STUDY ON SECURITY ISSUES AND POSSIBLE SOLUTIONS IN CLOUD COMPUTING

Pranayanath Reddy Anantula[*]

Dr.G Manoj Someswar[**]

Abstract

Security in any type of system is trivial. Security in terms of data, access, management and so on. The Majority of systems now a day's uses a client server model, where any number of client's can access the Server system from anywhere in the world. This leads to monitor/apply some security measures in order to safeguard the system and the data from intruders. With the current trend majority of the organizations are moving to cloud base applications due to the advantages of cloud services such as PAAS, IAAS, and SAAS. Despite its advantages, benefits and ROI of cloud computing some of the organizations are not accepting the cloud due to its security issues & challenges associate with it. Organizations should have a checklist or they should maintain a security model to monitor the service provides services. In order to motivate the organizations, Third party cloud service providers should come up with a good security model as one of the trivial components of the process model. In this paper we discuss the security issues and challenges associated with cloud computing and proposed some possible solutions for some of the issues.

Keywords— Cloud, Security, Security Challenges, Cloud Computing, Cloud Services

[*] Assistant Professor, Alliance University

[**] Principal and Professor of CSE, Anwarul- Uloom College of Engineering and Technology

1. Introduction

Organizations are moving towards cloud computing as delivery solutions due its quick time to market, low-capital cost, low-maintenance, mobility flexibility, scalability increase in availability, decreasing implementation and maintenance cost and different services provided by it. Though it provides such benefits still the concern is about the security and privacy of data. If we look at the Security, It is a two sided coin in the world of cloud computing which has both pros and corns. The security community is also coming together through various limitations arise at education & guidelines creation.

The NIST is relaying the guidelines for agencies that want to use cloud computing and Groups such as Jericho forum are bring security executives together to collaborate & deliver solutions.[1]

As with the emerging technology there exists a leaning curse with regards to security. And also other issues such as data ownership rights, performance, availability of solutions does exist and is being fine-tuned every day.

In any type of application /system the critical element is Data. Data security is the major concern than other issues such as performance, scalability etc. The data need to be securely stored, managed and also analyzed for complex applications to improve the quality & productivity of the organization.

In a current trend most of the organizations are moving towards the cloud due to its benefits as it makes the organization to focus on the project strategies rather than on maintenance of infrastructure.

Cloud is like a tree which provides different services based upon the requirement of the user. The Cloud provides different services such as SAAS, PAAS, and IAAS where the company can use the application without any installations, maintenance at each terminal where the application is used. *Figure 1* describes the cloud Computing System. The user can access the application via the internet from anywhere without any installation of the software's that required to run the application.

Due to the exponential growth in internet service and bandwidth most of the organizations are migrating their applications onto the cloud. Figure 1 shows the cloud computing system.

For example consider Google website which is the best example of cloud computing technology, Google.com provides different services such as maps, drives, apps, email, documents, google+ etc., to all the users without any software installations for every user? To access any of its services users need to have an account with Google. Whenever Google comes up with a new service the users can easily use them by accepting some service agreements before using it.

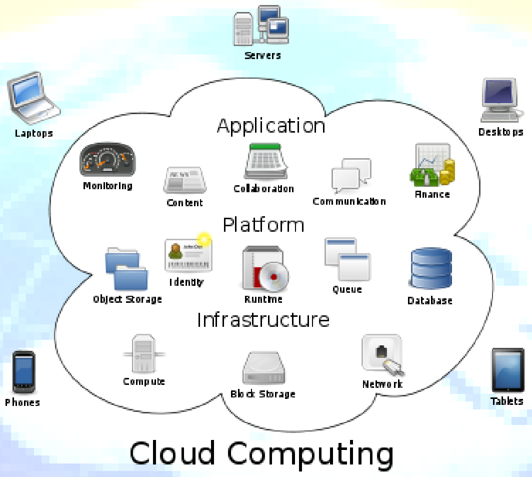


Figure 1: Cloud Computing System

The beauty of cloud computing is that some service provider will host your application and you can access it through their sites. The service provider will provide all the services such as PAAS, SAAS, and IAAS.

Any user who wants to deploy the application in the cloud will have to hand over the application and data.

The service providers will handle the servers, mange software updates, manage data backups etc. and all these depends on how you have crafted your contract. *Figure 2* shows the architecture of the cloud computing.

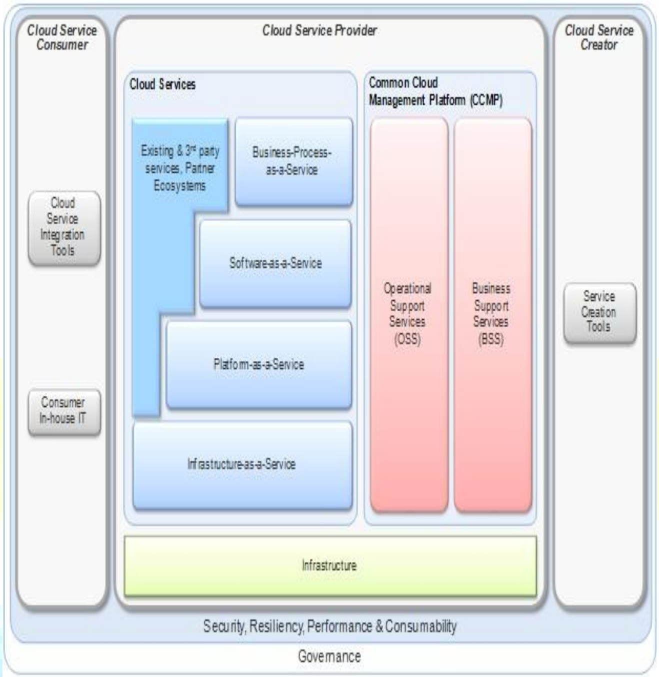

Cloud Service Consumer
Cloud Service Provider
Cloud Service Creator
Cloud Services
Common Cloud Management Platform (CCMP)
Existing & 3rd party services, Partner Ecosystems
Business-Process-as-a-Service
Software-as-a-Service
Platform-as-a-Service
Infrastructure-as-a-Service
Operational Support Services (OSS)
Business Support Services (BSS)
Cloud Service Integration Tools
Consumer In-house IT
Service Creation Tools
Infrastructure
Security, Resiliency, Performance & Consumability
Governance

Figure 2: Cloud Computing Architecture

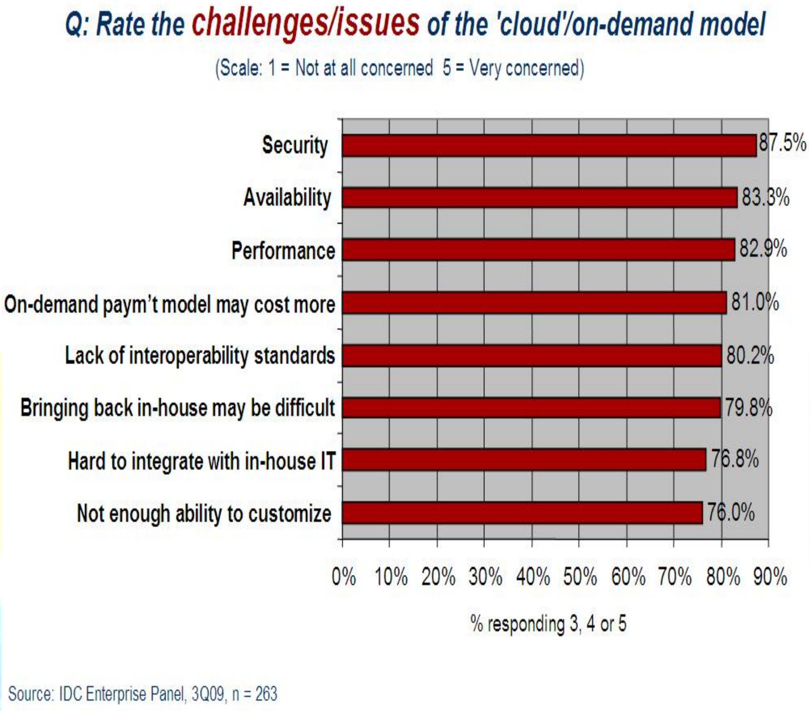
This may lead to some of the issues such as disclosing sensitive or proprietary information, weak links, security, application integrity, location etc.

In cloud computing the application is accessed through the internet, which can access from a web browser in desktops or mobiles, as the software and data are residing on the server at some remote locations. Because of the critical /sensitive nature of applications it is important that the cloud need to be secure.

The concern is the user doesn't have any control over the sensitive data as the data is distributed over the wide area where greater no of devices are being shared by unrelated users. User access to security audit logs may be impossible or difficult.

The major security challenge with cloud is that the access of the data may not have control of where the data is placed.

Security issues in cloud computing have played a major role in slowing down its acceptance. In fact security was ranked as the most challenging issues of cloud computing in the IDC survey which was conducted by 244 IT executives on cloud services. [2] *Figure 3* show the survey results.


Q: Rate the challenges/issues of the 'cloud'/on-demand model

(Scale: 1 = Not at all concerned 5 = Very concerned)

Source: IDC Enterprise Panel, 3Q09, n = 263

Figure 3: IDC Survey on Cloud Computing Systems

If the provider has not done a good security model of their own environment. The consumer could be in massive trouble. In reality, even if providers are doing their best to secure data, it can still be hacked or misused. The better plan of action is not to do move sensitive application or data into the cloud without executing security control management by the customer organization.

The hacker can sell your proprietary information to your competitors or misuse the data or delete entire data. This may happen because your data is held on someone else equipment. The security control management must have proper planning and execution of cloud providers in terms of monitoring logs, and have secure environment. If we look at the SME's approach to cloud Computing as shown in *Figure 4* [3] we can observe that Privacy, Integrity, Availability of service and Loss of Control of data are the major known concerns for any project.

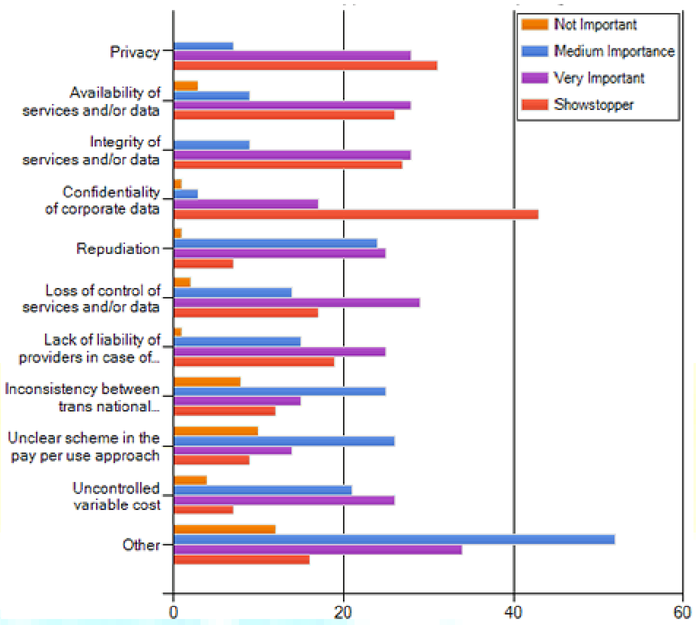


Figure 4: Main Concerns in SME's Approach to Cloud Computing

The organization of the paper is as follows, First we go through the overview of related work done on security issues then the types of cloud and its issues & challenges, cloud computing challenges with respect to the customer and possible solutions and conclusion.

2. Related Work

Several studies have been carried out relating to security issues in cloud computing, Gartner 2008 identified seven security issues that need to be addressed before enterprises consider switching to the cloud computing model. They are as follows: (1) privileged user access (2) Regulatory compliance (3) data location (4) data segregation (5) Recovery (6) investigative support (7) Long-term viability. [4]

The Cloud Computing Use Case Discussion Group discusses the different Use Case scenarios and related requirements that may exist in the cloud model. They consider use cases from different perspectives including customers, developers and security engineers. [5]

ENISA investigated the different security risks related to adopting cloud computing along with the affected assets, the risk likelihood, impacts, and vulnerabilities in the cloud computing may lead to such risks.[6]

Balachandra et al, 2009 discussed the security SLA's specification and objectives related to data locations, segregation and data recovery. [7]

Kresimir et al, 2010 discussed high level security concerns in the cloud computing model such as data integrity, payment and privacy of sensitive information. [8]

Bernd et al, 2010 discuss the security vulnerabilities existing in the cloud platform. The authors grouped the possible vulnerabilities into technology-related, cloud characteristics-related, security controls related. [9]

Subashini et al, discusses the security challenges of the cloud service delivery model, focusing on the SaaS model.[10]

This paper is a proposal to the different security issues & challenges associated with cloud computing systems. The paper focuses on security issues and challenges on different types of clouds and the services provided by them.

In any cloud the general Security issues are networked, database, operating system, Virtualization, scheduling resources, transaction management, load balancing, concurrency control, and memory management.

The Network has to be secured, virtually mapping machine to physical machine has to be carried out securely, data security involves encrypting and ensuring appropriate policies are enforced while sharing.

Data mining techniques may be applicable to malware detection in clouds; this is extending the technologies to the concept of secure cloud, another way of securing the cloud is through layer framework i.e., securing Virtual machine, cloud storage, data layer, virtual network monitoring and policy layers and risk analysis layers. *Figure 5* shows layer framework for cloud systems.

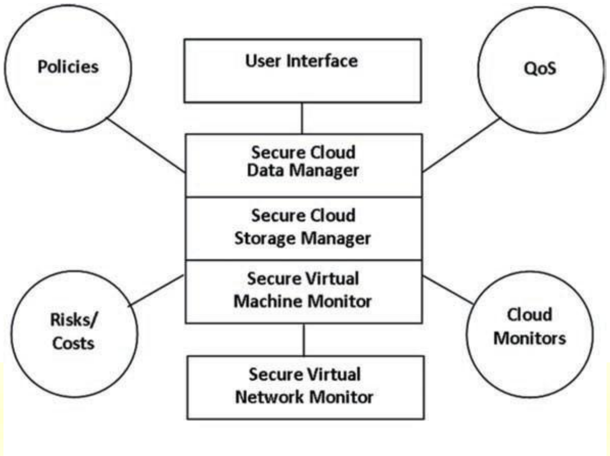

Policies
User Interface
QoS
Secure Cloud Data Manager
Secure Cloud Storage Manager
Secure Virtual Machine Monitor
Risks/ Costs
Cloud Monitors
Secure Virtual Network Monitor

Figure 5: Layer Framework for Cloud Systems

3. Types of Cloud and its Issues & Challenges

Cloud computing has 4 types of models

1) Private 2) Public 3) Hybrid 4) Community

Public cloud: It is a traditional framework where resources are dynamically provided. A Third party provider will share resources and bill on units bases. It is same as pay-per use model. Public clouds are maintained by different providers, the computing infrastructure may be hosted at a remote location that may be in shared between multiple organizations. Even though they apply good security model but still it has some security issues because the user doesn't have control on the allocation of resources that directly affect the data access. So the user needs to do additional work to ensure data and applications are not malicious attack.

Private cloud: In private cloud infrastructure is dedicated and not shared with other organizations. Using the private cloud the user has the control over the data. As the user will have a private network it is similar to the setup within the organization internal data center. In private cloud you can scale & pool the services for cloud users to share & use. Utilization of private cloud is more secure that of public as only organization & designated stakeholders may have access to operate any specific private cloud. They have all the rights to select the resources and locations. Private clouds are of two types: *On-premise* and *externally hosted*. On- Premises is managed by the organization and externally hosted are hosted by third party service providers and they are exclusively use by one organization.

Hybrid: Mixture of one or more external cloud services, which has centrally manger & provides as a single unit & through a secure network. It provides Virtualization from both public and private clouds.

Community cloud: involves sharing of computing infrastructure among organizations of the same community by binding to some policy issues.

Table 1 List out the major security concerns in each cloud system. These issues may be the subset of each other system.

Table 1: Security issues in Cloud Computing Systems

Private Cloud
➢ Identity & Access Management ➢ Data Protection ➢ Security Intelligence ➢ Software, Platform And Infrastructure Security
Public Cloud
➢ Denial of Service (DOS) Attacks ➢ Attack on Virtual Machine ➢ Placing malicious code ➢ Attack on physical machine
Hybrid Cloud
➢ Risk of Multiple Cloud Tenants. ➢ Ongoing Compliance Concerns ➢ Access Control and Identity Management. ➢ Access Control and Identity Management. ➢ Data Slinging
Community Cloud
➢ Compliance And Auditing ➢ Intrusion Detection (IDS) and Firewall Features. ➢ Access Control ➢ Anti Virus/Anti Malware Protection.

Clouds are classified based upon service provided in the following ways.

1. Infrastructure as a service (IaaS)

It involves service offering related to hardware and usage principles of cloud computing. It deals with hardware required for the system to execute. Such as processing speed, storage area for processing or storing the database. Leading vendors that provide Infrastructure as a service are Amazon EC2, Amazon S3, Rackspace Cloud Servers and Flexi scale.

2. Platform as a Service (PaaS)

It involves offering a development environment in the cloud. It provides the platform for the developers to develop the systems and deploy the application on the cloud. The entire development platform is provided on the internet. So there is no need of setting up the development or test platform in individual systems. Platforms provided by different vendors are typically not compatible. Typical players in PAAS are Google Application Engine, Microsoft's Azure, and Salesforce.com.

3. Software as a service (SaaS)

It includes a complete set of software's offering on the cloud. Users can access software hosted by the cloud vendor on pay-per-use basis. Most of the vendors are well-established in this sector. The pioneer in this field has been Salesforce.com. Sales force is offering the online Customer Relationship Management (CRM) space. Other examples are online email providers like Google's Gmail and Microsoft's Hotmail, Google docs and Microsoft's online version of office called BPOS (Business Productivity Online Standard Suite). *Figure 6* shows the Security concerns of Cloud Computing System.

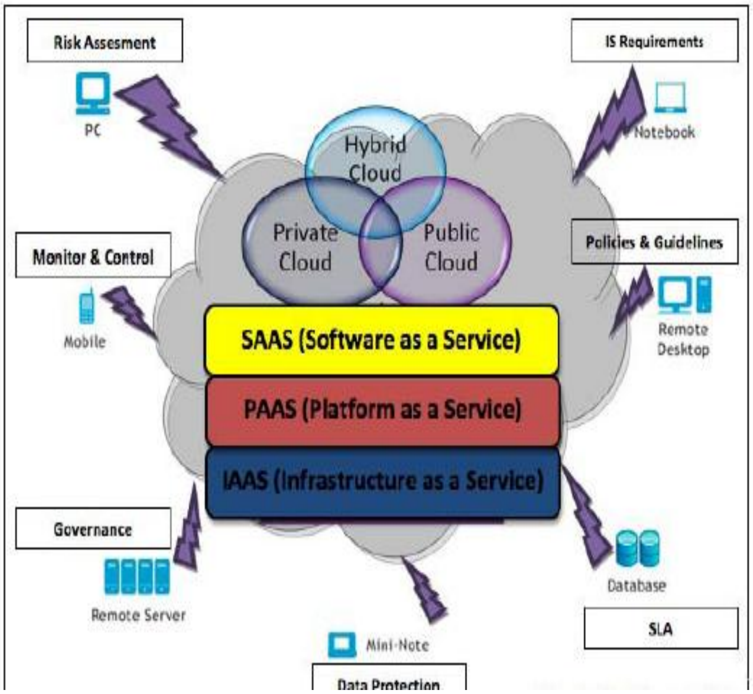


Figure 6: Security Concerns of Cloud Computing System

Some of the security concerns related to the Cloud services are

IAAS

- VM Level Attack
- Isolation Failure
- High Availability
- Disaster Recovery
- Load Balancing
- Multi Tenancy
- Quality Of Service (QOS)
- Virtual Network
- Virtual Storage
- Virtual Computation

PAAS

- Vendor Locking
- Lack Of Security Tools

- Privilege User Attack
- Cloud Provider Long Term Violability
- Database, Web, Workflow, Analytics, Reporting, Contact , Service Business Etc

SAAS

- Malicious Attack
- Insecure Interfaces And APIS
- Data Loss And Leakages
- Account Or Services Hijacking
- Management Interface Compromises

David Linthicum describes a more granular classification on the basis of service provided. These are listed below: [11]

1. Storage-as-a-service
2. Database-as-a-service
3. Information-as-a-service
4. Process-as-a-service
5. Application-as-a-service
6. Platform-as-a-service
7. Integration-as-a-service
8. Security-as-a-service
9. Management/Governance-as-a-service
10. Testing-as-a-service
11. Infrastructure-as-a-service

4. Challenges and Possible Solutions

For any cloud computing system following are the major concerns with repsect to customer. *Figure 7* shows the Security measures to be taken at different level of system architecture.

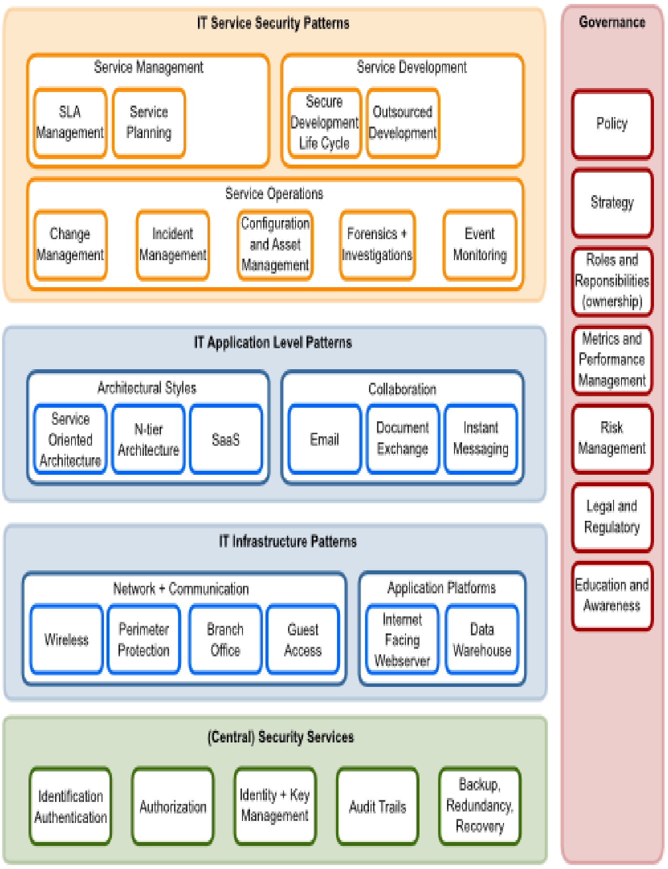


Figure 7: Secuirty Measures at Different Levels of System Architecture

The security measures are broadly classified as

- Governance
- IT Security services (central)
- IT Service security patterns

Governance:

Every system must bind with some set of rules and regulations in order to access the system either in the cloud or on-premises of the Organization. In order to access the system we have to Create System policies, role and responsibilities to access the system effectively and also if anything goes wrong or any malfunction happens proper strategies need to be followed. For any system we need to have a Risk Management and strategies to overcome the risks whenever they come across. When dealing with cloud service providers we need to have proper legal agreement regarding the access of the system. As we know that Cloud is multi tenancy architecture multiple Organization data may be present on the same infrastructure. We should make proper policies and agreements before moving the system on to the cloud.

IT Security services (Central):

Service Providers must have proper Backup, Redundancy, Recovery, Authentication, Identity Management, and Audit Trails. The main concern is data and availability of data at any time and location. No intruder should be allowed to access the data without proper authentication. Data availability is should be done by making the redundant copy of the data at different locations. Here the user must have a proper legal agreement with the service providers because of different geographical location policies. Audit Trials must be done every month to check the system status.

IT Service security patterns

Service management:

Service level agreement (SLA) and service planning are the key functionalities. An organization must have an SLA’s for services begin rented from the service providers and the alliance must be accepted by both the parties.

Service development:

An organization that develops the system using cloud services (PAAS, SAAS) must have a strong security development model and outsource development management. The developer may be in house or outsource to some other organization. All developers are having the access to development and testing the system via cloud. To maintain the integrity of the system cloud service provider must have a support to provide the logs of each and every user activity for audit and to investigate if anything wrong happens to the system.

Service operations:

Different operations performed by using the services are change management, incident management, configuration and asset management, Forensic and Investigation and Monitoring. Service operation helps in development and service management Organizations must come up with the checklist for each and every service and operations. The checklist should contain all the required information for every individual operation, So that by looking at the checklists we can get an overview of the status of the entire system i.e., whether the system is completely under compliance with the Service security and Governance or not.

5. Conclusion

Cloud is a Multi Tenancy architecture approach where the storage space is shared by multiple organizations. The services and sharing of resources are taken care by cloud providers. Measuring the quality of cloud providers approach towards security is difficult task because cloud providers will not expose their infrastructure to customers. Selecting the type of Cloud and cloud services must be done by analyzing the pros and cons of the cloud and their security issues and challenges need to be handled when migrating/moving the application into the cloud. Before moving the application into the cloud we need to apply different security measures at different levels of system architecture to safeguard the application and data from intruders.

References

[1] Jericho Forum and Cloud Security Alliance Join Forces To Address Cloud Computing Security: *https://cloudsecurityalliance.org*

[2] F. Gens. (2009, Feb.). "New IDC IT Cloud Services Survey: Top Benefits and Challenges", IDC eXchange, Available: <http://blogs.idc.com/ie/?p=730> [Feb. 18, 2010].

[3] Website: http://www.surveymonkey.com/s.aspx?sm=CZdVubBa9LIzYlR3KNeZIQ_3d_3d

[4] J. Brodkin. (2008, Jun.). "Gartner: Seven cloud-computing security risks." InfoWorld, [Mar. 13, 2009].

[5] Cloud Computing Use Case Discussion Group. "Cloud Computing Use Cases Version 3.0," 2010.

[6] ENISA. (2009, Feb) "Cloud computing: benefits, risks and recommendations for information security." Available: http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computingrisk-assessment [Jul. 10, 2010].

[7] R. K. Balachandra, P. V. Ramakrishna and A. Rakshit. “Cloud Security Issues.” In PROC ‘09 IEEE International Conference on Services Computing, 2009, pp 517-520.

[8] P. Kresimir and H. Zeljko "Cloud computing security issues and challenges." In PROC Third International Conference on Advances in Human-oriented and Personalized Mechanisms, Technologies, and Services, 2010, pp. 344-349.

[9] B. Grobauer, T. Walloschek and E. Stöcker, "Understanding Cloud Computing Vulnerabilities," IEEE Security and Privacy, vol. 99, 2010.

[10] 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.

[11] David S. Linthicum, “Cloud Computing and SOA Convergence in Your Enterprise: A Step-by-Step Guide” Pearson Edition -2010

[12] S. Ramgovind, M. M. Eloff, E. Smith. “The Management of Security in Cloud Computing” In PROC 2010 IEEE International Conference on Cloud Computing 2010.

[13] M. A. Morsy, J. Grundy and Müller I. “An Analysis of the Cloud Computing Security Problem” In PROC APSEC 2010 Cloud Workshop. 2010.

[14] Cloud Security Alliance (CSA). Available: http://www.cloudsecurityalliance.org [Mar.19, 2010]

[15] S. Arnold (2009, Jul.). “Cloud computing and the issue of privacy.” KM World, pp14-22. Available: www.kmworld.com [Aug. 19, 2009].

[16] C. Weinhardt, A. Anandasivam, B. Blau, and J. Stosser. “Business Models in the Service World.” IT Professional, vol. 11, pp. 28-33, 2009.

[17] N. Gruschka, L. L. Iancono, M. Jensen and J. Schwenk. “On Technical Security Issues in

[18] Cloud Computing” In PROC 09 IEEE International Conference on Cloud Computing, 2009pp 110-112.

[19] N. Leavitt. “Is Cloud Computing Really Ready for Prime Time?” Computer, vol. 42, pp. 15-20, 2009.

[20] M. Jensen, J. Schwenk, N. Gruschka and L. L. Iacono, "On Technical Security Issues in Cloud Computing." in PROC IEEE ICCC, Bangalore 2009, pp. 109-116.