Reviewing Security Concerns in Cloud Environment

Shivani Garg[*]
CSE Department
Sharda University
shivani.garg@sharda.ac.in

Mukul Varshney
CSE Department
Sharda University
mukul.varshney@sharda.ac.in

Abha Kiran Rajpoot
CSE Department
Sharda University
abhakiran.rajpoot@sharda.ac.in

Jyotsna
CSE Department
Sharda University
jyotsna.seth@sharda.ac.in

Abstract— Cloud computing is a set of IT services provided to a customer over a network with the ability to scale up or down the service requirements. Cloud computing is being considered as the next generation architecture for IT enterprises. In cloud, data is transferred among the server and client. This technology allows much more efficient computing by centralizing data storage, processing and bandwidth. The emergence of cloud computing has left a tremendous impact on the Information Technology (IT) industry over the past few years. This paper discusses various issues and challenges of cloud computing security.
Keywords— Cloud computing, privacy, infrastructure, virtualization, Information Technology

I. INTRODUCTION

For years, the Internet has been represented on network diagrams by a cloud symbol. But it is only until 2008 when a variety of new services started to emerge that permitted computing resources, as shown in figure1, to be accessed over the Internet termed cloud computing. Cloud computing includes activities like 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 provides a way of increasing the capacity or adding capabilities dynamically without investing in new infrastructure, training new personnel, or licensing new software. It is used to extend 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 fastest growing segments of the IT industry. But with the growing information placed on the cloud, safety concerns on the cloud environment have begun to grow. Despite of the popularity of the cloud, customers are still reluctant to deploy their business in the cloud. Security issues in cloud computing are a major hindrance on its acceptance. Security is the greatest challenging issue of cloud computing.
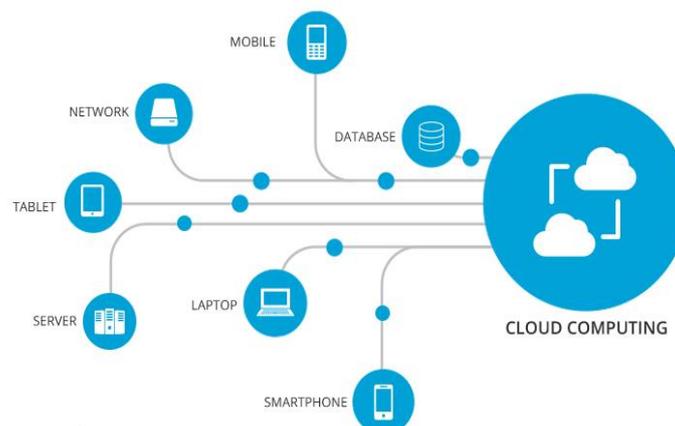

FIGURE 1: Cloud computing environment

On one hand, security could improve due to centralization of data and increased security-focused resources. 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 survey more specific to the different security issues and the associated challenges that has emanated in the cloud computing system.

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. In the last few years, cloud computing [6] received considerable attention, as a promising approach for delivering Information and Communication Technology (ICT) services. With the fast development of processing, storage technologies, the sensation of the Internet, and computing resources have become cheaper, more powerful and more universally available than ever before. This technological trend has enabled the realization of a new computing model called cloud computing. From the past few years, the cloud computing has made a tremendous impact on the Information Technology (IT) industry, where large companies such as Google, IBM, Amazon and Microsoft struggle to provide more powerful, reliable and cost-efficient cloud platforms, and business enterprises seek to find new paradigm in their business models [16].

II. RELATED WORK

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 - information transmitted from the client through the Internet poses a certain degree of risk, because of issues of data ownership; enterprises should spend time getting to know their providers and their regulations as much as possible before assigning some trivial applications first to test the water,
2. Regulatory compliance - clients are accountable for the security of their solution, as they can choose between providers that allow to be audited by 3rd party organizations that check levels of security and providers that don't.
3. Data location - depending on contracts, some clients might never know what country or what jurisdiction their data is located.
4. Data segregation - encrypted information from multiple companies may be stored on the same hard disk, so a mechanism to separate data should be deployed by the provider.
5. Recovery - every provider should have a disaster recovery protocol to protect user data.
6. Investigative support - if a client suspects faulty activity from the provider, it may not have many legal ways pursue an investigation
7. Long-term viability - refers to the ability to retract a contract and all data if the current provider is bought out by another firm. [2]

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.[7] ENISA investigated the different security risks related to adopting cloud computing along with the affected assets, the risks likelihood, impacts, and vulnerabilities in the cloud computing may lead to such risks.[8] Balachandra et al, 2009 discussed the security SLA's specification and objectives related to data locations, segregation and data recovery.[9] Kresimir et al, 2010 discussed high level security concerns in the cloud computing model such as data integrity, payment and privacy of sensitive information.[10] 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.[11] Subashini et al discuss the security challenges of the cloud service delivery model, focusing on the SaaS model.[12] Ramgovind et al, (2010) discussed the management of security in Cloud computing focusing on Gartner's list on cloud security issues and the findings from the International Data Corporation enterprise.[13] Morsy et al, 2010 investigated cloud computing problems from the cloud architecture, cloud offered characteristics, cloud stakeholders, and cloud service delivery models perspectives.[14] A recent survey by Cloud Security Alliance (CSA)&IEEE indicates that enterprises across sectors are eager to adopt cloud computing but that security are needed both to accelerate cloud adoption on a wide scale and to respond to regulatory drivers. It also details that cloud computing is shaping the future of IT but the absence of a compliance environment is having dramatic impact on cloud computing growth.[15] Several studies have been carried out relating to security issues in cloud computing but this work presents a detailed analysis of the cloud computing security issues and challenges focusing on the cloud computing deployment types and the service delivery types.

III.SECURITY ISSUES IN CLOUD COMPUTING

3.1 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 depicted in figure 2. The Cloud Computing model has three main deployment models which are:

3.1.1 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 data centre. 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, like an 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. [15]

3.1.2 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, like a prepaid electricity metering system which is flexible enough to cater for spikes in demand for cloud optimization. [16] 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.

3.1.3 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 [20]. 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.
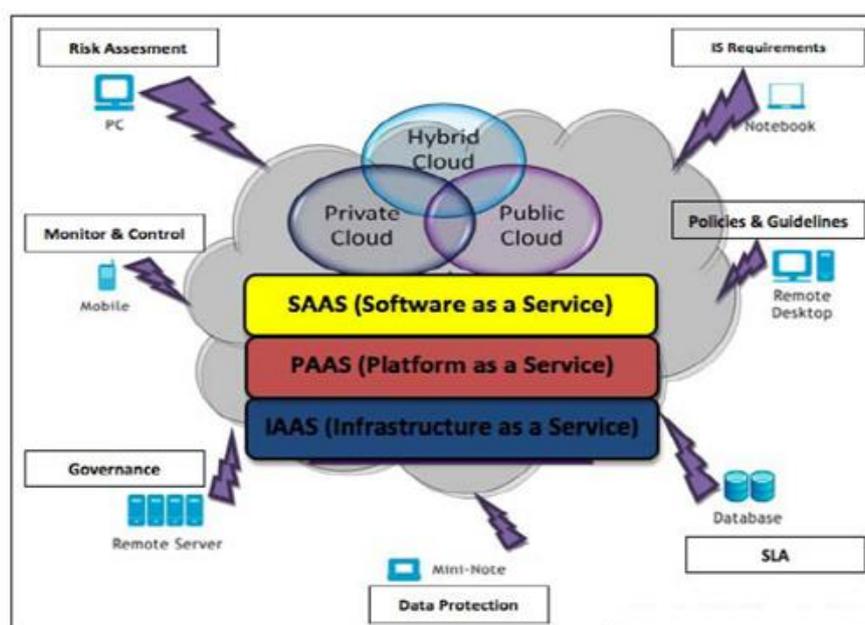

FIGURE 2: Cloud deployment model [13]

3.2 Cloud Computing Service Delivery Models

Following on the cloud deployment models, the next security consideration relates to the various cloud computing service delivery 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).

3.2.1 Infrastructure as a Service (IaaS)

Infrastructure as a Service is a single tenant cloud layer where the Cloud computing vendor's dedicated resources are only shared with contracted clients at a pay-per-use fee. This greatly minimizes the need for huge initial investment in computing hardware such as servers, networking devices and processing power. They also allow varying degrees of financial and functional flexibility not found in internal data centres or with collocation services, because computing resources can be added or released much more quickly and cost-effectively than in an internal data centre or with a collocation service [2]. IaaS and other associated services have enabled start-ups and other businesses focus on their core competencies without worrying much about the provisioning and management of infrastructure. IaaS completely

abstracted the hardware beneath it and allowed users to consume infrastructure as a service without bothering anything about the underlying complexities. The cloud has a compelling value proposition in terms of cost, but 'out of the box' IaaS only provides basic security (perimeter firewall, load balancing, etc.) and applications moving into the cloud will need higher levels of security provided at the host.

3.2.2. Platform as a service (PaaS)

Platform-as-a-Service (PaaS) is a set of software and development tools hosted on the provider's servers. It is one layer above IaaS on the stack and abstracts away everything up to OS, middleware, etc. This offers an integrated set of developer environment that a developer can tap to build their applications without having any clue about what is going on underneath the service. It offers developers a service that provides a complete software development life cycle management, from planning to design to building applications to deployment to testing to maintenance. Everything else is abstracted away from the "view" of the developers. Platform as a service cloud layer works like IaaS but it provides an additional level of 'rented' functionality. Clients using PaaS services transfer even more costs from capital investment to operational expenses but must acknowledge the additional constraints and possibly some degree of lock-in posed by the additional functionality layers [17]. The use of virtual machines act as a catalyst in the PaaS layer in Cloud computing. Virtual machines must be protected against malicious attacks such as cloud malware. Therefore, maintaining the integrity of applications and well enforcing accurate authentication checks during the transfer of data across the entire networking channels is fundamental.

3.2.3 Software as a Service

Software-as-a-Service is a software distribution model in which applications are hosted by a vendor or service provider and made available to customers over a network, typically the Internet. SaaS is becoming an increasingly prevalent delivery model as underlying technologies that support web services and service-oriented architecture (SOA) mature and new developmental approaches become popular. SaaS is also often associated with a pay-as-you-go subscription licensing model. Meanwhile, broadband service has become increasingly available to support user access from more areas around the world. SaaS is most often implemented to provide business software functionality to enterprise customers at a low cost while allowing those customers to obtain the same benefits of commercially licensed, internally operated software without the associated complexity of installation, management, support, licensing, and high initial cost. The architecture of SaaS-based applications is specifically designed to support many concurrent users (multitenancy) at once. Software as a service applications are accessed using web browsers over the Internet therefore web browser security is vitally important. Information security officers will need to consider various methods of securing SaaS applications. Web Services (WS) security, Extendable Markup Language (XML) encryption, Secure Socket Layer (SSL) and available options which are used in enforcing data protection transmitted over the Internet. [11]
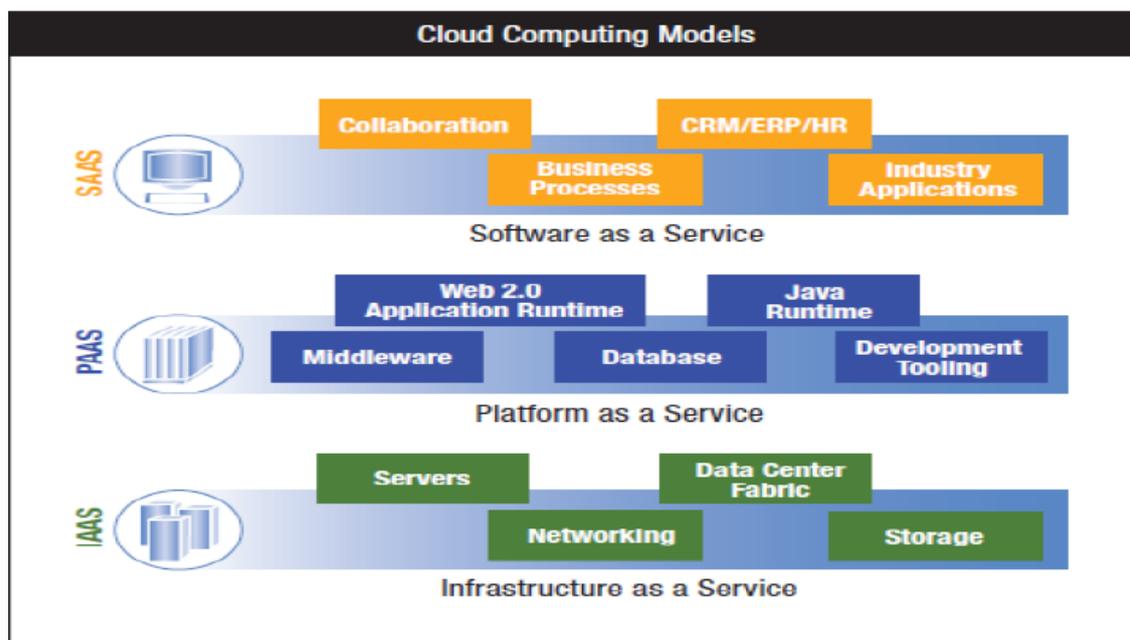

FIGURE 2: Cloud computing service delivery models [15]

Combining the three types of clouds with the delivery models we get a holistic cloud illustration as seen in Figure 3, surrounded by connectivity devices coupled with information security themes. Virtualized physical resources, virtualized infrastructure, as well as virtualized middleware platforms and business applications are being provided and consumed as services in the Cloud [18]. Cloud vendors and clients' need to maintain Cloud computing security at all interfaces. Figure 4 presents a comparison between various Cloud Computing service delivery models. It shows what things customer

needs to manage at its own end and what things the vendor will manage for the customer. The next section of the paper introduces challenges faced in the Cloud computing domain.
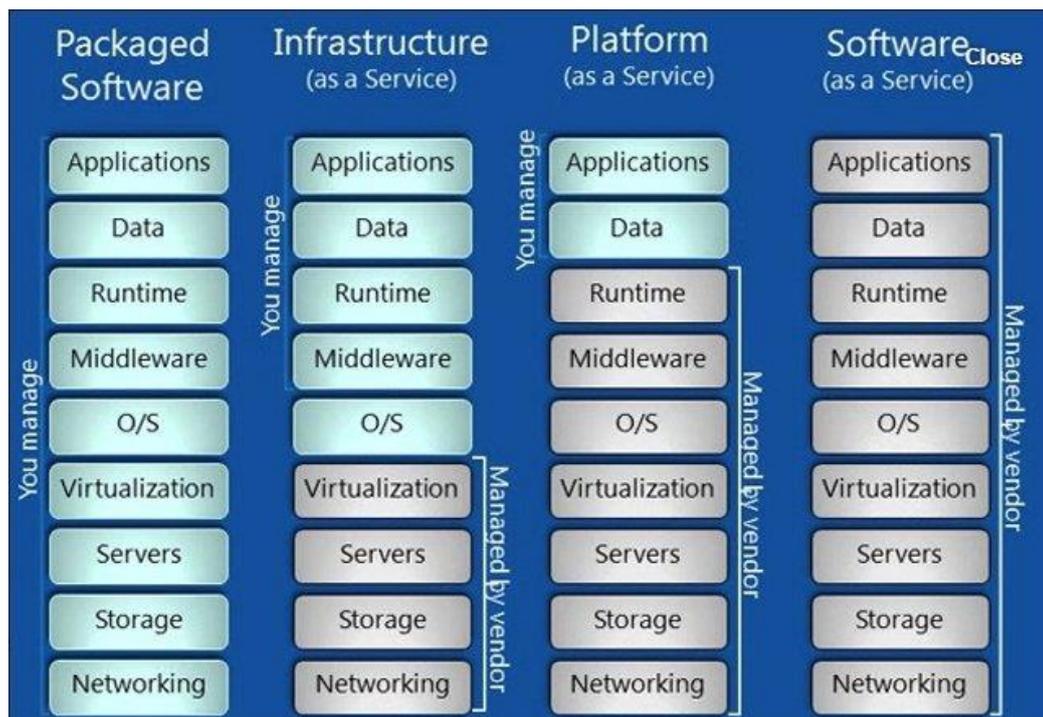

FIGURE 4: Comparison of Cloud Computing Service Delivery Models

IV. CLOUD COMPUTING CHALLENGES

The current adoption of cloud computing is associated with numerous challenges because users are still skeptical about its authenticity. Based on a survey conducted by IDC in 2008, the major challenges that prevent Cloud Computing from being adopted are recognized by organizations are as follows:

A. Security: The security issue has played the most important role in hindering Cloud computing acceptance. Without doubt, putting your data, running your software on someone else's hard disk using someone else's CPU appears daunting to many. Well-known security issues such as data loss, phishing, botnet (running remotely on a collection of machines) pose serious threats to organization's data and software. Moreover, the multi-tenancy model and the pooled computing resources in cloud computing has introduced new security challenges that require novel techniques to tackle with. For example, hackers can use Cloud to organize botnet as Cloud often provides more reliable infrastructure services at a relatively cheaper price for them to start an attack.[12]

B. 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, ondemand computing makes sense only for CPU intensive jobs.[12]

C. 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 multitenancy 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 multitenancy 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. [12]

D. Service Level Agreement (SLA): Although cloud consumers do not have control over the underlying computing resources, they do need to ensure the quality, availability, reliability, and performance of these resources when consumers have migrated their core business functions onto their entrusted cloud. In other words, it is vital for consumers to obtain guarantees from providers on service delivery. Typically, these are provided through Service Level Agreements (SLAs) negotiated between the providers and consumers. The very first issue is the definition of SLA specifications in

such a way that has an appropriate level of granularity, namely the tradeoffs between expressiveness and complicatedness, so that they can cover most of the consumer expectations and is relatively simple to be weighted, verified, evaluated, and enforced by the resource allocation mechanism on the cloud. In addition, different cloud offerings (IaaS, PaaS, and SaaS) will need to define different SLA metaspecifications. This poses several implementation problems for the cloud providers. Furthermore, advanced SLA mechanisms need to constantly incorporate user feedback and customization features into the SLA evaluation framework. [19]

E. What to migrate: Based on a survey (Sample size = 244) conducted by IDC in 2008, the seven IT systems/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]

F. 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 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 centre 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 several 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, often, for optimization purpose, an organization may need to outsource several 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 take off, the interoperability problem has not appeared on the pressing agenda of major industry cloud vendors. [12]

V. CONCLUSIONS

Although Cloud computing be a new phenomenon which is set to revolutionise the way we use the Internet, there is much to be cautious about. There are many new technologies emerging at a rapid rate, each with technological advancements and with the potential of making human's lives easier. However, one must be very careful to understand the security risks and challenges posed in utilizing these technologies. Cloud computing is no exception. In this paper key security considerations and challenges which are currently faced in the Cloud computing are highlighted. Cloud computing has the potential to become a frontrunner in promoting a secure, virtual and economically viable IT solution in the future.

REFERENCES

[1] F. Gens. (2009, Feb.). "New IDC IT Cloud Services Survey: Top Benefits and Challenges", IDC eXchange, Available: [Feb. 18, 2010].

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

[3] A Platform Computing Whitepaper. "Enterprise Cloud Computing: Transforming IT." Platform Computing, pp6, 2010.

[4] Arnold S., "Cloud computing and the issue of privacy." KM World, pp14-22. Available: www.kmworld.com [Aug. 19, 2009].

[5] Available from: http://csrc.nist.gov/publications/nistpubs/800- 145/SP800-145.pdf. Last visited on the 12th November, 2012.

[6] Cloud Computing Use Case Discussion Group. "Cloud Computing UseCases Version 3.0," 2010.

[7] 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].

[8] 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.

[9] 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.

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

[11] 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.

[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] A Platform Computing Whitepaper. "Enterprise Cloud Computing: Transforming IT." Platform Computing, pp6, 2010.

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

[18] M. Klems, A. Lenk, J. Nimis, T. Sandholm and S. Tai. "What's Inside the Cloud? An Architectural Map of the Cloud Landscape." IEEE Xplore, pp 23-31, Jun. 2009.

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

[20] N. Gruschka, L. L. Iancono, M. Jensen and J. Schwenk. "On Technical Security Issues in Cloud Computing" In PROC 09 IEEE International Conference on Cloud Computing, 2009 pp 110-112.