A review of security models in cloud computing and an Innovative approach

Dr. Amit Chaturvedi#1, Sajad Ahmad Zarger *2

#1Assistant Prof.MCA Deptt., Govt. Engineering College, Ajmer

*2 M.Phil. Scholar, Ajmer, India

Abstract: *Cloud computing is introducing many huge changes to world of computing and working pattern recently for its multitudinous benefits. However, the security of cloud computing is always the focus of numerous potential cloud customers, and a big barrier for its widespread applications. Actually data security is the main concern. Because of diversity in service models proposed for cloud computing, providing acceptable level of security is main concern. In this paper, we have surveyed several security models and proposed a data security model for cloud computing based on separation of security in different category layers. The proposed model certifies that our method can improve security levels in service oriented systems, especially in cloud computing applications.*

Keywords: *Data security, Cloud computing, cloud service, cloud security, SSL, TSL, security model.*

I. Introduction of cloud computing

Cloud computing can be defined as a model for enabling 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 interaction".

One of the main tenets of Cloud Computing is the `as-a-Service' paradigm in which `some' service is offered by a Service Provider (also known as a Cloud Service Provider) to a User (consumer) for use. This service can also be categorised according to the application domain of its deployment.

Examples of application domains that offer services are: Financial e.g. Mint.com, Managerial e.g. Ever Note and Analytical e.g. Google Analytics. The agreed terms of use, indicating the actions that must be taken by both the provider and consumer, are described in a contract that is agreed upon before service provision. This contract is often described as a Terms of Service or Service Level Agreement. Moreover, as part of this agreement the service provider will provide a Privacy Policy which outlines how the user's data will be stored, managed, used and protected.

Cloud computing provides the world of computing to a broader range of uses and increases the ease of use by giving access through any internet connection. Along with the booming of cloud computing technology, it becomes easier for organizations to access and use personal information in the Cloud. Once data has gone into a public cloud, data security and governance control is transferred in whole or part to the cloud provider. Traditional approach to preserve data privacy and security can be achieved by establishing a control policy and enabling a trust local authority to be responsible for its enforcement. However, it is difficult to have a trust party in the Cloud to ensure the privacy and security policy is actually operated as it is claimed. One of the biggest security concerns is how to maintain data security and privacy while outsourcing data to non-trusted cloud service providers. Yet cloud providers are not assuming full responsibility of security issues in the cloud.

The chief concern in cloud environments is to provide privacy and security around multi-tenancy and isolation, giving customers more comfort besides "trust us" idea of clouds. The sensitive data has to be encrypted before outsourcing to the cloud servers in order to ensure user data privacy. Devising an efficient and secure search scheme over encrypted data involves techniques from multiple domains.[1]

Various threat models have been designed and proposed in order to help clarify and categorize threats. A widely used threat model is Microsoft's STRIDE. STRIDE is used in order to classify threats in the following six categories: Spoofing, Tampering, Repudiation, and Information Disclosure, denial of service and elevation of privilege. The model also suggests some countermeasures in each category, which can be applied to mitigate the threats. Today, STRIDE is considered as a broad threat model and can be used to provide a wider and a more general idea of how threats can be identified.

Despite the many advantages provided by cloud computing are also accompanied by the Introduction of new risks. In addition to the continued presence of all the security issues that may affect its underlying technologies. Organisations have these services at their disposal but cannot disregard their security requirements. The security challenges for cloud computing approach are somewhat dynamic and vast. Data loss and various botnets are the things to breach security of cloud servers. Though, multi-tenancy model needs to be given attention (Kuyoro et al., 2011; Ogigau-Neamtiu, 2012) when talking about the security. Data location is also a critical factor in cloud computing security . One of the prominent flexibilities for cloud computing is Location transparency that is a security issue in the meantime – Remaining unfamiliar with the specific location of data storage, the provision of data protection act for some region certainly be damaged and violated. Thus the personal data of Cloud clients is a matter of concern in a cloud computing environment (Joint, Baker &Eccles, 2009; Ismail, 2011; King & Raja, 2012). Moreover Trust is also a security concerns for the clients to utilize a cloud service (Ryan &Falvy, 2012) because it is directly related to the authenticity and credibility of the cloud service holder.[2] [3]

All kinds of attacks that are applicable to a computer network and the data in transit equally applies to cloud based services – some security issues in such aspect are man-in-the-middle attack, , sniffing, phishing, eavesdropping and other related attacks. DDoS (Distributed Denial of Service) attack is one famous but crucial attack for cloud computing infrastructure (Dou, Chen & Chen, 2013).Other threats to cloud computing include Abuse and Nefarious Use of Cloud Computing ,Insecure Application Programming Interfaces, Shared Technology Vulnerabilities, unknown risk profile.[4]

II. Need of proposed work

One of the most significant barriers to adoption is security because Cloud Computing represents a relatively new computing model, there is a great deal of uncertainty about how security at all levels (e.g., network, host, application, and data levels) can be achieved and how applications security is moved to Cloud Computing. That uncertainty has consistently led information executives to state that security is their number one concern with Cloud Computing. Security concerns relate to risk areas such as external data storage, dependency on the “public” internet, lack of control, multi-tenancy and integration with internal Security. However, new security techniques are needed as well as redesigned traditional solutions that can work with cloud architectures.

One of the characteristics of cloud computing is resources pooling & efficient sharing of resources, which means resources including computing capability, storage and bandwidth are virtualized and shared among various consumers. Therefore, limited data protection in the Cloud will lead to a tough security issue compared to traditional information technology.

Except for private cloud, handing over control to an external CSP is obviously a risk to data security. Cloud consumers, including organizations and individuals, have to rely on the CSPs to implement security features to protect private data in the Cloud.

A major challenge or concern in the cloud computing paradigm is data privacy. On one hand, there is a demand to leverage the powerful resources of the cloud server to provide services to clients. On the other hand, the cloud server must not learn any sensitive information about the data being managed and the queries being answered..

The core issue of protecting data in the Cloud is to outsource data without outsourcing control. According to the guidance from “Safeguarding Privacy in a Connected World: A European Data Protection Framework for the 21st Century” , effort should be put on improving individuals’ ability to control their personal data in the public environment (cloud computing environment).

III. Review of cloud computing security models

A. *Multiple-Tenancy Model*

Multiple-tenancy is a major functional characteristic of cloud computing that permits multiple applications of cloud service organisation currently running on physical server to give cloud services for its clients. Users tenants are separated by virtual partitions, and each partition holds clients tenant's data, , customized settings and configuration settings. By running multiple virtual machines (VMs). In a physical machine, virtualization allows to share computing resource such as, memory, processor I/O and storage to different customers’ applications, and amends the utilization of cloud resources[5].

The impact of multiple-tenancy model is variable for different cloud deployment models. Taking SaaS as an example, Multi-tenant SaaS providers generally do a very great job of anticipating the needs of current and prospective clients and the standardized functionality that is eagerly needed by the company. SaaS with multiple-tenancy functionality is, it is easy to scale-out and scale-up to serve for a bunch of clients based on Web service. Multi-tenancy has brought different approach in Cloud Computing. Even though security experts point out that multi-tenancy is a vulnerability that may expose confidentiality between the tenants. The maintenance of consistency and isolation should be even more secure across multiple tents[6].

A “true” multi-tenant architecture has several key benefits for a SaaS provider:

- Efficiency and Sustainable Scalability: under the approach of “true” multi-tenant architecture, SaaS providers have the capability to make sure that delivery of applications should be at the lowest cost. Essentially no new software resources are required for each incremental user, the cost of on-boarding a new user begins to approach zero at full scale, resulting in ever-increasing marginal revenue associated with each new customer.[7]

z

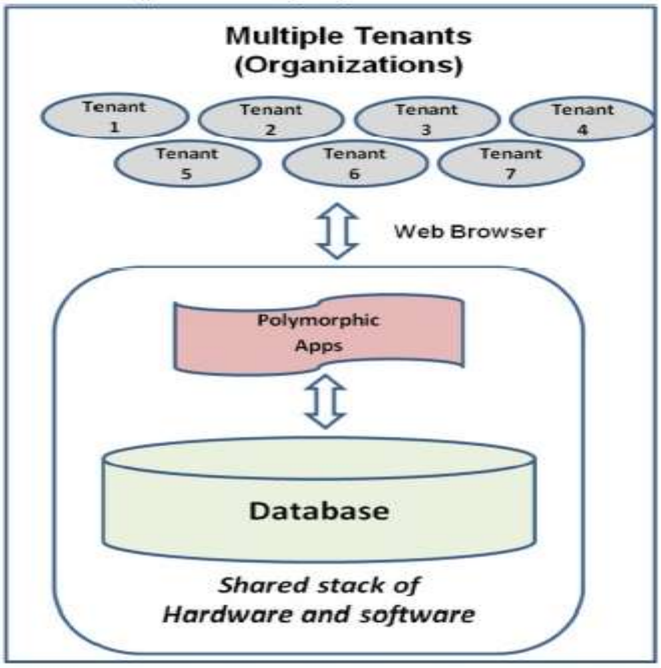


Fig1. multi-tenants model

- Dramatic reduction in operational cost and complexity over the product lifecycle: Since application upgrades can be applied to all tenants by simply upgrading the single instance of the application, the cost savings hence are generally reduced. The obvious conclusion is that "true" multi-tenancy is a requirement for SaaS. SaaS companies, such a Salesfore.com, NetSuite, and Success Factors, all utilize "true" multi-tenancy approach.
- Limitations: In multi-tenant environment, side channel attack is a significant risk, which is based on the information obtained from the bandwidth monitoring [8]. Multi-tenant resource being assigned to the clients whose identities and intentions are not known is another risk. Next security risk is that to reduce cost, providers may store data from multiple tenants in the same database table-spaces or in backup tapes.[9]

B. JericoFormu's Cloud Cube Model

Jericoformu's cloud cube security model is explained in following ways:

Internal/External: This entity defines the physical location of data. Data storage located within the owner's boundary, is internal otherwise it is external. Like the data centre of a private enterprise cloud is internal, and the data centre of Amazon's SC3 is external [10][11].Keep in view in making the statement that internal data is more secure than the external. The effective combination of both the data (internal/external) may lead to a more secure usage model.

Proprietary/Open: cloud's technology, service and interface etc. is determined in this model. This model indicates the portability of the data (interoperability) and application between proprietary system and cloud entities the ability of moving data from one cloud entity to another without any constraint. Proprietary means that a cloud service organisation holds the ownership of facilities giving cloud services since the operation of cloud is proprietary and customers are unable to move their applications from one to another cloud service holder without great effort or investment. The tools used in public cloud are usually *open* and uniform, suggesting that more available service providers and less constraint on data share and incorporation with business partners. Yet unproven premises open clouds can promote accurately the incorporation between multiple organizations.

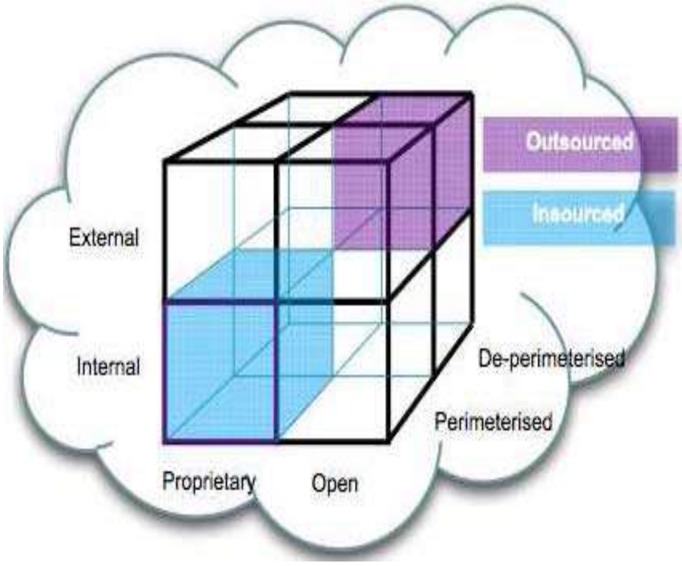


Fig 2 : Cloud cube model

Parameterised / De-parameterised: An entity used to explain "architectural setup" of security protection, i.e. clients application is inside or outside of traditional security boundary? *Parameterised* suggests that a client's application executes within traditional IT security boundary signalled by firewall that blocks the incorporation of various security areas. Though, clients running few applications inside the security area can extend/shrink their application entity to/back from external cloud environment by VPN. *De-parameterised* suggests that the fade away of traditional IT security boundary and the exposure of a customer's application operation. For secure de-parameterised environment, Jerico Forum utilizes the meta-data and mechanisms in their commandments and Collaboration Oriented Architectures Framework (COA) to encapsulate a client's data.

Insourced/Outsourced: an entity that suggests the 4th dimension which has two types in each of the eight cloud forms: *Per(IP,IO,EP,EO) and D-p(IP,IO,EP,EO)*.cloud service that is presented by an organization's own workers is referred as insourced, and on the other hand *Outsourced* means that cloud service is presented by a third party. These two above definitions give output of the question "who do you want to build or manage your cloud service?" This is a policy problem (i.e. a business but not a technical or architectural decision).In cloud cube model, other things such as Offshore and Onshore are usually same to cloud computing, but in this illustrated model we have pointed out the four dimensions mentioned in cloud cube model.[12]

C. *The Mapping Model of Cloud, Security and Compliance*

The mapping model gives a better method to analyse the gaps between cloud architecture and compliance framework and the corresponding security control strategies that should be provided by cloud service organisation, clients or third parties. To secure the cloud environment, we need to identify firstly the security risks tackled by cloud environment, and then point out the gap matrix in accordance with the cloud architecture and its compliance framework, then after we take some related security controls. Here, the compliance framework of cloud computing is not naturally existed with the cloud model correspondingly, the mapping model of cloud, security and compliance proposes whether to accept or refuse the security threat of cloud computing. Keep in view that as a computing paradigm, cloud computing does not influence the satisfaction of compliance. many reviews such as NIST 800-53 revision 3- Recommended Security Controls for Federal Information Systems and Organizations ,and the security architecture documents of Open Security Architecture Group greatly expatiate the general control framework.[13][14].

D. The Cloud Risk Accumulation Model of CSA

Cloud computing uses three service delivery models by which different types of services are delivered to the end customer. The three delivery models are the SaaS, PaaS and IaaS .so cloud service models has various security requirements due to layer dependency. IaaS is the first layer, PaaS is built upon IaaS and SaaS is built upon PaaS, so there is a driven relationship between different layers in cloud computing, hence in service capability too. As Same as that of the inheritance of cloud service capability, the security needs of cloud computing is always inherited between different service layers .[15]

- SaaS gives the least customer extensibility, because client has to depend upon the service provider but the most integrated service and the highest integrated security among three service layers. Actually in SaaS, clients pay for little security effort on the SaaS platform whereas the more security responsibilities are taken in charge by the cloud service provider. A crucial thing about the cloud security system is that customer is in more security capabilities and more management duties which happens usually at the time when the cloud service holder is in the lower service layer. Cloud service holder here should focus for satisfaction of the demands on monitor, compliance , SLA, security, and duty expectation etc in SaaS [16].
- Based on the PaaS platform criteria users have more extensibility than SaaSand PaaS offers the capability of developing customized applications. Although In PaaSthe intrinsic security function and capability are incomplete, yet users has more flexibility for the implementation of additional security.
- In IaaS the consumer is able to deploy and run arbitrary software. IaaS give maximum extensibility for users, meaning that IaaS holds little security functions and capabilities. Users can tackle the security of software applications, operating systems and contents etc in accordance to the IaaS demands.

IV. Proposed Model and Methodology

Here in figure 3 which explains the complexity in security of cloud computing. The main security issues addressed in the below given figure are :

a. Security related to Third Party Resources
b. Application Security
c. Data Transmission Security
d. Data Storage Security

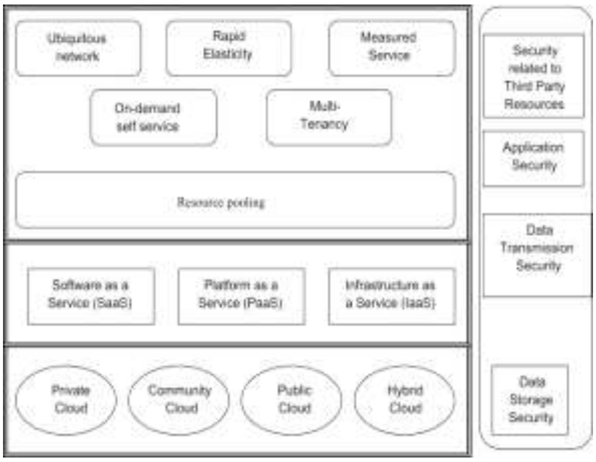


Fig 3: Complexities in Security of cloud computing

We are proposing a model that will address the complexity issues mentioned in figure 3.

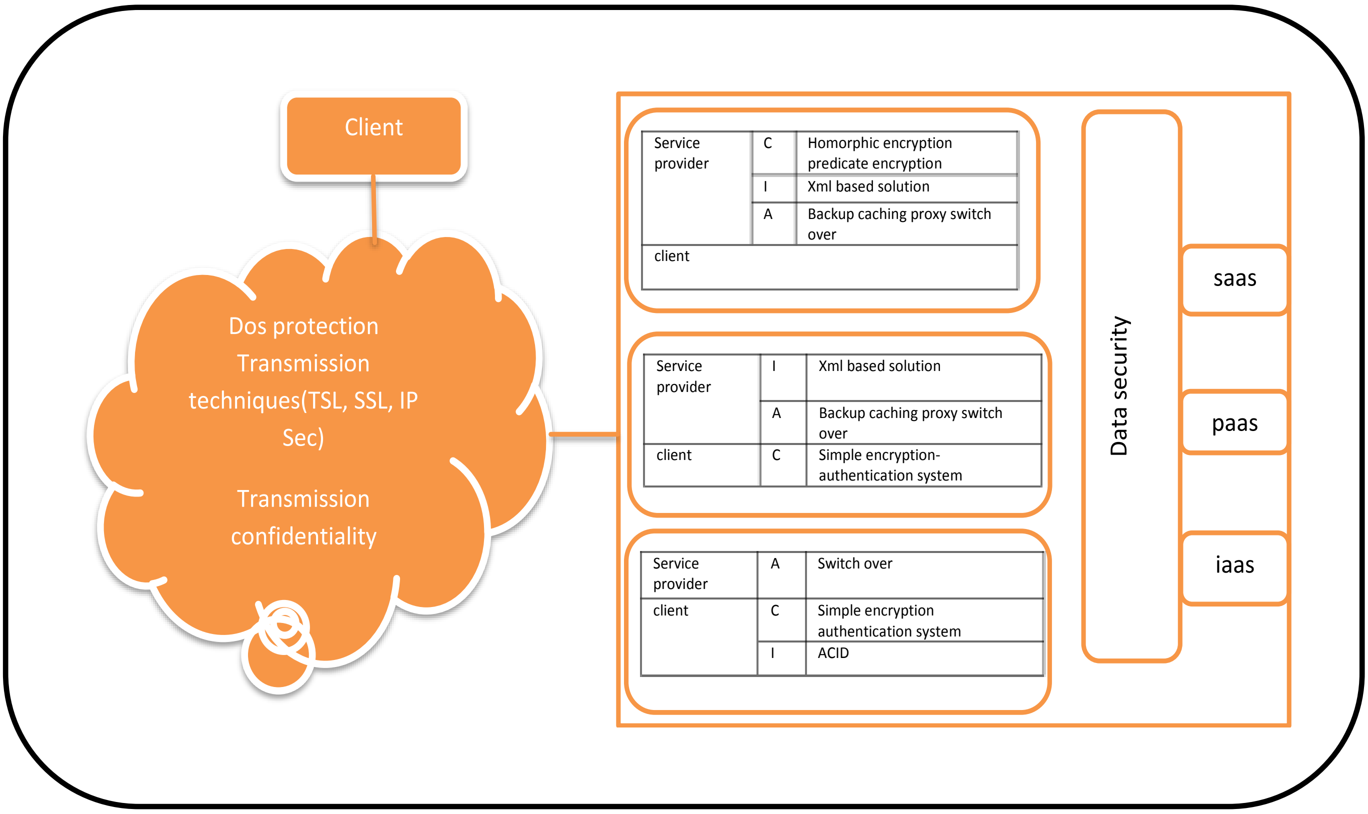
Security related to third party: usually the attacks that are applicable to a computer network and the data in transit equally applies to cloud based services – some security issues in such aspect are man-in-the-middle attack, , sniffing, phishing, eavesdropping and other related attacks.. DDoS

(Distributed Denial of Service) attack is one famous but crucial attack for cloud computing infrastructure

Data security: There are many ways to compromise data. Deletion or alteration of records without a backup of the original content is an obvious example. Unlinking a record from a larger context may render it unrecoverable, as can storage on unreliable media. Loss of an encoding key may result in effective destruction. Finally, unauthorized parties must be prevented from gaining access to sensitive data.The core issue of protecting data in the Cloud is to outsource data without outsourcing control. Application security: the things that get murky is at the protocol layers where exploitation can be no way for the application instance to recognise such an attack.

In proposed model, from the unsecure environment, the techniques that are helpful for protecting data in all levels of cloud environments are explained. Different methods for protecting different kind of cloud service providers are described in Figure 4. The cloud environment is accessed by end users via internet as an entry point and this could be an entry point for secure connection. The cloud is beneficial for the cloud organisation but disadvantageous for the users when there is a Strong log-in to access,. This model must ensure security on clients and as well on the cloud too. From any client with malicious intent that may attempt to gain access to information or shut down a service, cloud needs to be secure. For such an attack, the cloud should provide a denial of service (DoS) protection. The better and secure option is using more bandwidth and better computational power.

After logging in to cloud, it must pay attention to data transmission between users and the cloud provider. Data encryption before sending them by client is a good idea and the better way for sending the data is using the transmission techniques like TSL, SSL and IPsec. In order to make end user and cloud more secure the major concern here is no one should be watching on the conversation between authenticated user and the cloud. These given ways can also guarantee confidentiality. Data security is the main responsibility of the cloud service organisation and each organisation use the special techniques for securing the resources. According to new data security model the three layers are doing specific work on each separate layer to ensure the proper security.


Client
Dos protection
Transmission techniques(TSL, SSL, IP Sec)
Transmission confidentiality
Data security
saas
paas
iaas

Service provider	C	Homorphic encryption predicate encryption
	I	Xml based solution
	A	Backup caching proxy switch over
client		

Service provider	I	Xml based solution
	A	Backup caching proxy switch over
client	C	Simple encryption- authentication system

Service provider	A	Switch over
client	C	Simple encryption authentication system
	I	ACID

Fig 4: a new data security model

V. Conclusion and Future Scope

Cloud Computing is a relatively new concept that presents a good number of benefits for its users; however, it also raises some security problems which may slow down its use. The prevalence of cloud computing is blocked by its security to a great extent. Cloud computing has its special security threats due to virtualization and these threats are completely different from threats in physical systems. In this paper, we have reviewed several security models of cloud computing and proposed a new model for these environments. In this model security issues and their solutions are categorized in three layers of security services to secure accessing to data resources in cloud environment. Although when some of the operational responsibilities are transferred to the provider, the existing variability will depend on some of factors, like the provider service-level agreement (SLA), service delivery model (SPI), and provider-specific capabilities to support the extension of your internal security management processes and tools. In providing data security in cloud environment, the relationship between client and cloud service organisation is displayed in this model and a new solution is proposed for it. As in information security: - confidentiality, integrity, and availability of the details must. Hence, it is a widely used benchmark for evaluation of information systems security; this model may be a good idea. Better security management processes are also aligned with an organization's IT policies, with the aim of protecting the confidentiality, integrity, and availability of information. The proposed model look after towards parameters like (CIA) in all three layers of services that cloud organisation offer to their clients.

Using this method, we can calculate different security measures that can mitigate some types of risks. Also this way, if another security measure costs are less, we can choose it. Parameters that make up the utility functions also need some work to provide better answers. The relationship between client (end users) and cloud service organisation is showed in this model and according to their responsibilities is providing data security in cloud environment, a new solution is proposed for it. In future we will work more on parameters (CIA) in the all three layers of services that cloud organisation provide to its users, in order to make data security more and more secure and efficient.

References

[1] Takabi H, Joshi J B D, Ahn G. Security a nd privacy challenges in cloud computing environments. IEEE Security & Privacy;2010;

[2] Monjur Ahmed1 and Mohammad Ashraf HossainCloud computing and security issues in cloud computing in 2014International Journal of Network Security & Its Applications (IJNSA) 2014

[3] Top threats to cloud computing prepared by security alliance 2010 http://www. cloudsecurityalliance.org/ topthreats

[4] Agarwal, A. and Agarwal, A. . The Security Risks Associated with Cloud Computing, International Journal of Computer Applications in Engineering Sciences,2011

[5] VMware. Inc. Understanding full virtualization, Para virtualization and hardware assist. Technical report, VMware, 2007.www.elsevier.com

[6] Patrick Nicolas, "Multi tenant deployment model for SaaS", White paper , 2006.

[7] Yichuan Zhang, Bin Zhang, Ying Liu, "A Method of SaaS Multi-Tenant Model Recommendation Based on Graph Matching".

[8] S. Subashini n, V.Kavitha A survey on security issues in service delivery models of cloud computing 2010 Journal of Network and Computer Applications

[9] . Jansen W, GranceT Guidelines on Security and privacy in public Cloud Computing. NIST, Special Publication 800–144, Gaithersburg, MD 2011

[10] Varia, J., Mathew, S..Overview of amazon web services. http://aws.amazon.com/ whitepapers; 2013

[11]Agarwal, A. and Agarwal, A. (2011). The Security Risks Associated with Cloud Computing, International Journal of Computer Applications in Engineering Sciences, 1 (Special Issue on CNS),

[12] jerichoforum Cloud cube model v.1 2009 http://www.opengroup.org/jericho/publications.htm, ww.jerichoforum.org

[13] Security guidance for critical areas of focus in cloud computing v2.1 by cloud security alliance 2009

[14] Heiser J. What you need to know about cloud computing security and compliance, Gartner, Research, ID Number:G00168345, 2009.

[15] JianhuaChea*, YaminDuanb, Tao Zhanga, JieFanaStudy on security models and strategies of cloud computing 2011 www.elesevier.com

[16] Wayne J. Brown, Vince Anderson, Qing Tan "Multitenancy - Security Risks and Countermeasures", 2012 15th International Conference on Network-Based Information Systems, IEEE