A Study on Cloud Computing Security Issues & Challenges

Thanjida Akhter
Department of Computer Science
Memorial University of Newfoundland
takhter@mun.ca
201691489

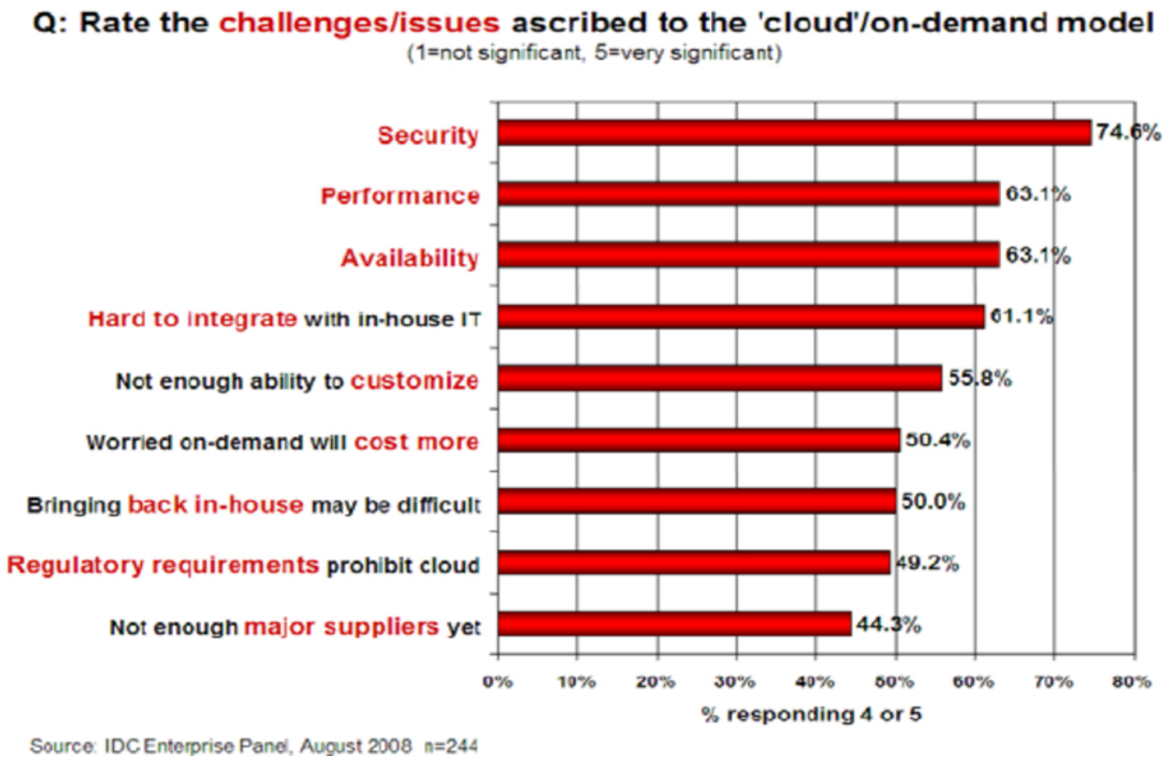
ABSTRACT

Cloud computing is a set of IT services that are provided to a customer over a network on a leased basis and with the ability to scale up or down their service requirements. Usually cloud computing services are delivered by a third party provider who owns the infrastructure. Cloud computing offers an innovative business model for organizations to adopt IT services without upfront investment. Despite the potential gains achieved from the cloud computing, the organizations are slow in accepting it due to security issues and challenges associated with it. Security is one of the major issues which hamper the growth of cloud. The idea of handing over important data to another company is worrisome; such that the consumers need to be vigilant in understanding the risks of data breaches in this new environment. This paper introduces a detailed analysis of the cloud computing security issues and challenges focusing on the cloud computing types and the service delivery types.

1.0 INTRODUCTION

Cloud Computing has become more popular after Web 2.0. Some technologies such as utility computing cluster computing, distributed systems and grid computing paradigm has intricate connection with Cloud Computing. Security issues present a strong barrier for users to adapt into Cloud Computing systems. Several surveys of potential cloud adopters indicate that security is the primary concern hindering its adoption. For years the Internet has been represented on network diagrams by a cloud symbol until 2008 when a variety of new services started to emerge that permitted computing resources to be accessed over the Internet termed cloud computing. Cloud computing encompasses activities such as the use of social networking sites and other forms of interpersonal computing; however, most of the time cloud computing is concerned with accessing online software applications, data storage and processing power. Cloud computing is a way to increase the capacity or add capabilities dynamically without investing in new infrastructure, training new personnel, or licensing new software. It extends Information Technology's (IT) existing capabilities. In the last few years, cloud computing has grown from being a promising business concept to one of the fast growing segments of the IT industry. But as more and more information on individuals and companies are placed in the cloud, concerns are beginning to grow about just how safe an environment it is.

Despite of all the hype surrounding the cloud, customers are still reluctant to deploy their business in the cloud. Security issues in cloud computing has played a major role in slowing down its acceptance, in fact security ranked first as the greatest challenge issue of cloud computing as depicted in figure 1.



Source: IDC Enterprise Panel, August 2008 n=244

Figure 1: Results of IDC survey ranking security challenges, 2008 [1]

On the other hand concerns persist about loss of control over certain sensitive data, and the lack of security for stored kernels entrusted to cloud providers. If those providers have not done good jobs securing their own environments, the consumers could be in trouble. Measuring the quality of cloud providers' approach to security is difficult because many cloud providers will not expose their infrastructure to customers. This work is a study more specific to the different security issues and the challenges that has emanated in the cloud computing system. The following section review of literature on security issues and challenges in cloud computing and the remaining sections are organized as follows. In section 2.0 try to define cloud computing. Section 3.0 discusses about Cloud computing architecture both service model and cloud computing deployment methods. Section 4.0 talks about mail topic security issues in cloud computing highlight on Cloud computing architecture deliberates on associated cloud computing challenges on section 5.0; and Section 6.0 presents the conclusion.

2.0 CLOUD COMPUTING DEFINITION AND FEATURES

2.1 Definition

A number of computing researchers and practitioners have attempted to define Clouds in various ways. Here are some definitions: NIST [10] definition of cloud computing: " Cloud computing is 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”. Buyya [5] defined Cloud as follows:

“A Cloud is a type of parallel and distributed system consisting of a collection of inter-connected and virtualized computers that are dynamically provisioned and presented as one or more unified computing resource(s) based on service-level agreements established through negotiation between the service provider and consumers."

To understand the importance of cloud computing and its adoption, one must have to understand its principal characteristics, its delivery and deployment models.

2.2 Characteristics

The five key characteristics of cloud computing defined by NIST includes [10]:

2.2.1 On-demand self-service

A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed without requiring human interaction with each service’s provider.

2.2.2 Ubiquitous network access

Accessed through standard mechanisms on heterogeneous thin and thick clients. Both high bandwidth and low latency are expected.

2.2.3 Location-independent resource pooling

The provider’s computing resources are pooled to serve all consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand.

2.2.4 Rapid elasticity

Let’s us quickly scale up (or down) resources.

2.2.5 **Measured service**

Are primarily derived from business model properties and indicate that cloud service providers control and optimize the use of computing resources through automated resource allocation, load balancing, and metering tools.

3.0 CLOUD COMPUTING ARCHITECTURE

3.1 Cloud Computing Service Models

The three main cloud service delivery models are: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS).

3.1.1 Software as a Service (SaaS)

If provide software services on demand. The use of single instance of the application runs on the cloud services and multiple end users or client organizations. The most widely known example of SaaS is salesforce.com, though many other examples have come to market, including the Google Apps offering of basic business services including email and word processing. Although salesforce.com preceded the definition of cloud computing by a few years, it now operates by leveraging its companion force.com, which can be defined as a platform as a service.

3.1.2 Platform as a service (PaaS)

Platform as a service encapsulates a layer of software and provides it as a service that can beused to build higher level services. There are at least two perspectives on PaaS depending on theperspective of the producer or consumer of the services:

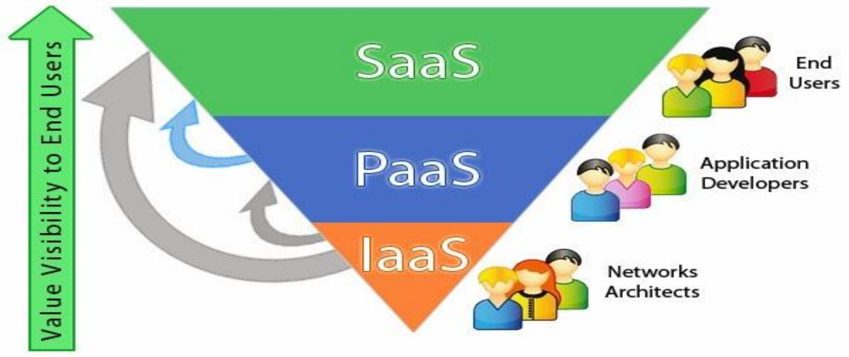


Figure 2: Cloud Services model also called Cloud Service Stack

3.1.2.1 Someone producing PaaS might produce a platform by integrating an OS, middleware, application software, and even a development environment that is then provided to a customer as a service

3.1.2.2 Someone using PaaS would see an encapsulated service that is presented to them through an API. The customer interacts with the platform through the API, and the platform does what is necessary to manage and scale itself to provide a given level of service.

Commercial examples of PaaS include the Google Apps Engine, which serves applications on Google’s infrastructure. PaaS services such as these can provide a powerful basis on which to deploy applications, however they may be constrained by the capabilities that the cloud provider chooses to deliver.

3.1.3 Infrastructure as a service (IaaS)

Infrastructure as a service delivers basic storage and compute capabilities as standardized services over the network. Servers, storage systems, switches, routers, and other systems are pooled and made available to handle workloads that range from application components to high-performance computing applications. Commercial examples of IaaS include Joying, whose main product is a line of virtualized servers that provide a highly available on demand infrastructure.

3.2 Cloud Deployments Models

In the cloud deployment model, networking, platform, storage, and software infrastructure are provided as services that scale up or down depending on the demand as. The Cloud Computing model has there are four main deployment models which are

3.2.1 Private cloud

Private cloud is a new term that some vendors have recently used to describe offerings that emulate cloud computing on private networks. It is set up within an organization's internal enterprise datacenter. In the private cloud, scalable resources and virtual applications provided by the cloud vendor are pooled together and available for cloud users to share and use. It differs from the public cloud in that all the cloud resources and applications are managed by the organization itself, similar to Intranet functionality. Utilization on the private cloud can be much more secure than that of the public cloud because of its specified internal exposure. Only the organization and designated stakeholders may have access to operate on a specific Private cloud.[2]

3.2.2 Public cloud

Public cloud describes cloud computing in the traditional mainstream sense, whereby resources are dynamically provisioned on a fine-grained, self-service basis over the Internet, via web applications/web services, from an off-site third-party provider who shares resources and bills on a fine-grained utility computing basis. It is typically based on a pay-per-use model, similar to a prepaid electricity metering system which is flexible enough to cater for spikes in demand for cloud optimization.[3] Public clouds are less secure than the other cloud models because it places an additional burden of ensuring all applications and data accessed on the public cloud are not subjected to malicious attacks.

3.2.3 Hybrid cloud

Hybrid cloud is a private cloud linked to one or more external cloud services, centrally managed, provisioned as a single unit, and circumscribed by a secure network [4]. It provides virtual IT solutions through a mix of both public and private clouds. Hybrid Cloud provides more secure control of the data and applications and allows various parties to access information over the Internet. It also has an open architecture that allows interfaces with other management systems. Hybrid cloud can describe configuration combining a local device, such as a Plug computer with cloud services. It can also describe configurations combining virtual and physical, collocated
Assets -for example, a mostly virtualized environment that requires physical servers, routers, or other hardware such as a network appliance acting as a firewall or spam filter.

4.0 SECURITY ISSUES

In SaaS, providers are more responsible for security. The clients have to depend on providers for security measures. As public cloud is less secure than private clouds, the stronger security measures are required in public cloud. Also in SaaS, it becomes difficult for the user to ensure that proper security is maintained or not. Private clouds could also demand more extensibility to accommodate customized requirements.

The following key security elements [7] should be carefully considered as an integral part of the SaaS application development and deployment process:

1. Privileged access
2. Data location
3. Data segregation
4. Data availability
5. Regulatory compliance
6. Recovery
7. Investigative Support
8. Long-term viability

In PaaS, customers are able to build their own applications on top of the platforms provided. Thus it is the responsibility of the customers to protect their applications as providers are only responsible for isolating the customers' applications and workspaces from one another [5]. So, maintaining the integrity of applications and enforcing the authentication checks are the fundamental security requirements in PaaS.

The world's leading information technology research and advisory company, has identified seven security concerns that an enterprise cloud computing user should address with cloud computing providers (Edwards, 2009) before adopting. IaaS is mainly used as a delivery model. The major security concern in IaaS is to maintain the control over the customer's data that is stored in provider's hardware. The consumers are responsible for securing the operating systems, applications, and content. The cloud provider must provide low-level data protection capabilities [5].

Based upon the deployment model, public clouds are less secure than the other cloud models as it allows users to access the data across wide area network. In public cloud, additional security measurements like trust are required to ensure all applications and data accessed on the public cloud are not subjected to malicious attacks [8]. Utilization on the private cloud can be much more secure than that of the public cloud because of it is specified for some particular organization. A hybrid cloud is a private cloud linked to one or more public clouds. Hybrid clouds provide more secure control of the data and applications as each and everything is centrally managed [8]. Each of the security requirements will be highlighted below in context of cloud computing:

4.1 User/Privileged Access

Ask providers for specific information on the hiring and oversight of privileged administrators and the controls over their access to information. Major Companies should demand and enforce their own hiring criteria for personnel that will Operate their cloud computing environments.

4.2 Regulatory Compliance

Make sure your provider is willing to submit to external Audits and security certifications.

4.3 Data location

Enterprises should require that the cloud computing provider store and process data in specific jurisdictions and should obey the privacy rules of those Jurisdictions

4.4 Data Segregation

Find out what is done to segregate your data, and ask for proof that encryption schemes are deployed and are effective.

4.5 Disaster Recovery Verification

Know what will happen if disaster strikes by asking whether your provider will be able to completely restore your data and service, and find out how long it will take.

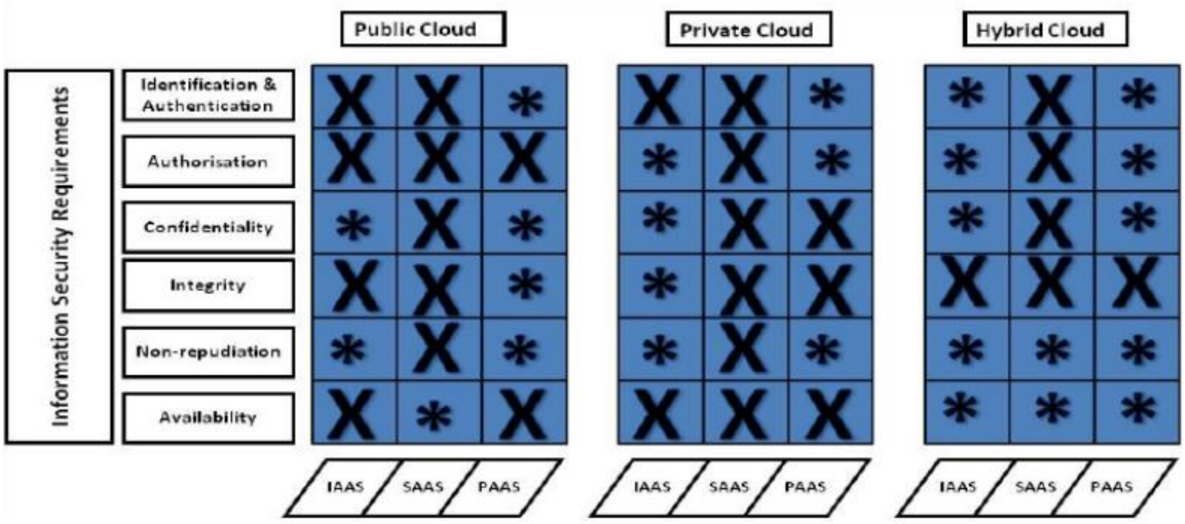
4.6 Disaster Recovery

Ask the provider for a contractual commitment to support specific types of investigations, such as the research involved in the discovery phase of a lawsuit, and verify that the provider has successfully supported such activities in the past. Without evidence, don't assume that it can do so.

4.7 Long-term Viability

Ask prospective providers how you would get your data back if they were to fail or be acquired, and find out if the data would be in a format that you could easily import into a replacement application

Fig 3, illustrates the information security requirements coupled with the Cloud computing deployment model and delivery models [8, 13]. In Fig 3[8], an “X” denoting mandatory requirements and an asterisk (*) denoting optional requirements. Each of the security requirements will be highlighted below in context of cloud computing



Information Security Requirements	Public Cloud			Private Cloud			Hybrid Cloud		
	IAAS	SAAS	PAAS	IAAS	SAAS	PAAS	IAAS	SAAS	PAAS
Identification & Authentication	X	X	*	X	X	*	*	X	*
Authorisation	X	X	X	*	X	*	*	X	*
Confidentiality	*	X	*	*	X	X	*	X	*
Integrity	X	X	*	*	X	X	X	X	X
Non-repudiation	*	X	*	*	X	*	*	*	*
Availability	X	*	X	X	X	X	*	*	*

Figure 3: Cloud computing security requirements

1. **Authorization**

Authorization is an important information security requirement in Cloud computing to ensure referential integrity is maintained. It follows on in exerting control and privileges over process flows within cloud computing. In case of public cloud, multiple customers share the computing resources provided by a single service provider. So proper authorization is required irrelevant of the delivery model used. In private cloud, authorization is maintained by the system administrator, identification & authentication. As the major concerns in public and private cloud include internal and external threats, data collection, privacy and compliance, so, it is the cloud service provider's ability to have a secure infrastructure to protect customer data and guard against unauthorized access. We need to have some identification and authentication process to verifying and validating individual cloud users based upon their credentials before accessing any data over the cloud. That's why identification and authentication is mandatory security requirement in public and private cloud.

2. **Integrity**

The integrity requirement lies in applying the due diligence within the cloud domain mainly when accessing data. Therefore ACID (atomicity, consistency, isolation and durability) properties of the cloud's data should without a doubt be robustly imposed across all Cloud computing delivery models.

3. **Confidentiality**

In Cloud computing, confidentiality plays a major part especially in maintaining control over organizations' data situated across multiple distributed databases. Asserting confidentiality of users' profiles and protecting their data, that is virtually accessed, allows for information security protocols to be enforced at various different layers of cloud applications. Data confidentiality is one of the most difficult things to guarantee in a public cloud computing environment. There are several reasons for that: First, as public clouds grow, the number of people working for the cloud provider who actually have access to customer data (whether they are entitled to it or not) grows as well, thereby multiplying the number of potential sources for a confidentiality breach. Second, the needs for elasticity, performance, and fault-tolerance lead to massive data duplication and require aggressive data caching, which in turn multiply the number of targets a data thief can go after. Third, end-to-end data encryption is not yet available. So, data confidentiality will be maximized by using a large number of private clouds managed by trusted parties.

4. Availability

Availability is one of the most critical information security requirements in Cloud computing because it is a key decision factor when deciding among private, public or hybrid cloud vendors as well as in the delivery models. The service level agreement is the most important document which highlights the trepidation of availability in cloud services and resources between the cloud provider and client. The goal of availability for Cloud Computing systems (including applications and its infrastructures) is to ensure its users can use them at any time, at any place. Many Cloud Computing system vendors provide Cloud infrastructures and platforms based on virtual machines. So availability is a mandatory security requirement for IaaS and PaaS whether the public cloud is used or private cloud. As in private cloud, all services are internal to the enterprise, so availability is also required when SaaS is to be used.

5. Non-repudiation

Non-repudiation in cloud computing can be obtained by applying the traditional ecommerce security protocols and token provisioning to data transmission within cloud applications such as digital signatures, timestamps and confirmation receipts services (digital receipting of messages confirming data sent/received).

5.0 SECURITY CHALLENGES

Cloud computing environments are multinomial environments in which each domain can use different security, privacy, and trust requirements and potentially employ various mechanisms, interfaces, and semantics [5]. Main security challenges in cloud computing and their solutions are discussed below:

1. Service Level Agreement
2. Authentication and Identity Management
3. Data Security and Protection
4. Trust Management
5. Access Control and Accounting
6. Charging Model
7. Costing Model
8. What to migrate
9. Cloud Interoperability Issue

5.1 Service Level Agreement

A Service level agreement (SLA) [6] is a part of a service contract between the consumer and provider that formally defines the level of service. It is used to identify and define the customer's needs and to reduce areas of conflict like Services to be delivered Performance, Tracking and Reporting Problem Management Legal Compliance and Resolution of Disputes, Customer Duties and Responsibilities, Security IPR and Confidential Information Termination.

5.2 Authentication and Identity Management

By using the cloud services, the user can access the information from various places over the internet. So we need some Identity Management (IDM) [5] mechanism to authenticate users and provide services to them based on credentials and characteristics. An IDM system should be able to protect private and sensitive information related to users and processes .Every enterprise will have its own identity management system to control access to information and computing resources.

5.3 Data Centric Security and Protection

In cloud computing, number of customers can share, save and access the data over the cloud. So data from one customer must be properly segregated from that of another and it must be able to move securely from one location to another [5]. Cloud providers must implement the proper security measures to prevent data leaks or access by third unauthorized parties. The cloud provider should carefully assign privileges to the customers and also ensure that assigned duties cannot be defeated, even by privileged users at the cloud provider. Access control policies should be properly implemented. When someone wants to access data, the system should check its policy rules and reveal it only if the policies are satisfied. Existing cryptographic techniques can be used for data security.

5.4 Trust Management

In cloud computing environments, the customer is dependent on provider for various services. In many services, the customer has to store his confidential data on the provider’s side. Thus, a trust framework should be developed to allow for efficiently capturing a generic set of parameters required for establishing trust and to manage evolving trust and interaction/sharing requirements.

5.5 Access Control and Accounting

Due to heterogeneity and diversity in cloud computing services, a fine grained access control policies should be enforced. Access control services should be flexible enough to capture dynamic, attribute- or credential-based access requirements. The access control models should also be able to capture relevant aspects of SLAs. As the cloud computing model is pay-per-usage model, so proper accounting records for users are required for billing purposes. In clouds, service providers usually do not know their users in advance, so it is difficult to assign roles to users directly. Therefore, credential- or attribute-based policies can be used to enhance this capability. Security Assertion Markup Language (SAML), Extensible Access Control Markup Language (XACML), and Web services standards can be used to specify the secure access control policies.

5.6 Charging Model

The elastic resource pool has made the cost analysis a lot more complicated than regular data centers, which often calculates their cost based on consumptions of static computing. Moreover, an instantiated virtual machine has become the unit of cost analysis rather than the underlying physical server. For SaaS cloud providers, the cost of developing multitenant within their offering can be very substantial. These include: re-design and redevelopment of the software that was originally used for single-tenancy, cost of providing new features that allow for intensive customization, performance and security enhancement for concurrent user access, and dealing with complexities induced by the above changes. Consequently, SaaS providers need to weigh up the trade-off between the provision of multitenant and the cost-savings yielded by multi-tenancy such as reduced overhead through amortization, reduced number of on-site software licenses, etc. Therefore, a strategic and viable charging model for SaaS provider is crucial for the profitability and sustainability of SaaS cloud providers. [8]

5.7 Costing Model

Cloud consumers must consider the tradeoffs amongst computation, communication, and integration. While migrating to the Cloud can significantly reduce the infrastructure cost, it does raise the cost of data communication, i.e. the cost of transferring an organization's data to and from the public and community Cloud and the cost per unit of computing resource used is likely to be higher. This problem is particularly prominent if the consumer uses the hybrid cloud deployment model where the organization's data is distributed amongst a number of public/private (in-house IT infrastructure)/community clouds. Intuitively, on demand computing makes sense only for CPU intensive jobs. [8]

5.8 What to migrate

Based on a survey (Sample size = 244) conducted by IDC in 2008, the seven IT systems or applications being migrated to the cloud are: IT Management Applications (26.2%), Collaborative Applications (25.4%), Personal Applications (25%), Business Applications (23.4%), Applications Development and Deployment (16.8%), Server Capacity (15.6%), and Storage Capacity (15.5%). This result reveals that organizations still have security/privacy concerns in moving their data on to the Cloud. Currently, peripheral functions such as IT management and personal applications are the easiest IT systems to move. Organizations are conservative in employing IaaS compared to SaaS. This is partly because marginal functions are often outsourced to the Cloud, and core activities are kept in-house. The survey also shows that in three years' time, 31.5% of the organization will move their Storage Capacity to the cloud. However this number is still relatively low compared to Collaborative Applications (46.3%) at that time. [1]

5.9 Cloud Interoperability Issue

Currently, each cloud offering has its own way on how cloud clients/applications/users interact with the cloud, leading to the "Hazy Cloud" phenomenon. This severely hinders the development of cloud ecosystems by forcing vendor locking, which prohibits the ability of users to choose from alternative vendors/offering simultaneously in order to optimize resources at different levels within an organization. More importantly, proprietary cloud APIs makes it very difficult to integrate cloud services with an organization's own existing legacy systems (e.g. an on-premise data center for highly interactive modeling applications in a pharmaceutical company).The primary goal of interoperability is to realize the seamless fluid data across clouds and between cloud and local applications. There are a number of levels that interoperability is essential for cloud computing. First, to optimize the IT asset and computing resources, an organization often needs to keep in-house IT assets and capabilities associated with their core competencies while outsourcing marginal functions and activities (e.g. the human resource system) on to the cloud. Second, more often than not, for the purpose of optimization, an organization may need to outsource a number of marginal functions to cloud services offered by different vendors. Standardization appears to be a good solution to address the interoperability issue. However, as cloud computing just starts to takeoff, the interoperability problem has not appeared on the pressing agenda of major industry cloud vendors. [8]

6.0CONCLUSION

We have argued that it is very important to take security and privacy into account when designing and using cloud services. In this paper security in cloud computing was elaborated in a way that covers security issues and challenges, security standards and security management models.

- Security issues indicate potential problems which might arise.
- Security standards offer some kind of security templates which cloud service providers (CSP) could obey. The most promising standard for the future would be OVF format which promises creation of new business models that will allow companies to sell a single product on premises, on demand, or in a hybrid deployment model.
- Security management models offer recommendations based on security standards and best practices. [12]

These are all very important topics which will be certainly discussed in the upcoming years of cloud computing. Based on IDC survey [13] the security and vulnerability market should exceed revenue of $4.4 billion by the end of 2013, with a climbing annual growth rate resulting in a compound annual growth rate (CAGR) of 10.8%. This survey shows that products that fall within the security and vulnerability management market will remain in high demand.

7.0 REFERENCES

1. 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].

2. S. Arnold (2009, Jul.). “Cloud computing and the issue of privacy.” KM World, pp14-22. Available: www.kmworld.com [Aug. 19, 2009] cloudcomputingsecurity-risks-853? page=0, 1> [Mar. 13, 2009].

3. A Platform Computing Whitepaper. “Enterprise Cloud Computing: Transforming IT.” Platform Computing, pp6, 2010.

4. Global Netoptex Incorporated.“Demystifying the cloud. Important opportunities, crucial choices.” pp4-14. Available: http://www.gni.com [Dec. 13, 2009].

5. Takabi, H., Joshi, J.B.D.: Security and privacy challenges in cloud computing environment. IEEE Journal on Securityand Privacy 8(6) (November 2010)

6. Kandukuri, B.R., Paturi, R., Rakshit, A.: Cloud Security Issues. In: The Proceedings of IEEE International Conference on Service Computing, pp. 517–520 (2009)

7. Subashini, S., Kavitha, V.: A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Application, 1–11 (2010)

8. Ramgovind, S., Eloff, M.M., Smith, E.: The management of security in cloud computing. In: The Proceedings of IEEE Conference on Information Security for South Africa-2010 (2010)

9. Dlamini, M.T., Eloff, M.M., Eloff, J.H.P.: Internet of People, Things and Services – The Convergence of Security, Trust and Privacy. In: The Proceeding of 3rd Annual CompanionAble Consortium Workshop-IoPTs, Brussel (December 2009)

10. Mell, P., Grance, T.: The NIST definition of Cloud Computing, version 15. National Institute of Standards and Technology (NIST), Information Technology Laboratory (October 7, 2009), http://www.csrc.nist.gov

11. Buyya, R., Yeo, C.S., Venugopal, S., Broberg, J., Bandic, I.: Cloud Computing and emerging IT platforms: vision, hype, and relatity for deliverling computing as the 5th utility. Future Generation Computer System 25(6), 599–616 (2009)

12. Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud Computing V2.1, http://www.cloudsecurityalliance.org/, December 2009

13. International Data Corporation, Worldwide Security and Vulnerability Management 2009 2013 Forecast and 2008 Vendor Shares, http://vulnerabilitymanagement.com/docs/IDC_MA_2009.pdf

14. Popović, Krešimir, and Željko Hocenski. "Cloud computing security issues and challenges." MIPRO, 2010 proceedings of the 33rd international convention. IEEE, 2010.

15. So, Kuyoro. "Cloud computing security issues and challenges." International Journal of Computer Networks 3.5 (2011): 247-55.

16. Swapna, K., and Praveen Gupta. "Cloud Computing: Security Issues and Challenges." AADYA-National Journal of Management and Technology (NJMT) 3.2 (2015): 149-154.

17. Verma, Amandeep, and Sakshi Kaushal. "Cloud computing security issues and challenges: a survey." Advances in Computing and Communications (2011): 445-454.