Security in Cloud Computing

Rajarshi Roy Chowdhury
American International University-Bangladesh

Security in Cloud Computing

Rajarshi Roy Chowdhury
Lecturer, Dept. of CSE
Sylhet International University
Shamimabad, Sylhet

ABSTRACT

Cloud computing refers to high scalable computing applications, storages and platforms as a service to companies, individuals and governments. Therefore, SMB (Small and Medium Business) organizations are adapting cloud computing services gradually to save cost and to increase efficiency in their business environment. While cloud service benefits and robustness are comprehensible, but now more concern about security in cloud computing "How much secure is cloud computing environment?". Noted that security is one of the main barrier for continuing growth of cloud computing. For some major security risks and issues enterprises and individuals are unwilling to deploy their data and applications in cloud environment. In this paper, the main objective is to identified major security risks and issues those are need to think about during deployment and development of services in cloud and the way how to mitigate those security risks and issues. However, it is significant to know that, cloud computing is not insecure primarily, it just needs to be managed and accessed securely.

Keywords

Cloud computing, Service models, Security risks and issues, Risk mitigation and Cloud services.

1. INTRODUCTION

IT (Information Technology) industries are driving technology to a new arena from time to time. The Internet is one of the most popular technology now-a-days by the elegance of IT. Now it is on the edge of revolution, where resources are globally interconnected. Hence, resources can be easily shared and managed from anywhere and anytime. Cloud computing is the main element of this standard, that provides a large storage area where resources are available from everywhere to everyone as a service rather than as a product. Throughout in the history of computer science various attempts have been made to release users from the needs of computer hardware (such as storage) and software, since time-sharing utilities envisioned in 1960s, network computers in 1990s and commercial grid computing to cloud computing in more recent years. Cloud computing comes focus only when think about what IT always needs: a way to increase the capabilities of a system on fly without investing any new infrastructure, training a new personnel and licensing of any new software. Today cloud services provide subscription or pay-per-use based service; the services provide over the Internet in real time, in which extends basic IT capabilities into robust area. The SMB companies are realizing that simply by tapping into cloud environment they can gain fast access to best business applications facilities and dramatically boost their resource infrastructure at very minimum cost "[1]".

Cloud services are mainly focus to reduce overall client side requirements (hardware and software) and complexity. It has been changing IT delivery model for services since cloud services introduced in 1990. From the statistic shown that massive developments and implementations of cloud computing services market is likely to accomplish between $150 billion and $222.5 billion respectively in 2014 and 2015 "[2]". Although many benefits are introduced in cloud computing uses, but great deal of risks and issues are associated with implementation, management, disaster recovery, business continuity, regulation and legislations and lack of standards and guidelines in cloud computing technologies. According to IDCI survey in 2009, 74% of IT executives and CIO's (Chief Information Officer) cited that security is the top challenge to prevent adoption of cloud services "[3]". Management of cloud services always under presser to ensure adequate mitigation of risks to reduce impact on business. There are some major security challenges arise as a result of cloud computing where application software and databases are moved to untrustworthy large data centers. This concept poses many security challenges such as – web application vulnerabilities, SQL (Structured Query Language) injection and cross-site scripting, physical access and privacy control issues come up from third parties having control over physical data, identity and credential management issues crop up for data verification, integrity and confidentiality relates for authentication in terms of respondent devices. The main focus of this study is to describe various security issues due to cloud service delivery models and provides some recommendation to mitigate cloud computing risks as for development guidelines and standards for secure cloud computing environment.

This paper is organized as follows: Background is discussed in Section 2. Motivation of this work is discussed clearly in Section 3. Cloud computing benefits and related works are discussed accordingly in Section 4 and 5. Cloud computing risks are conversed in Section 6 and security issues in Section 7. Mitigation of security risks are discussed in Section 8. Finally Recommendation and Conclusion are discussed accordingly in Section 9 and 10.

2. BACKGROUND OF CLOUD COMPUTING

Cloud computing resulted from the convergence of Grid computing technology. In an early 1990s, high performance computers were interconnected via fast data communication link to support complex and scientific calculation. Grid computing defines – a hardware and software infrastructure that provides consistent, pervasive and inexpensive access to high-end computational facilities over communicational network.

A. Cloud Computing

Cloud computing refers to an promising model of computing technology where machines with large data centers can be dynamically provisioned, configured, controlled and reconfigured to deliver services in a scalable manner. It is an innovative IS (Information System) architecture; where visualization as what may be the future of computing "[4]". As being refers to cloud computing, it delivers computing as a service rather than as a product; in which share resources, application software and information to provide computers or other electronic devices as a utility over the Internet in real time. There is a logical diagram of the cloud computing technologies as shown in "Fig 1".

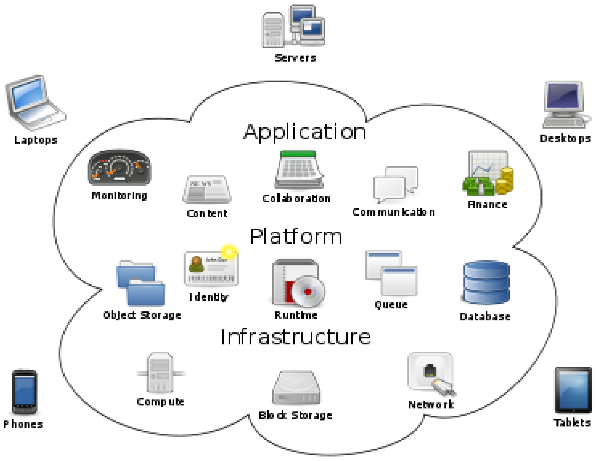


Fig 1: Logical cloud computing

In this diagram, cloud computing service models are all inside in the cloud sing and laptops, desktops, phones and tablets are acts like clients to get services from the cloud. Servers provide services to clients according to their request or pay base. Cloud computing provides a shared pool of configurable IT resources on demand, in which needs minimal effort of management to get better services. Services are based on various agreement SLA (Service Level Agreement) between service providers and consumers. There are some key characteristics of cloud computing as follows:

- **Application Programming Interface (API)** – To enable a machine to interact with cloud software as the same way the interaction between humans/users and computers by using interface services.
- **Maintenance** – Applications are not necessarily to be installed in each client's system, therefore easy to support maintenance.
- **Performance** – Web services are constructed by using loosely couple techniques and consistent architectures and monitoring systems to improve services.
- **Scalability and Elasticity** – Any number of nodes can be added and dropped at any time without much modification of infrastructure and software. A user can get required services without any human interaction. In most cases cloud system scales up automatically.
- **Broad Network Access** – Cloud services are available over the network, therefore a standard mechanisms are used to provide services on heterogeneous platforms.
- **Location Independency** – Users are unacquainted about exact location of services except high level of abstraction regard services, such as country, state.
- **Reliability** – Multiple redundant sites are made for cloud computing environment to support continuity and disaster recovery service for businesses.
- **Cost Effectiveness** – Centralize infrastructure enables sharing of costs in between large number of users from same or variant locations, such as real estate, electricity (e.g. deployment of cloud services near to the cheap power stations).
- **Sustainability** – Appropriate resource utilizations for efficient system.
- **Security** – Due to centralize data center it is possible to improve the level of data security. In present time security is better than the traditional systems, as service providers are able to offer some kind of services to resolve security issues that may not be able to afford by a consumer or a company individually. However, complexity of the security is increased when decentralization of data over the wide area of network and various devices are used to get services. But private deployment model of cloud computing service provides an organization to control information or data security. "[4]"

B. Service Delivery Models

Cloud is the Internet based computing environment where shared resources, software and information as a service to consumer(s) on demand. Service models are following hierarchy standard to provide services over the network. There are three fundamental service models, such as:

- **Software as a Service (SaaS)** – To deliver software as a service over the Internet through slender client interface such as web browser. SaaS reduces the need for customer's computer or server to install, manage and run all applications, such as: Facebook, SalesForce.
- **Platform as a Service (PaaS)** – To deliver a computing platform as a service for software development, storage and hosting over the Internet. A consumer does not require to control fundamental cloud infrastructure but has control to deploy applications, such as: WOLF (cloud middleware), Windows Azure (cloud OS).
- **Infrastructure as a Service (IaaS)** – To deliver infrastructure as a service along with storage and network, typically makes obtainable virtualization. Services are paid by consumers based on amount of resources consumed, such as: virtual servers leased by Amazon, GoGrid.

There are some other service models exists apart from the three vital (SaaS, PaaS and IaaS) molds, such as: CaaS (Communication as a Service), STaaS (STorage as a service), DTaaS (DeskTop as a Service), ITaaS (IT as a service), CCaaS (Compute Capacity as a Service) and BPaaS (Business Process as a Service) "[2]". Basic layers of cloud computing architecture are listed in "Table 1", where in client-server model how services are provided on hierarchically.

Table 1. Basic Cloud Computing Layers

Layers	Examples
Client	Computers, phones, other electronic devices, operating systems and browsers.
Application (SaaS)	Facebook, SalesForce, BaseCamp.
Platform (PaaS)	Google App Engine, Force.com, Windows Azure, WOLF.
Infrastructure (IaaS)	Virtual servers leased by Amazon, Rackspace, GoGrid.
Server	Multi-core processors, cloud-specific operating systems and combined offerings.

C. Cloud Computing Deployment Models

There are three fundamental deployment models for cloud computing environment but NIST (National Institute of Standards and Technology) proposed four set of deployment models, all are listed in "Table 2" "[5]".

- **Public Cloud** – In this model of cloud infrastructure represents a cloud environment which is publicly accessible and manageable by an organization or a third party cloud service providers.
- **Private Cloud** – This model of infrastructure is managed and operated only by private organization. The primary goal of this type of cloud model is to sustain consistent level of security and privacy.
- **Community Cloud** – This type of model shares infrastructure between organizations or communities have common mission and vision such as: security, jurisdiction. Services are managed by organizations or third parties.
- **Hybrid Cloud** – This type of deployment model is composition of two or more cloud models; they are bound together but each of them remains unique entities.

"[4]"

Table 2. Cloud Computing Development Models

Models	Managed By	Infrastructure		Accessible and Consumed By
		Owned By	Located	
Public	TPP	TPP	Off-P	Un-trusted
Private	Org	Org	On-P	Trusted
	TPP	TPP	Off-P	
Community	TPP	TPP	On-P	Trusted & Un-trusted
Hybrid	Org & TPP	Org & TPP	Off-P & On-P	

Note: Org: Organization, TPP: Third Party Provider, Off-P: Off Premise, On-P: On Premise.

3. MOTIVATION OF CLOUD COMPUTING

Cloud computing is the Internet based computing technology, which is empowered by virtualization. It describes a new model of IT services based on user consumption and delivery services. Virtualization is the creation of virtual or logical version rather than physical such as: hardware, platform, operating system and storage or network resources. Virtualization in cloud computing achieves high level of resource utilization by allowing one server to compute several task concurrently. The main motive of cloud computing is to offer robustness and ease traffic congestion for IT services over the network. In business environment cloud computing concept is growing fast to increase facilities. Gradually more and more individuals and companies are placed information and data in cloud environment, thus arise a number of serious issues, such as: how much secure their services, how service providers are providing data and application safety in cloud environment. Despite of all beneficial services enterprise customers are still unwilling to deploy their business in cloud. In where, security is the major issue to reduce the growth of cloud computing adaption. According to E-Crime study conducted by E-Crime congress collaboration with KPMG in 2009, stated that 63% of respondents mentioned that their customers were predominately affected by poisoned websites in cloud. In addition, around 40% of total respondents said that there had been an increased attacked against their customers by technical sophistication "[6]". New risks and possible threats are exploited in cloud computing services. It is necessary to analysis and understand cloud computing risks and threats in order to protect systems and data from vulnerabilities. Improvement of cloud computing security mechanisms are primary step towards to ensure secure cloud computing environment. Consumer only can rely on cloud computing if their services are secure enough to use. There some security challenges are needed to concern such as: application security, data transmission security, storage security and security related to use third party resources.

4. BENEFITS OF USING CLOUD COMPUTING

Cloud computing provides highly scalable computing environment for an assortment of IT services. It provides services to client individual, to big organizations or companies. As a result, IT departments and individuals are saved application developments, deployments, securities, purchasing new hardware and software and maintenance time and cost effectively. Cloud service helps to reduce power consumption, cooling, storage and uses space for cloud users or consumers in cloud environment. There are two key factors for an organization to concern: Going green and saving charge. In general, most of the benefits are shown based on bar chart in 'Fig 2' from most significant to lest significant according to the numbers from 1to13.

Note:

1	Cost efficiency	8	Deployments & change management
2	Scalability	9	Performance
3	Flexibility	10	Mobility
4	Agility	11	Automation & supported management
5	IT Resource management and business	12	Security
6	Efficiency	13	Green-IT data center
7	Reliability and Availability		

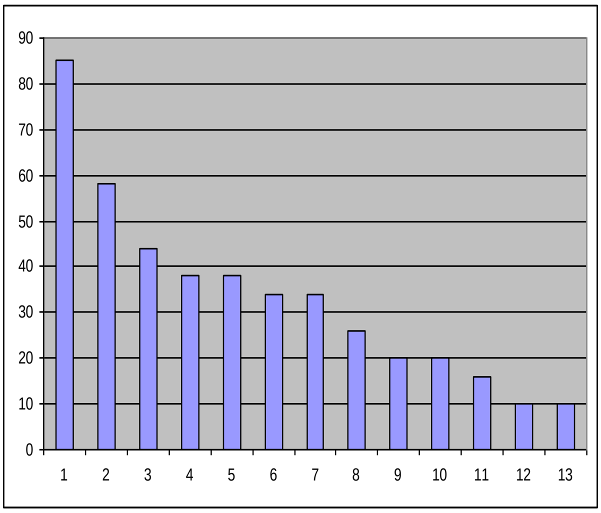


Fig 2: Benefits of cloud computing

From this chart, it is comprehensible that the main key features to adapt cloud computing to minimize cost efficiently. Other benefits are arranged according to their significant features such as: scalability, flexibility, agility, better IT resource management and business focus, efficiency, higher reliability and availability, rapid development, deployment and change management, better performance and greater mobility. However it is prominent that, automation improvement, support and management, security and green-IT data centers are the lowest considerable facilities from the survey . “[2]”

5. RELATED WORKS

For advance technology based services in IT industry provides various types of web services either secure or non-secure way. Cloud computing is one of the service model that required adequate security to adapt in business environment. It needs secure web services that is rarely available. Various security measurements are discussed in few papers deeply and recommended some possible way to resolve and mitigate those problems. Introduced some trusted third parties they can assure some security (Data confidentiality, integrity and availability) in cloud environment based on PKI (public key infrastructure), pioneer by D., Zissis and D.,Lekkas in 2010. By Y.,Xiang offers cloud protector which was designed and trained to detect and filter HTTP (Hypertext Transfer Protocol) and XML (Extensible Markup Language) based DoS (Denial of Service) threats, by using CTB (Cloud TraceBack, in 2010. The researchers S., Paquette, P.,T., Jaeger and S.,C., Wilson argue that a well define risk management program in cloud computing is part of the IT administration, in 2010. In cloud technologies Hive and Hadoop with XACML (eXtensible Access Control Markup Language) policy based security mechanisms provide fine-grained data access policies for common and shared storage space in cloud, argue by the scholars B.,Thuraisingham, V., Khadilkar, A., Gupta, M., Kantarcioglu and L., Khan in 2011. To understand the implication of security in cloud computing by the use of IT auditing for data security, privacy, regulation and compliance, which argued by Z., Chen and J., Yoon in 2010. There are many authors pointing out cloud security issues in different prospectus, but the main goal is to provide adequate security for cloud services. It is noted that none of them discuss clearly about a common standard, SLA (Service Level Agreement) policies such that: what does consumer need to know and what does service provider need to provide and some other security measurements and quality of services.

6. SECURITY RISKS IN CLOUD SERVICES

In general cloud computing provides persuasive benefits in IT world as regard of their beneficial characteristics and service models. But it is not completely secure and risk free in terms of data security challenges as like any other communication models or services. Cloud performance is affected as a result of security issues. Therefore, service providers are responsible for good care of security in systems and data. Service managements and governances are enforced some policies and procedures to overcome such issues, for example: virtualization, authentication mechanisms and cryptography techniques, but those technologies and methods have some vulnerabilities in the state of art implementations “[7]”. To analysis and identify appropriate security risks are vital, expect implementation scope for monitoring and auditing in cloud environment. To understand and mitigate security risks and issues are important step forward for securing cloud computing. When data, web applications and services are being hosted in cloud environment by service providers, control of these are no longer in their hand to manage; here also arise some issues about loose of control to secure data and other. Cloud services are shared infrastructure to increase potential vulnerabilities in terms of unauthorized data access, which concern about data privacy, identity management, authentication, compliance, confidentiality, integrity, availability, encryption, internet protocol (IP) vulnerabilities (most of the cases IP is un-trusted which allows man in the middle attack) “[7]”, network security and physical security. Some other matters are also need to distress apart from security such as: SLA (service contract between service provider and consumer) and third party management, performance, virtualization risks, lack of standards and auditing procedures and compliance laws and regulations. There are some major risks related to cloud security shown in ‘Fig 3’. The numbers represent priority according to their occurrences form 1 to 10.

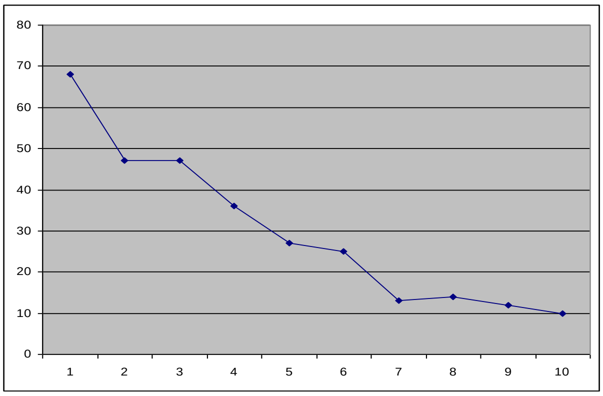
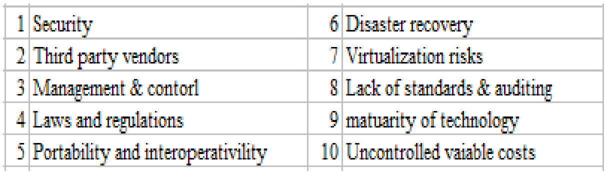


Fig 3: Cloud computing risks

Note:



1	Security	6	Disaster recovery
2	Third party vendors	7	Virtualization risks
3	Management & contorl	8	Lack of standards & auditing
4	Laws and regulations	9	matuarity of technology
5	Portability and interoperativility	10	Uncontrolled vaiable costs

An interview report based on specific security risks area shown that data and information security is the major risk area in cloud computing environment according to 91.7% of the respondents. About 66.7% respondents identified that disaster recovery is the second highest critical risk area in cloud. However, operation management, change management and third party management are being rated somewhat important to mitigate risks according to 58.3%, 50.0% and 50.0%. Cloud computing and virtualization are critical risk area listed in “Table 3” “[2]”.

Table 3. Cloud Computing Risks

Risk Area	Critical	Somewhat Important	Not so Important
Information security	91.70%	08.30%	00.00%
Disaster recovery	66.70%	33.30%	00.00%
Operations management	41.70%	58.30%	00.00%
Change management	41.70%	50.00%	08.30%
Third party management	41.70%	41.70%	16.70%
Regulations and legislation	33.30%	41.70%	25.00%
Interface management	08.30%	50.00%	41.70%

7. SECURITY ISSUES IN CLOUD SERVICES

Cloud computing service models are SaaS, PaaS and IaaS, which provides software as a service, platform as a services and infrastructure as a service to end users or customers. These three service models are built on top of each other, as shown in "Fig. 4"; as a result their capabilities are inherited as well as security issues and risks.

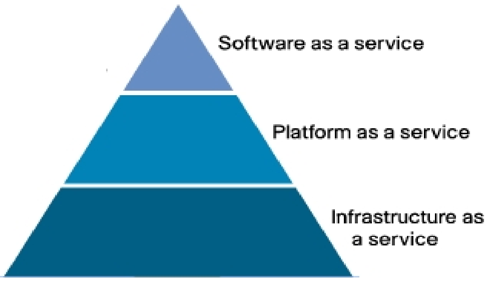


Fig 4: Cloud computing service models

So, service providers are not be able to take care only part of it, rather than as a whole to provide secure environment. In this part of this paper clearly indicate major security issues based on these service models and what needs to be addressed by implementing appropriate countermeasures.

I. **Security issues in SaaS:** In term of SaaS, a consumer needs to depend on the service providers for data security and service providers have to be responsible for providing proper security mechanism to protect data and applications. In this model data is being stored in cloud along with others companies or individuals data. The cloud service providers may replicate data in various places for data availability and efficiency. As a result, there are some security issues arise such as: how is being data stored and where, what types of security is being provided for data manipulation and storage. There are some key security basics need to be considered during SaaS deployment and development. There are:

   - **Data Security:** When enterprise sensitive data are stored in cloud, vendors should provide physical and logical security, secure access policies and some additional security checks due to security vulnerabilities in applications and concern about malicious employees, who can exploit weakness in data security model. Data control over cloud services make difficult to protect and enforce identity theft and cyber crime security. Sharing resources across multiple domains and failures of data backup also arise some data leakage.
   - **Network Security :** In cloud environment data are being transferred over the Internet, thus data flow security is an important issue to avoid leakage of information. To sniff network packets an intruder can make use of data packet to analyze weakness in network security configuration. Attackers can gain access applications and data through hacking such as: some kind of remote access mechanism and injection (SQL and some bad command) vulnerabilities. DoS (Denial of Service), DDoS (Distributed DoS), man in the middle attacks, social networking attacks and some unauthorized attacks creates grate security issues in cloud.
   - **Data Confidentiality:** Privacy and confidentiality issues are take placed when data shares between various users, devices and applications. Here multi-tenancy and multitasking (resource sharing and sharing processing resources: CPU- Central Processing Unit) presents a number of confidentiality threats and risks. Data confidentiality in cloud environment related to user authentication. For overall system security software and data confidentiality is also important to prevent unauthorized use of data.
   - **Data Integrity:** Data integrity ensures that data are being integral and modified by only authorize entity. Due to increasing number of entities and access points in cloud, authorization becomes crucial that only authorized entities are interact with data. If cloud system resources are not properly segregated among clients then some security issues arise for data integrity. Inadequate encryption and week key management scheme can also lead to security breach.
   - **Availability:** Cloud services access on demand by authorized parties even if some authorized entities misbehave or any security breaches. To test availability of the SaaS vendors need to consider authentication process and session management weakness issues. Other issues are also need to consider as well such as: data and information service lock in, bandwidth and connectivity speed over the network in cloud services.
   - **Data Locality:** In the SaaS model, the consumers are unaware that, where there data is being resided. Some cases it is an issue for some companies for data privacy laws in various countries. So, this service model must be capable of proving data security based on location issues.
   - **Access Control:** Many SMB companies store their employees' data in cloud database. The companies have its own policies to access or use data based on their user limitation. So, when an employee left and onboard the SaaS users must bear in mind to enable or disable users account else security breach might be occurred. The SaaS service providers must offer some flexibility to adhere companies' policies in cloud to avoid intrusion of data by unauthorized users.

II. **Security issues in PaaS:** The main purpose of this model is to protect data. In this model, service provider gives possible command of control such as: OS (Operating System) platform, program development tools and storage area, to build application or program on top of service platform by using resources. Even though some controls are given to the clients, but still need to consider and control some security issues below the application levels such as: network and host intrusion. The service providers have to assure against possible use of outage and data remain inaccessible between different applications. Another aspect of security issue needs to consider that load balancing across on platforms. The vulnerabilities in the cloud computing environment are not only related to web related applications but also machine to machine service oriented architecture applications (SOA). It is noted that, SOA applications are progressively more deployed in cloud.

III. **Security issues in IaaS:** Cloud computing combines virtualization technologies are creative way to provide better IT services to consumers. Due to rising virtualization technology poses some security issues for control over the owner of data regardless of physical location. Various security issues are arise to deploy models in IaaS. Private cloud environment creates fewer security risks compared to public cloud. The cloud concept implemented just over the Internet, so whatever security issues and threats are facing in the Internet, for cloud services need to consider as well. Infrastructure is not only appropriate for hardware resources, where data is being reside or processed, but also the way data are being transmitted over the media from source to destination over the open network. There are some possibilities that data can be routed through intruder's network or infrastructure.

"[3][4]"

8. MITIGATION OF SECURITY RISKS

In network, there is no complete security solution to protect data and applications or services, but satisfactory risk management can reduce the level of risks. In this part of the paper, explained some policies, procedures and some tools to mitigate risk of data and applications whether it is in public or private cloud and combination of both (hybrid).

- **Data Security and Control:** Data in cloud environment should be identified and classified according to their types. The service providers should have enough skills to prevent, detect and react according to various security breach. Service logs and service agreement terms inspections are performed regularly. However, there are some validity tests also required for companies to avoid security breach because of malicious data are in cloud such as: cross-sire scripting, insecure configuration, SQL injection flaws and weakness in access control inside companies policies. Service providers should provide transparent services (controls, security and operations) for clients.
- **Network Security:** For a secure system to prevent unauthorized modification and access to data by using adequate set up or configuration of firewall and auditable access rights. Service providers also need to do some tests and validate network security by using some prominence security tools such as: SSL, session management and packet analysis to avoid hijacking active session and access clients' credential data. To secure data traffic, some policies should be implemented in router and layer three switch. Additionally, interaction between mobile users and cloud services providers are also need to be controlled.
- **Data Confidentiality and Integrity:** Proper authentication and authorization mechanism should implement to protect illegal disclose and modification of data. Service development and deployment models must be clear for a developer to protect and restrict use of data. Security parameters are appropriately defined for data segregation and secure cryptographic methods and properties should be implemented in control manner such as: for secure key transfer can be used RAS and for encryption key size should be consider according to their priority of data security or uses.
- **Data and Service Availability:** Internet speed (bandwidth) and connectivity should be considered during data and applications transmission over the network. Network service providers must be able to monitor network load or traffic for proper load balancing and data distribution over network. Data replication and backup policies are also need to be standard and provided auditable proof for data restore procedures, which includes accuracy and completeness over time.
- **Access Control:** Service providers should prove that they have adequate security mechanism to protect unauthorized access. All access or changes in cloud services (resources and data) ought to provide auditable report whether it is success or fail and review along with monitoring to be performed regular basis. To generate trusted user profiles based on their definitions and roles. Identity management and access security mechanism should be implemented and monitored according to their regular schedule.

9. RECOMMENDATION

Cloud computing technologies are implemented various way based on their different service and deployment models. It is constant development process, when the field will be matured there are various aspect of security risk will reduce and certainly will emerge new issues. For proper security service, all issues arising from all direction (vendors and consumers) are need to analyze clearly. However, after reviewing some papers notice that, there are several indispensable key points need to be considered for security in cloud computing environment.

i. Every element in cloud environment should be analyzed at micro and macro level.
ii. An application runs in virtual machine (such as: JVM – Java Virtual Machine) does not it means this application will perform in cloud environment. Therefore, before deployment in cloud environment the application need to be tested with proper test methods and dataset.
iii. Consumers are need to evaluate cloud service providers/vendors as they are proving same types of services based on their service cost, efficiency and security mechanisms and some other issues.
iv. All service providers should provide a standard risks list and protection mechanism and evaluation against it.
v. SLAs (Service Level Agreements) should endow with continuous security review and protection against serious threats.
vi. To secure data and application based on their values, not all data in cloud need to be secured such as: government and organizational data needed to more secure compare to public or individual data. It is note that security always affects the performance of data delivery and efficiency.
vii. DDoS (Distributed denial of service) is a major issue in network; some researchers are need to conduct how to mitigate that risk.
viii. For cloud computing security models there is no global standard or framework for service providers and consumers. To establish a common security tools, mechanism and standard that all vendors and consumers must follow. Additionally, if vendors are want to add supplementary security policies then allow them to impose in their own services.
ix. It is recommended that, all parties require to follow some guidelines and standards for secure cloud environment such as: NIST published a guidelines for security and privacy in public cloud computing by W., Jansen and T., Grance in early 2011 "[10]".

Without any appropriate security model for the cloud environment, potential users will not be able to influence to take advantages of cloud computing technologies completely. In future to work on mutual authentication mechanism and secure data transfer process in cloud services.

10. CONCLUSION

Cloud computing model has the ability to scale up services and virtual resources on demand. To process users conventional cluster system, cloud services provides a lot of advantages. There is no big investment required to update infrastructure, labor and continuing cost. In fact cost is almost zero when resources are not in used (pay per use).

Throughout this paper clearly discussed about security risks and issues in various aspects, such as CIAA (Confidentiality, Integrity, Availability and Authenticity) and issues related to various service delivery models such as: DoS, network security, data security and locality in SaaS models, network and host intrusion in PaaS and IaaS not only considered where data is being stored and process but also concerned the media of data transfer is being used over the Internet. Mitigation of risks and issues are the important part of this paper where described the possible way to reduce risks such as: to implement proper access control, monitoring, auditing and some standard data security mechanism. Finally, provide some recommendations based on literature review on a number of papers in recent years. Thus cloud computing is not mature enough, therefore many academic researches and industries are moving toward to cloud computing environment. Cloud technology is still now in cloud for users.

11. REFERENCES

[1] S. Subashini, V. Kavitha, A survey on security issues in service delivery models of cloud computing, Journal of Network and Computer Applications, vol. 34, Issue 1, pp. 1-11, 2011.

[2] M.Carroll, A.Van der Merwe, P.Kotze, Secure cloud computing: Benefits, risks and controls, Information Security South Africa (ISSA), pp. 1-9, September 2011.

[3] S. Subashini, V. Kavitha, A survey on security issues in service delivery models of cloud computing, Journal of Network and Computer Applications, vol. 34, Issue 1, pp. 1-11, July 2010.

[4] D. Zissis, D. Lekkas, Addressing cloud computing security issues, Future Generation Computer Systems, 2011.

[5] National Institute of Standards and Technology, NIST Cloud Computing Program, 2010 <http://www.nist.gov/itl/cloud/> [Accessed on: 18 October 2011].

[6] Chonka, Y. Xiang, W. Zhou, A. Bonti, Cloud security defence to protect cloud computing against HTTP-DOS and XML-Dos attacks, Journal o Network and Computer Applications, vol. 34, pp. 1097-1107, 2010.

[7] Grobauer, T. Walloschek, E. Stocker, Understanding Cloud Computing Vulnerabilities, Security & Privacy, IEEE, vol. 9, Issue 2, pp. 50-57, March 2011.

[8] B.,Thuraisingham, V., Khadilkar, A., Gupta, M., Kantarcioglu, L., Khan, Secure data storage and retrival in the clod, Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom), 2010 6th International Conference on, pp. 1-8, May 2011.

[9] Z., Chen, J., Yoon, IT Auditing to Assure a Secure Cloud Computing, Services (SERVICES-1), 2010 6th World Congress on, pp. 253-259, September 2010.

[10] J., Wayne, T., Grance, Guidelines on Security and Privacy in Public Cloud Computing, U.S. Department of Commerce, January 2011. http://csrc.nist.gov/publications/drafts/800-144/Draft-SP-800-144_cloud-computing.pdf [Accessed on: 23 October 2011].