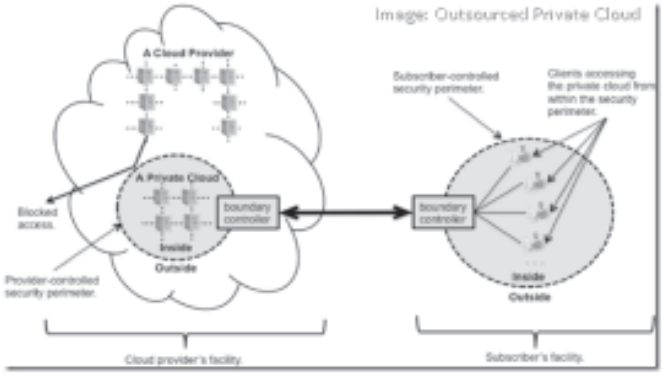


IMAGE: OUTSOURCED PRIVAT CLOUD

COMMUNITY CLOUD - According to NIST [1]"the community cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise". This type of cloud is mostly useful in Government departments, universities, central banks etc. Community cloud also has two possible scenarios:

- ❑ On-site Community Cloud Scenario
  - ♦ Applies to community clouds implemented on the premises of the customers composing a community cloud
- ❑ Outsourced Community Cloud
  - ♦ Applies to community clouds where the server side is outsourced to a hosting company.

Examples of Community Cloud:

- ❖ Google Apps for Government
- ❖ Microsoft Government Community Cloud

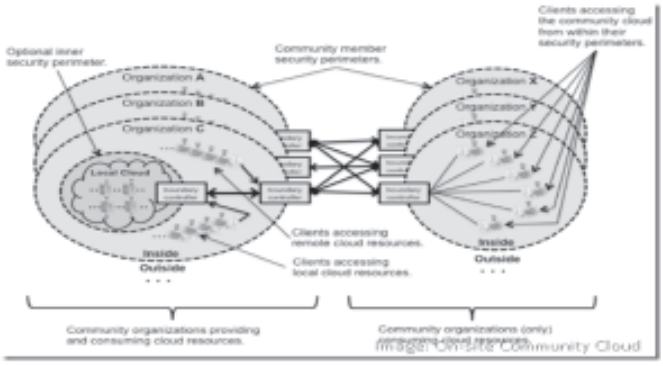


IMAGE: ON-SITE COMMUNITY CLOUD

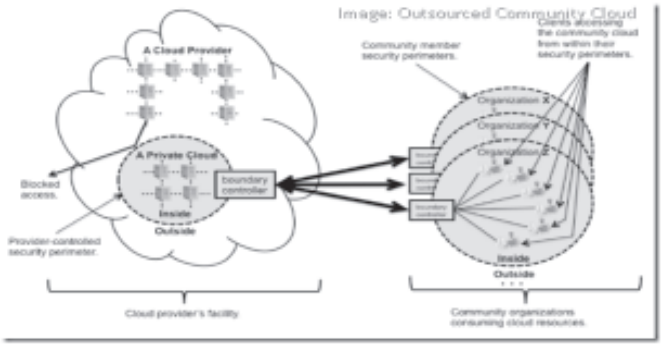


IMAGE: OUTSOURCED COMMUNITY CLOUD

PUBLIC CLOUD - According to NIST "this 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. In this model, vendors dynamically allocate resources (hard drive space, RAM, and processor power) on a per-user basis through web applications". Salesforce.com and ADP are two well-known vendors that offer public cloud computing services. The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services. Examples of Public Cloud are:-

- ❖ Google App Engine
- ❖ Microsoft Windows Azure
- ❖ IBM Smart Cloud
- ❖ Amazon EC2

In a public cloud scenario, a single machine may be shared by the workloads of any combination of subscribers. This indeed raises the security risk as the number of potential attackers increases with number of subscribers

HYBRID CLOUD –According to NIST " The hybrid cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by

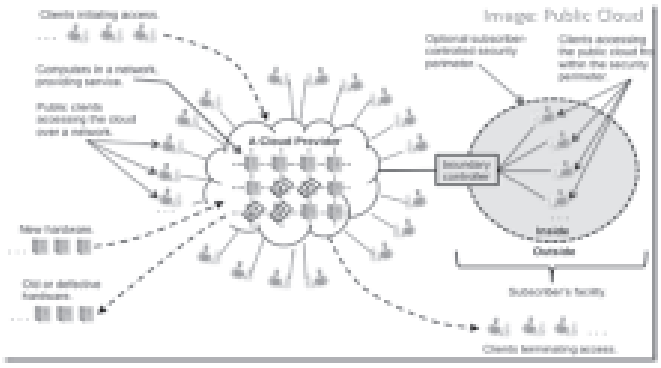


IMAGE: PUBLIC CLOUD

standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds)". But hybrid clouds lack the flexibility, security and certainty of in-house applications [2]. Hybrid cloud architecture requires both on-premises resources and off-site (remote) server-based cloud infrastructure.

Examples of Hybrid Cloud:-

- ❖ Windows Azure (capable of Hybrid Cloud)
- ❖ VMware vCloud (Hybrid Cloud Services)

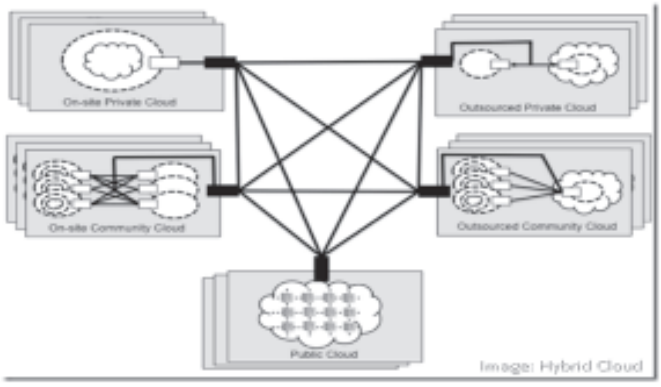


IMAGE: HYBRID CLOUD

NIST explicitly qualifies each such statement with the type of cloud to which it applies; i.e., each statement has a "scope."

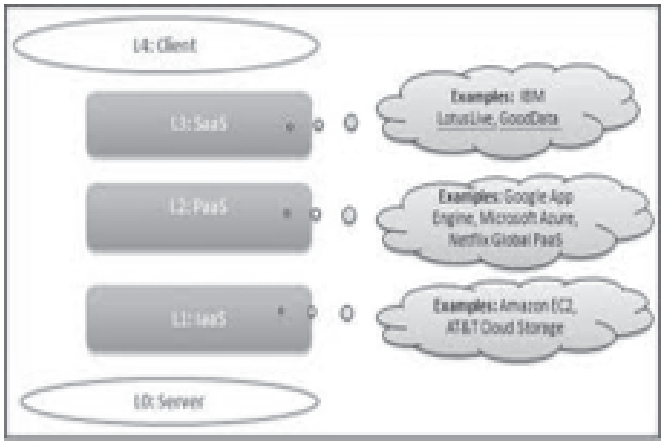
CLOUD COMPUTING SERVICE DELIVERY MODELS

The three main cloud service delivery models are:

- Infrastructure-as-a-Service (IaaS)

Scope Name	Applicability
general	Applies to all cloud deployment models.
on-site-private	Applies to private clouds implemented at a customer's premises.
outsourced-private	Applies to private clouds where the server side is outsourced to a hosting company.
on-site-community	Applies to community clouds implemented on the premises of the customers composing a community cloud.
outsourced-community	Applies to community clouds where the server side is outsourced to a hosting company.
public	Applies to public clouds.

- Platform-as-a-Service (PaaS)
- Software-as-a-Service (SaaS).



INFRASTRUCTURE-AS-A-SERVICE

In this most basic cloud service model, IaaS providers offer computers, as physical or more often as virtual machines, and other resources. The virtual machines are run as guests by a hypervisor, such as Xen or KVM. Pools of hypervisors within the cloud operational support system support large numbers of virtual machines and the ability to scale services up and down according to customers' varying requirements [3].

In IaaS user can control of software environment, but there is no need to maintain and buy any equipment and server .User can put any software on the server. The

cloud service providers provide storage space or other required resources and the client has to pay-per-use. Due to this the need for huge initial investment in computing hardware such as servers, networking devices and processing power is dramatically reduced and also there is no need to worry about the provisioning and management of infrastructure. They also allow varying degrees of financial and functional flexibility not found in internal data centres or with collocation services, because computing resources can be added or released much more quickly and cost-effectively than in an internal data centre or with a collocation service[4].

This model basically focuses on managing virtual machines. IaaS requires governance and usage monitoring .O'Neill recommends that enterprises establish cloud service governance frameworks that help prevent employees accessing information or services they are not permitted to use. He also said that "It also prevents them from running up costs on virtual machines or setting up their own accounts to access services paid for by the organization.

The cloud has a compelling value proposition in terms of cost, but IaaS only provides basic security like perimeter firewall, load balancing, etc, but applications moving into the cloud will need higher levels of security provided at the host. Examples of IaaS providers include Amazon Cloud Formation, Amazon EC2, Windows Azure Virtual Machines, DynDNS, Google Compute Engine, HP Cloud, Joyent, Rackspace Cloud, ReadySpace Cloud Services, and Terremark.

PLATFORM -AS-A-SERVICE

Platform-as-a-Service (PaaS) is a set of software and development tools hosted on the cloud service provider's servers. It is one layer above IaaS on the stack and abstracts away everything up to OS, middleware, etc. It allows the consumer to deploy the applications created using programming languages and tools supported by the provider onto the cloud infrastructure .In the PaaS model, cloud providers deliver a computing platform typically including operating system, programming language execution environment, database, and web server. Application developers can develop and run their software solutions on a cloud platform without the cost and complexity of buying and managing the underlying hardware and software layers. With some PaaS offers, the underlying computer and storage resources scale automatically to match application demand such that cloud user does not have to allocate resources manually. [5]

This offers an integrated set of developer environment and a complete software development life cycle management to the developers, which help them to develop their applications without having worrying about what is going on underneath the service as everything else is abstracted away from the "view" of the developers. Clients using PaaS services transfer even more costs from capital investment to operational expenses but must acknowledge the additional constraints and possibly some degree of lock-in posed by the additional functionality layers [6].

A key element to be considered within PaaS is the ability to deal with the possibility of outages from a Cloud provider. The security operation must provide the ability of load balancing in the events of outages. The use of virtual machines act as a catalyst in the PaaS layer in Cloud computing. Virtual machines must be protected against malicious attacks such as cloud malware. Therefore maintaining the integrity of applications and well enforcing accurate authentication checks during the transfer of data across the entire networking channels is fundamental.

Examples of PaaS include: Amazon Elastic Beanstalk, Cloud Foundry, Heroku, Force.com, EngineYard, Mendix, Google App Engine, Windows Azure Compute and OrangeScape.

SOFTWARE-AS-A-SERVICE

Hamdaqa, Mohammad said that in the SaaS model, cloud providers install and operate application software in the cloud and cloud users access the software from cloud clients. The cloud users do not manage the cloud infrastructure and platform on which the application is running. This eliminates the need to install and run the application on the cloud user's own computers simplifying maintenance and support. What makes a cloud application different from other applications is its scalability. This can be achieved by cloning tasks onto multiple virtual machines at run-time to meet the changing work demand**.** Load balancers distribute the work over the set of virtual machines. This process is transparent to the cloud user who sees only a single access point.

The pricing model for SaaS applications is typically a monthly or yearly flat fee per user [7] .so price is scalable and adjustable if users are added or removed at any point. SaaS is also often associated with a pay-as-you-go subscription licensing model.

This model is particularly focused on managing access to applications. For example, policy controls may dictate that a sales person can only download particular information from sales CRM applications. [8]

The architecture of SaaS-based applications is specifically designed to support many concurrent users at once. Software as a service applications are accessed using web browsers over the Internet therefore web browser

security is vitally important. Information security officers will need to consider various methods of securing SaaS applications. Web Services (WS) security, Extendable Mark up Language (XML) encryption, Secure Socket Layer (SSL) and available options which are used in enforcing data protection transmitted over the Internet. [9].Examples of SaaS include: Google Apps, Microsoft Office 365, Onlive, GT Nexus, Marketo,and TradeCard.

Combining the three types of clouds with the delivery models we get a holistic cloud illustration surrounded by connectivity devices coupled with information security themes.

Virtualized physical resources, virtualized infrastructure, as well as virtualized middleware platforms and business applications are being provided and consumed as services in the Cloud [10].

Image:-Cloud computing service delivery models

Underpinning a successful cloud infrastructure is delivering the required QoS levels to its users in a way that minimizes risk, which is measured in terms of a combination of the likelihood of an event and its impact on the provision of functionality. Earlier work in risk management for distributed systems has mainly focused on operational aspects such as failures and performance degradation, and assumed a very IaaS centric view under a specific resource reservation model [11].

As defined in COSO's 2004 Enterprise Risk Management – Integrated Framework3: "Risk is the possibility that an event will occur and adversely affect the achievement of objectives."

Cloud computing efficiently serves the dynamically growing storage and data processing needs; however it has also associated with a number of risks. The risks arise due to the various factors such as availability of the data, network load, the location of the data centres, data segregation, data integrity, lack of knowledge and transparency, about the governing policies. In a cloud computing environment, the resources are used when required and this is expected to translate into reduced costs of maintenance and elastic scalability. For example, in order to process a user request, the service provider decides upon the resources to be utilised for the particular task and when these resources needs to be released. Since the entire process is carried out by the service provider and not by the user, the security and integrity of the user's data becomes a significant concern.

The year 2011 was a banner year for cyber attacks and data breaches, and with cloud computing bringing information from various IT departments under a single physical server, the risks going forward are even greater.

Security breaches have become the most prominent topic, so as the pressure to protect the integrity and confidentiality of critical information has never been greater.

"Traditional systems are masked behind firewalls, NATs, and other gateway boundaries, so attackers must do intensive intelligence gathering to know that they exist, "explains Greg Day, security analyst at McAfee. Cloud services, on the other hand, are highly visible and are designed to be accessible from anywhere by anyone. As far as malicious hackers are concerned, that is like painting a large target on them. "Last year, Monster was hacked and millions of contact details stolen which unleashed a phishing attack," says Day. "When it comes to business services in the cloud, the cyber criminal only needs to hack one site to get access to multiple companies."

In the field of cloud computing there is a wide scope in security research, new solutions need to be evolved which help data centres to manage and secure vital user's information.

Today in the generation of technology where the world is getting interconnected, it has become more important to be aware and educated about the risks associated with cloud for everyone involving in the development of the product as well as for the client users. The cloud computing model provides cost savings through economies of scale, but it not only introduces the same risks as any externally provided service, it also includes some unique risk challenges.

The word "cloud" suggests something big and accessible, but externally opaque. You can't see into the cloud — you just assume that it works. Obviously, a service provider has far more flexibility by avoiding specifics about its location, staff, technology, processes or subcontractors. Increasingly, service is being offered by a chain of providers, each invisibly offering processing or storage services on behalf of a service provider that might not be directly controlling any of the technology, and each able to invisibly access unencrypted data in its facility. All this makes it easier for them to keep their costs down and scale to meet changing customer demands, but it also makes it harder to assess the risk to your organization from using such a service. Organizations potentially can gain a competitive or cost advantage through selective adoption of cloud computing, but not without first taking a comprehensive look at the associated risks, ensuring that they are consistent with business goals, along with the expectations of regulators, auditors, shareholders and partners. It is especially challenging to understand the risks associated with cloud computing, and CIOs, chief information security officers, compliance and privacy officers, and line-of-business managers should be involved in the risk assessment of new cloud-based services. cloud computing is becoming more popular than ever as more and more applications core to our businesses move into the cloud we need to consider some of our own risks.

According to Bob Laliberte, analyst at Enterprise Strategy Group- "Clouds pose more than just legal problems; there are technical ones, too."

Laliberte says. "It's even more with clouds. You have to try to manage someone else's hardware that's lying to you."He also said that "A lot of CIOs are interested in internal clouds, but they're leery of the performance issues and security inherent in the cloud environment"

According to survey [12,13],74% of IT Executives and Chief Information Officers are not willing to adopt cloud services due to the risks associated with security and privacy.

There are numerous challenges existing in the field of cloud computing, including data replication, consistency, limited scalability, unreliability, unreliable availability of cloud resources, portability (due to lack in cloud provider standard), trust, security, and privacy [14].

There are still some grey areas that need to be addressed, such as the security and privacy of user's data stored on cloud server(s), security threats caused by multiple virtual machines, and intrusion detection. Google like big fish in cloud invest a lot more in the security of their data centres than do small- or medium-size companies. When it comes to security, the giants simply have more money to spend.

If a company is considering the use of an external service of any sort, then it needs to:

- Assess the security, privacy and regulatory compliance risks
- Identify use cases that are inappropriate for this service delivery method, based on risk
- level and current controls
- Identify use cases that pose an acceptable level of risk for the service delivery method
- Choose and implement compensating controls before going fully operational [15].

Gartner recently outlined seven security issues:-

1. Privileged user access
2. Regulatory compliance
3. Data location
4. Data segregation
5. Recovery
6. Investigative support, and
7. Long-term viability

"The majority of the threats are going to come from conventional sources, "says Ken Munro, director of penetration and security testing company Secure Test. "You need to be able to log into the service, you need to give people a route to access it, you need protocols to send traffic to it." These raise classic issues, Munro suggests, and the problems are likely to be the standard ones of poorly implemented protocols, authentication processes and so on.

RISK ANALYSIS

SECURITY— security is a process of preventing system, information and services from unintended or unauthorized access, or vulnerable attacks. Today, business is being transacted virtually everywhere which provide us endless opportunities, but risks also come along with as a free gift. As far as cloud concerns, it requires secure interfaces between users and the outermost devices on a network; between the outermost devices on a network and backend infrastructure; and between services. The cloud however is said to be more susceptible to data leaks and attacks than old networking implementations like traditional solutions**.** Using a cloud service provider (CSP) can complicate privacy of data because of the extent to which virtualization for cloud processing (virtual machines) and cloud storage are used to implement cloud service [16]. A perceived lack of privacy is another reason some companies has been reluctant to put their data in the cloud. They don't want anyone—including the cloud provider—to have access to their data. From a security and risk perspective, it is the least transparent externally

sourced service delivery method, storing and processing data externally in multiple unspecified locations, often sourced from other, unnamed providers, and containing data from multiple customers. Seven important identity factors for risk in a cloud computing model are: Access, Availability, and Network load, Integrity, Data Security, Data Location and Data Segregation.

USER ACCESS CONTROL-According to Gartner cloud computing is a style of computing where massively scalable IT-enabled capabilities are delivered as a service to external customers using Internet technologies. In a private organization only the authenticated users can access the data but an inherent risk of unauthorized access of data is always there in processing the sensitive data stored on a cloud-outside the enterprise. Organizational managers are not much aware of the nature and level of such risks, and they cannot control these risks directly. The Amazon Web Services platform, designed with application tools predicated on social networking design objectives of being purely collaborative and egalitarian by default share every data element in an Amazon Web Services account. This has led to users being able to see other user's information and the ability to even run reports in other's Amazon Web Services Accounts (Siegel, et.al.). Depending on the cloud solution used (SaaS, PaaS, or IaaS), a cloud customer organization may be unable to obtain and review network operations or security incident logs because they are in the possession of the CSP. The CSP may be under no obligation to reveal this information or might be unable to do so without violating the confidentiality of the other tenants sharing the cloud infrastructure.

AVAILABILITY- Availability plays a major role in IT especially when it relates to cloud computing since the needs of the customers is likely to be attended on time. Public and private cloud providers depend on system availability and uptime. According to a survey- on an average a cloud service is down for an average of 7.5 hours yearly. Amadeus, a travel service providers, pegs it outages cost at $89,000 per hour while Paypal computes its outages cost at $225,000 per hour. The International Working Group on Cloud Computing Resiliency (IWGCR) concluded that the total downtime of 13 well-known cloud services since 2007 amounts to 568 hours, which has an economic impact of around $71.7 million dollars. A recent report from International Working Group on Cloud Computing Resiliency (IWGCR) says customers have suffered 568 hours of downtime from 13 well-known cloud services since 2007, which resulted in $71.7 million of economic loss. In July, 2012 Amazon cloud infrastructure suffered a power outage last week, creating problems for their clients which lasted more than 24 hours. This resulted in a loss of

According to ENISA probability, impact, vulnerabilities, affected assets, and effect of lock-in is as follows:-

Probability	**VERY HIGH**	**Comparative: Higher**
Impact	VERY HIGH (depends on organization) (IaaS VERY HIGH, SaaS Low)	Comparative: Equal
Vulnerabilities	❑ Unclear roles and responsibilities ❑ Poor enforcement of role definitions ❑ Synchronizing reponsibilities or contractual obligations external to cloud ❑ SLA clauses with conflicting promises to different stakeholders ❑ Audit or certification not available to customers ❑ Cross-cloud applications creating hidden dependency ❑ Lack of standard technologies and solutions ❑ Storage of data in multiple jurisdictions and lack of transparency about **THIS** ❑ No source escrow agreement ❑ No control on vulnerability assessment process ❑ Certification schemes not adapted to cloud infrastructures ❑ Lack of information on jurisdictions ❑ Lack of completeness and transparency in terms of use ❑ Unclear asset ownership	
Affected assets	❑ Company reputation ❑ Customer trust ❑ Employee loyalty and experience ❑ Personal sensitive data ❑ Personal data ❑ Personal data - critical ❑ Service delivery – real time services ❑ Service delivery	
Risk	**HIGH**	

SOURCE: - http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment

confidence among the customers and the vendors. Every cloud provider should develop such mechanism which provides high availability, replication, and disaster recovery solutions to achieve the necessary reliability.

NETWORK LOAD- cloud-computing service model proves to be more cost effective to make the capital investment for an internal platform .but at the same time bandwidth to and from the cloud provider is a bottleneck for the cloud computing. When applications use or generate very large amounts of data then the application users may find that there's just not sufficient bandwidth available to jostle the data through, given the network bandwidth made available by appropriate carriers. If the capacity of the cloud is greater than 80%, then the computers can become unresponsive due to high volumes .The computers and the servers crash due to high volume motion of data between the disk and the computer memory. The percentage of capacity threshold also poses a risk to the cloud users. When the threshold exceeds 80%, the vendors protect their services and pass the degradation on to customers. It has been indicated that in certain cases the outage of the system to the users are still not accessed [17].

LOCK-IN: Many cloud service providers offer application software development tools, procedures or standard data formats or services interfaces with their cloud solutions. When these tools are proprietary, clients may create applications that work only within the cloud service providers ''s specific solution architecture- that is there could be no guarantee of data, application and service portability. And it could also make difficult for the customer to migrate from one provider to another or migrate data and services back to an in-house IT environment. Thus, the fundamental aspect of data portability is not available and there would be a dependency on a particular service provider.

RELIABILITY AND PERFORMANCE ISSUES- The crucial problem with cloud computing is lack of desired reliability and security. Both of these key features need to be duly and timely assessed in order to manage cloud computing. NIST says that "For the cloud, reliability is broadly a function of the reliability of four individual components: (1) the hardware and software facilities offered by providers, (2) the provider's personnel, (3) connectivity to the subscribed services and (4) the consumer's personnel,". A problem in any one of those areas can have repercussions [18].

Another challenge with cloud computing is a risk of system failure .Although service-level agreements can be structured to meet particular requirements, Cloud Service Provider's solutions might sometimes be unable to meet these performance metrics if a cloud tenant or incident puts an unexpected resource demand on the cloud infrastructure.

In 2011 the high visibility outage impacted many companies that depend on Amazon for either primary or overflow computing and storage services. Impacting a large number of databases, applications and sites across the web, the outage shows just how pervasive use of cloud computing has become [19].

LACK OF TRANSPARENCY – Transparency is of key importance for a fair and legitimate processing of personal data. Directive 95/46/EC obliges the cloud client to provide a data subject from whom data relating to him are collected with information on his identity and the purpose of the processing. The cloud client should also provide any further information such as on the recipients or categories of recipients of the data, which can also include processors and sub-processors in so far as such further information is necessary to guarantee fair processing in respect of the data subject (cf. Article 10 of the Directive).A corresponding duty to inform the data subject exists when data that have not been obtained from the data subject himself, but from different sources are recorded or disclosed to a third party (cf. Article 11).But it has seen that usually cloud service providers are unlikely to divulge detailed information about its processes, operations, controls, and methodologies. Due to insufficient information about a cloud service's processing operations poses a risk to controllers as well as to data subjects because they might not be aware of potential threats and risks and thus cannot take measures they deem appropriate

LACK OF ISOLATION: Sustainability in Cloud is a matter of privacy, which in Cloud is called "isolation". A cloud provider may use its physical control over data from different clients to link personal data. If administrators are facilitated with sufficiently privileged access rights, they could link information from different clients. The basic characteristics of cloud computing are multi-tenancy and shared resources. On the other side of the coin these characteristics imposes the threat of the failure of mechanisms separating storage, memory, routing and even reputation between different tenants (e.g., so-called guest-hopping attacks).

COMPLIANCE RISKS: Compliance includes correspondence of the appearance of the constitute specifications, standards and Law. So the compliance are one of the most important issue in cloud computing In spite of the fact that cloud computing offers exciting and cost-effective ways for businesses to enhance their computing capacity while also lowering their costs. Yet the risks presented by outsourcing computing capacity come with significant legal and compliance implications. It is not possible to ensure regulatory compliance every time and sometimes it's impossible. Jim Haskin, senior vice

president at Websense Inc stated that "It is difficult to take full responsibility for who can access data, who sees it and how it is stored, since the premise of the cloud is that customers don't necessarily need to know or care where their data is" .However ,there is always an user organization is responsible for figuring out who is doing what to its data and requiring assurances about the data staying in compliance, but in certain cases, using a cloud infrastructure implies that certain kinds of compliance cannot be achieved (e.g., PCI DSS (4)).Many of the regulations like Payment Card Industry Data Security Standard (PCI DSS) , the Health Insurance Portability and Accountability Act (HIPAA), require regular reporting and audit trails. Cloud providers must enable their customers to comply appropriately with these regulations [20].The key to managing such risks is effective due diligence by management and its auditors.

According to ENISA probability, impact, vulnerabilities, affected assets, and effect of compliance risk is as follows:-

Probability	**VERY HIGH -** depends on PCI, SOX	**Comparative: Higher**
Impact	HIGH	Comparative: Equal
Vulnerabilities	❑ Audit or certification not available to customers ❑ Lack of standard technologies and solutions ❑ Storage of data in multiple jurisdictions and lack of transparency about this ❑ Certification schemes not adapted to cloud infrastructures ❑ Lack of information on jurisdictions ❑ Lack of completeness and transparency in terms of use	
Affected assets	Certification	
Risk	**HIGH**	

SOURCE: - http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment

DATA LEAKAGE: A cloud environment is a multitenant environment where resources are shared by organisations and applications. This sharing involves a huge risk of data leakage which is not presented when one organisation or an individual uses the dedicated server and other resources. Moreover cloud users usually find difficult to ensure that whether their data is handled in a lawful way. This risk of data leakage presents an additional point of consideration with respect to meeting data privacy and confidentiality requirements.

According to ENISA probability, impact, vulnerabilities, affected assets, and effect of data leakage is as follows:-

Probability	**HIGH**
Impact	HIGH
Vulnerabilities	❑ Lack of information on jurisdictions ❑ Storage of data in multiple jurisdictions and lack of transparency about this
Affected assets	❑ Company reputation ❑ Customer trust ❑ Personal sensitive data ❑ Personal data ❑ Personal data - critical ❑ Service delivery – real time services ❑ Service delivery
Risk	HIGH

SOURCE: - http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment

INSECURE OR INCOMPLETE DATA DELETION:

A cloud provider may not provide the necessary measures and tools to assist the controller to manage the data in terms of, e.g., access, deletion or correction of data. When client asks for deletion of his data, its may possible that the data would not delete completely, as data could be stored on multiple clients on cloud. Hence multiple tenancies and the reuse of hardware resources represent a higher risk to the customer than with dedicated hardware.

MALICIOUS INSIDER: the damage of the data which may be caused by malicious insiders has been proved far greater. Cloud architectures necessitate certain roles which are extremely high-risk. Examples include CP system administrators and managed security service providers.

DATA LOCATION AND LACK OF CONTROL

In cloud-computing model, it is difficult for the user to know their data storage location. Indeed in a globalized

infrastructure, user might not even know in which country your data is stored, who is responsible for meeting national privacy regulations. Similarly several questions arises on the part of the cloud service providers, for instance, Will providers commit to storing and processing data in specific jurisdictions? If you are operating within a jurisdiction that has specific privacy requirements, is the provider willing to give a contractual commitment to obey the law on your behalf? Cloud users may no longer be in exclusive control of this data and cannot deploy the technical and organisational measures necessary to ensure the availability, integrity, confidentiality, transparency, isolation, intervenability and portability of the data.

DATA SEGREGATION

Data Segregation is not easily facilitated in all cloud environments as all the data cannot be segregated according to the user needs. Cloud computing is not an environment which works in a toolkit. The compromised servers are shut down whenever a data is needed to be recovered. The available data is not correctly sent to the customer at all times of need. When recovering the data there could be instances of replication of data in multiple sites. Arnon Rosenthal said that-the restoration of data must be quick and complete to avoid further risks. We examine how cloud computing is assessed in a biomedical laboratory which experiences risks due to hackers .The Data Base Manage System (DBMS) and web servers face vulnerability if the infrastructure of the cloud is not properly designed. There are certain non technical risks which arise due to outsourcing of information. Encrypting the data from the technical aspect is important to ensure that the data is not hacked or attacked. Strong encryption is needed for sensitive data and this would mean increased costs. Table provides a summary of the security mechanisms provided by major cloud service providers.

Security Issues	Results
Password Recovery	90% use common services10% use sophisticatedtechniques
Encryption Mechanism	40% use SSL encryption, 20% use encryption mechanism 40% utilize advanced methods like HTTP
Data Location	70% of data centres are located more than onecountry
Availability History	40% indicate data loss 60% indicates data availability is good
Proprietary/Open	10% have open mechanism
Monitoring Services	70% provide extra monitoring services 10% uses automatic techniques 20% are not open about the issue

Table: **Security Mechanisms of Service Providers**

Source- http://www.idt.mdh.se/kurser/ct3340/ht10/FinalPapers/16-Sneha_Mridula.pdf

ENISA specifies the technical risks, what is probability, impact, vulnerabilities, affected assets of this risk:-

Probability	Inability to provide additional capacity to a customer: MEDIUM	Comparative: N/A
	B. Inability to provide current agreed capacity level: LOW	Comparative: Higher
Impact	**A**. Inability to provide additional capacity to a customer: LOW/ MEDIUM (e.g., at Christmas)	Comparative: N/A
	B. Inability to provide current agreed capacity level: HIGH	Comparative: Same
Vulnerabilities	Inaccurate modelling of resource usage. Inadequate resource. Provisioning and investments in infrastructure. No policies for resource capping. Lack of supplier redundancy	
Affected Assets	Company reputation Customer trust Service delivery Access control / authentication / authorization (root/admin v others)	
Risk	**MEDIUM**	

SOURCE: - http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment

RESEARCH RECOMMENDATIONS

ENISA in its research recommended the following as priority areas for research in order to improve the security of cloud computing technologies:

BUILDING TRUST IN THE CLOUD

- Certification processes and standards for clouds: more generally, cloud computing security lifecycle standards that can be certified against cloud specific provisions for governance standards – COBIT (52), ITIL (53), etc;
- Metrics for security in cloud computing;
- Return on security investments (ROSI): the measures cloud computing can enable to improve the accuracy of ROI for security;
- Effects of different forms of reporting breaches on security;
- Techniques for increasing transparency while maintaining appropriate levels of security:
  - Tagging, e.g., location tagging, data type tagging, policy tagging
  - Privacy preserving data provenance systems, e.g., tracing data end-to-end through systems;
- End-to-end data confidentiality in the cloud and beyond:
  - Encrypted search (long term)
  - Encrypted processing schemes (long term)
  - Encryption and confidentiality tools for social applications in the cloud
  - Trusted computing in clouds, e.g., trusted boot sequences for virtual machine stacks;
- Higher assurance clouds, virtual private clouds, etc;
- Extending cloud-based trust to client-based data and applications.

DATA PROTECTION IN LARGE-SCALE CROSS-ORGANIZATIONAL SYSTEMS

The following areas require further research with respect to cloud computing:

- Data destruction and lifecycle management
- Integrity verification - of backups and archives in the cloud and their version management
- Forensics and evidence gathering mechanisms
- Incident handling - monitoring and traceability
- Dispute resolution and rules of evidence
- International differences in relevant regulations, including data protection and privacy
  - Legal means to facilitate the smooth functioning of multi-national cloud infrastructures
  - Automated means to mitigate problems with different jurisdictions.

LARGE-SCALE COMPUTER SYSTEMS ENGINEERING

- Security in depth within large-scale distributed computer systems;
- Security services in the cloud – de-parameterisation of security technologies and the adaptation of traditional security perimeter control technologies to the cloud, e.g., HSMs, web filters, firewalls, IDSs, etc;
- Resource isolation mechanisms - data, processing, memory, logs, etc;
- Interoperability between cloud providers;
- Portability of VM, data and VM security settings from one cloud provider to another (to avoid vendor lock-in), and maintaining state and session in VM backups and the long distance live migration of virtual machines;
- Standardization of interfaces to feed data, applications and whole systems to the cloud – so that every OS can develop the corresponding client interface;
- Resource (bandwidth and CPU, etc) provisioning and allocation at scale (elasticity);
- Scalable security management (policy and operating procedures) within cloud platforms:
  - automatic enforcement of security and data protection policies
  - secure operating processes of providers - the implementation of governance processes;
- Resilience of cloud computing - how to improve the resilience of a cloud:
  - use of cloud architectures at the client side (edge networks, p2p, etc)
  - aggregating multiple client networks
  - client-based redundancy and backup;
  - cloud bursting and global scale resilience in clouds.

In today's open business environment, managing security and access risk can be extremely challenging .Security has become a hot topic these days and many people have ideas about what should be done to achieve it. For years, the focus of many software vendors was on security features. Add a firewall. Add SSL to secure data flows. Positive security features are great, but they don't

do much to address every potential security issue that result from insecure code. However, data encryption, identity management, continuous monitoring, physical surveillance and more help assess and mitigate potential security breaches [21].

The security and privacy protection services can be achieved with the help of secure cloud application services. In addition to security and privacy, the secure cloud application services provide the user management, key management, encryption on demand, intrusion detection, authentication, and authorization services to mobile users. To provide the transparent cloud environment, cloud users must have the facility to audit the security level of the hosted services. The audit can be done with the help of a cloud service monitor. The cloud service monitor examines the security level and flows of the running environment. The security level should meet the user security requirements and the flow of the running environment should be normal. The security verification of uploaded data on cloud can be done using a storage security verification service. The physical security of the data centre plays a very important role to achieve security and privacy. Physical security deals with the measures taken to avoid unauthorized personnel physically accessing the resources of the cloud service provider. Physical security can be achieved with the help of security guards, video surveillance security lighting, sensors, and alarms. The researchers have done a massive amount of work [22–29] to provide an energy-aware high performance computing environment.

CONCLUSION

Recently, news broke of Dropbox allegedly misleading customers regarding the levels of data protection provided by its service. This occurred shortly after Amazon's EC2 service experienced major outages. With these and other events, media reports are asking, "Is this the end of the innocence of the cloud computing ideal?" The reality is that, as cloud services struggling in its infancy, there will be some derailments along the way.

Pasik and Coughlin believe: All businesses should be thinking about the cloud. "If you don't become educated about cloud computing and the potential it has for expanding your business and lowering operating costs, you will be at a significant competitive disadvantage.

In this paper we had discussed some of the issues related to risks, there are number of risks and uncertainties in transitioning to the cloud, and it appears that the security systems of cloud computing requires an in-depth analysis, strong governance and control are an essential part of any decision to transition to the cloud because cloud systems can be exploited via various vulnerabilities. Client's request can be manipulated during data transit from the client to the cloud system. This make possible for the intruder to gain unauthorised access to the cloud system. And by this unauthorized access an intruder can even damage the cloud system or can affect the cost of the cloud services-client may have to pay more charges than utilization, or they can make cloud client unable to request for the services. It is often possible, and in some cases advisable, for the cloud customer to transfer risk to the cloud provider; however not all risks can be transferred. If a risk leads to the failure of a business, serious damage to reputation or legal implications, it is hard or impossible for any other party to compensate for this damage. Ultimately, you can outsource responsibility but you can't outsource accountability. Cloud computing is relatively new term, thus it has to face several issues in gaining recognition for its merits. Its security deficiencies and benefits need to be carefully weighed before making a decision to implement it. However, several people get attracted towards this topic and pursuing research to improve on its drawbacks.

RERERENCES

1. The NIST Definition of Cloud Computing". National Institute of Science and Technology, 24 July 2011.
2. Stevens, Alan,"When hybrid clouds are a mixed blessing", March 28, 2012.
3. http://en.wikipedia.org/wiki/Cloud_computing.
4. J. Brodkin,"Gartner: Seven cloud-computing security risks." *InfoWorld*, Available: <http://www.infoworld.com/d/security-central/gartner-seven-cloudcomputingsecurity-risks-853? Page=0, 1, Mar. 13, 2009.
5. http://en.wikipedia.org/wiki/Cloud_computing.
6. Global Netoptex Incorporated. "Demystifying the cloud. Important opportunities, crucial choices." pp4-14, Available: http://www.gni.com [Dec. 13, 2009].
7. Chou, Timothy, *Introduction to Cloud Computing: Business & Technology*.
8. *Mark O'Neill, Vordel for CSO, SaaS, PaaS, and IaaS: A security checklist for cloud models,January 31, 2011,Available-http://www.vordel.com/company/news/articles/31-01-11.html.*
9. S. Subashini, and V. Kavitha. (2010) "A survey on security issues in service delivery models of cloud computing." *J Network Comput Appl* doi:10.1016/j.jnca.2010.07.006. Jul.2010.

10. M. Klems, A. Lenk, J. Nimis, T. Sandholm and S. Tai. "What's Inside the Cloud? An Architectural Map of the Cloud Landscape." *IEEE Xplore*, pp 23-31, Jun. 2009.
11. K. Djemame, I. Gourlay, J. Padgett, K. Voss, O. Kao, Risk Management in Grids, in: R. Buyya, K. ubendorfer (Eds.), Market-Oriented Grid and Utility Computing, Wiley, 2009, pp. 335–353
12. S. Subashini, V. Kavitha, A survey on security issues in service delivery models of cloud computing, Journal of Network and Computer Applications 34 (1) (2011) 1–11)
13. R. Buyya, C.S. Yeo, S. Venugopal, J. Broberg, I. Brandic, Cloud computing and emerging IT platforms: vision, hype, and reality for delivering computing as the 5th utility, Future Generation Computer Systems 25 (6) (2009) 599–616.
14. D. Zissis, D. Lekkas, Addressing cloud computing security issues, Future Generation Computer Systems 28 (3) (2012) 583–592.
15. http://ccskguide.org/top-threats-to-cloud-computing/
16. Winkler, Vic (2011). *Securing the Cloud: Cloud Computer Security Techniques and Tactics*. Waltham, Massachusetts: Elsevier. p. 60. ISBN 978-1-59749-592-9.
17. Ortuatay B. "Twitter service restored after hacker attack", Journal *of the Baltimore Sun*, 2009.
18. NIST: Cloud reliability, information security remain 'open issues', Available: http://www.fiercegovernmentit.com/signup? sourceform= Viral-Tynt-FierceGovernmentIT-FierceGovernmentIT.
19. John Bair,On the Reliability of Cloud Computing , April 27, 2011,Available :- http://www.b-eye-network.com/view/15180.
20. http://en.wikipedia.org/wiki/Cloud_computing_security
21. security risk mgmt-http://blog.courion.com/access_risk_management_blog/?Tag=access+risk+management——for risk mgmt-'.
22. C.O. Diaz, M. Guzek, J.E. Pecero, P. Bouvry, S.U. Khan, Scalable and energy efficient scheduling techniques for large-scale systems, in: Proc. 11th IEEE Int.Conference on Computer and Information Technology, CIT '11, Pafos, Cyprus,Sep. 2011.
23. C. Cai, L. Wang, S.U. Khan, J. Tao, Energy-aware high performance computing: a taxonomy study, in: Proc. 17th IEEE Int. Conference on Parallel and Distributed Systems, ICPADS '11, Tainan, Taiwan, Dec. 2011.
24. I. Goiri, J.L. Berral, J.O. Fitó, F. Julià, R. Nou, J. Guitart, R. Gavaldà, J. Torres,Energy-efficient and multifaceted resource management for profit-driven virtualized data centres, Future Generation Computer Systems 28 (5) (2012)718–731.
25. D. Kliazovich, P. Bouvry, S.U. Khan, DENS: data center energy-efficient network-aware scheduling, in: Proc. ACM/IEEE Int. Conference on Green Computing and Communications, GreenCom '10, Hangzhou, China, Dec. 2010.
26. P. Lindberg, J. Leingang, D. Lysaker, S.U. Khan, J. Li, Comparison and analysis of eight scheduling heuristics for the optimization of energy consumption and makespan in large-scale distributed systems, Journal of Supercomputing 59 (1) (2012) 323–360.
27. D.M. Quan, F. Mezza, D. Sannenli, R. Giafreda, T -alloc: a practical energy efficient resource allocation algorithm for traditional data. [26] C.O. Diaz, M. Guzek, J.E. Pecero, G. Danoy, P. Bouvry, S.U. Khan, Energyaware fast scheduling heuristics in heterogeneous computing systems, in: Proc. ACM/IEEE/IFIP Int. Conference on High Performance Computing and Simulation, HPCS '11, Istanbul, Turkey, July 2011.
28. S.U. Khan, C. Ardil, A weighted sum technique for the joint optimization of performance and power consumption in data centers, International Journal of Electrical, Computer, and Systems Engineering 3 (1) (2009) 35–40.
29. S.U. Khan, A self-adaptive weighted sum technique for the joint optimization of performance and power consumption in data centers, in: Proc. 22nd Int. Conference on Parallel and Distributed Computing and Communication Systems, PDCCS '09, Louisville, KY, USA, Sep 2009. However, there is also a need for energy-efficient security frameworks for mobile devices to provide security and privacy services in an cloud computing environment [29]. Ref(W. Ren, L. Yu, R. Gao, F. Xiong, Lightweight and compromise resilient storage outsourcing with distributed secure accessibility in mobile cloud computing,Journal of Tsinghua Science and Technology 16 (5) (2011) 520–528.)