Efficient Appraisal of Cloud Computing Through Comprehensive Confrontation of Security Issues and Discrepancies Involved

Rajesh T[1], Vihari P[2]
[1]Department of ECE,
[2]Department of ECE,
K L University,Vaddeswaram
Guntur District

Abstract - Cloud computing is a new computational paradigm that an innovative business model allows organizations to adopt without prior IT investments well. Despite the potential benefits derived from the cloud computing, the security model is still the question of where the cloud model affects adoption. The security problem is complicated by the cloud model as new dimensions of the problem scope with respect to the model architecture, multi-tenancy, elasticity, and were entered. Dependency stack In this paper, a detailed analysis of the cloud security problem we. Introduce We investigated the problem from the perspective of architecture cloud, the cloud features offered perspective, the perspective of the cloud stakeholders, and cloud service delivery models perspective. Based on this analysis, we conduct a detailed specification of the cloud security problem and the main functions to be covered by any proposed security.
Keywords: cloud computing; cloud computing security; cloud computing security management.

I. INTRODUCTION

The term *cloud* has been used historically as a metaphor for the Internet. This usage was originally derived from its common depiction in network diagrams as an outline of a cloud, used to represent the transport of data across carrier backbones (which owned the cloud) to an endpoint location on the other side of the cloud. This concept dates back as early as 1961,when Professor John McCarthy suggested that computer time-sharing technology might lead to a future where computing power and even specific applications might be sold through a utility-type business model. This idea became very popular in the late 1960s, but by the mid-1970s the idea faded away when it became clear that the IT-related technologies of the day were unable to sustain such a futuristic computing model. However, since the turn of the millennium, the concept has been revitalized. It was during this time of revitalization that the term *cloud computing* began to emerge in technology circles**.**

Multi-tenancy and elasticity are two key characteristics of the cloud model. Multi-Tenancy enables sharing the same service instance among different tenants. Elasticity enables scaling up and down resources allocated to a service based on the current service demands. Both characteristics focus on improving resource utilization, cost and service availability. The cloud model has motivated industry and academia to adopt cloud computing to host a wide spectrum of applications ranging from high computationally intensive applications down to light weight services**..**

According to a Gartner survey on cloud computing revenues, the cloud market was worth USD 58.6B in 2009 , is expected to be USD 68B in 2010 and will reach USD 148B by 2014. These revenues imply that cloud computing is a promising platform. On the other hand, it increases the attackers' interest in finding existing vulnerabilities in the model.

Despite the potential benefits and revenues that could be gained from the cloud computing model, the model still has a lot of open issues that impact the model creditability and pervasiveness. Vendor lock-in, multi-tenancy and isolation, data management, service

portability, elasticity engines, SLA management, and cloud security are well known open research problems in the cloud computing model.From the cloud consumers' perspective, security is the major concern that hampers the adoption of the cloud computing model because:

- Hosting this set of valuable assets on publicly available infrastructure increases the probability of attacks.
- Co-existence of assets of different tenants in the same location and using the same instance of the service while being unaware of the strength of security controls used.
- The lack of security guarantees in the SLAs between the cloud consumers and the cloud providers.
- Enterprises outsource security management to a third party that hosts their IT assets (loss of control).

From the cloud providers' perspective, security requires a lot of expenditures (security solutions' licenses), resources (security is a resource consuming task), and is a difficult problem to master (as we discuss later). But skipping security from the cloud computing model roadmap will violate the expected revenues as explained above. So cloud providers have to understand consumers' concerns and seek out new security solutions

that resolve such concerns.

In this paper we analyze existing challenges and issues involved in the cloud computing security problem. We group these issues into architecture-related issues, service delivery model-related issues, cloud characteristic-related issues, and cloud stakeholder-related issues. This will help cloud providers and security vendors to have a better understanding of the problem. It also helps researchers being aware of the existing problem dimensions and gaps.

Our paper is organized as follows. In section II, we explore previous efforts in defining cloud security problems and challenges. Sections III to VII explore the cloud computing security problem from different perspectives. Section VIII discusses the key security enablers in the cloud model. Section IX summarizes our conclusions and what we believe are the key dimensions that should be covered by any cloud security solution. Finally, in section X we discuss the future work focusing on one of the discussed security enablers (cloud security management)

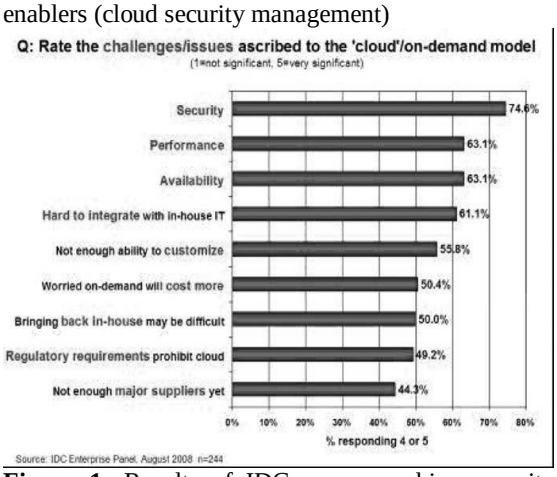

Figure 1: Results of IDC survey ranking security challenges

II. Cloud security challenges

Although virtualization and cloud computing can help companies accomplish more by breaking the physical bonds between an IT infrastructure and its users, heightened security threats must be over come in order to benefit fully from this new computing Paradigm. This is particularly true for the SaaS provider. Some security concerns are worth more discussion. For example, in the cloud, you lose control over assets in some respects, so your security model must be reassessed. Enterprise security is only as good as the least reliable partner, department, or vendor.

With the cloud model, you lose control over physical security. In a public cloud, you are sharing computing resources with other companies. In a shared pool outside the enterprise, you don't have any knowledge or control of where the resources run. Exposing your data in an environment shared with other companies could give the government "reasonable cause" to seize your assets because another company has violated the law. Simply because you share the environment in the cloud, may put your data at risk of seizure. Storage services provided by one cloud vendor may be incompatible with another vendor's services should you decide to move from one to the other. Vendors are known for creating what the hosting world calls "sticky services"—services that an end user may have difficulty transporting from one cloud vendor to another (e.g., Amazon's "Simple Storage Service" is incompatible with IBM's Blue Cloud, or Google, or Dell

Cloud-based services will result in many mobile IT users accessing business data and services without traversing the corporate network. This will increase the need for enterprises to place security controls between mobile users and cloud-based services. Placing large amounts of sensitive data in a globally accessible cloud leaves organizations open to large distributed threats—attackers no longer have to come onto the premises to steal data, and they can find it all in the one "virtual" location.

In our research we did a deep investigation in the cloud model to identify the root causes and key participating dimensions in such security issues/problems discussed by the previous work. This will help better to understand the problem and deliver solutions.

III. Architecture of Cloud computing

The Cloud Computing model has three service delivery models and main three deployment models . The deployment models are: (1) Private cloud: a cloud platform is dedicated for specific organization, (2) Public cloud: a cloud platform available to public users to register and use the available infrastructure, and (3) Hybrid cloud: a private cloud that can extend to use resources in public clouds. Public clouds are the most vulnerable deployment model because they are available for public users to host their services who may be malicious users.

The cloud service delivery models include:

-Communication-as-a-Service (CaaS):

CaaS is an outsourced enterprise communications solution. Providers of this type of cloud-based solution (known as CaaS vendors) are responsible for the management of hardware and software required for delivering Voiceover IP (VoIP) services, Instant Messaging (IM), and video conferencing capabilities to their customers. This model began its evolutionary process from within the telecommunications (Telco) industry, not unlike how the SaaS model arose from the software delivery services sector. CaaS vendors are responsible for all of the hardware and software management consumed by their user base. CaaS vendors typically offer guaranteed quality of service (QoS) under a service-level agreement (SLA)

-Infrastructure-as-a-Service (IaaS) :

Infrastructure-as-a-Service(IaaS) is the delivery of computer infrastructure (typically a platform virtualization environment) as a service. IaaS leverages significant technology,services, and data center investments to deliver IT as a service to customers.

Unlike traditional outsourcing, which requires extensive due

diligence, negotiations ad infinitum, and complex, lengthy contract vehicles, IaaS is centered around a model of service delivery that provisions a predefined, standardized infrastructure specifically optimized for the customer's applications. Simplified statements of work

and à la carte service-level choices make it easy to tailor a solution to a customer's specific application requirements. IaaS providers manage the transition and hosting of selected applications on their infrastructure. Customers maintain ownership and management of their application(s) while off-loading hosting operations and infrastructure management to the IaaS provider

- Monitoring-as-a-Service (MaaS):

Monitoring-as-a-Service (MaaS) is the outsourced provisioning of security, primarily on business platforms that leverage the Internet to conduct business.8 MaaS has become increasingly popular over the last decade. Since the advent of cloud computing, its popularity has, grown even more. Security monitoring involves protecting an enterprise or government client from cyber threats. A security team plays a crucial role in securing and maintaining the confidentiality, integrity, and availability of IT assets. However, time and resource constraints limit security operations and their effectiveness for most companies. This requires constant vigilance over the security infrastructure and critical information assets..

-Platform-as-a-Service (Paas) :

Cloud computing has evolved to include platforms for building and running custom web-based applications, a concept known as Platform-as-a-Service. PaaS is an outgrowth of the SaaS application delivery model. The PaaS model makes all of the facilities required to support the complete lifecycle of building and delivering web applications and services entirely available from the Internet, all with no software downloads or installation for developers, IT managers, or end users. Unlike the IaaS model, where developers may create a specific operating system instance with homegrown applications running, PaaS developers are concerned only with web based development and generally do not care what operating system is used..

-Software-as-a-Service (SaaS):

The traditional model of software distribution, in which software is purchased for and installed on personal computers, is sometimes referred to as Software-as-a-Product. 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.

IV. Cloud computing characteristics and Security implications

There are several key characteristics of a cloud computing environment. Service offerings are most often made available to specific consumers and small businesses that see the benefit of use because their capital expenditure is minimized. This serves to lower barriers to entry in the marketplace, since the infrastructure used to provide these offerings is owned by the cloud service provider and need not be purchased by the customer. Because users are not tied to a specific device (they need only the ability to access the Internet) and because the Internet allows for location independence, use of the cloud enables cloud computing service providers' customers to access cloud enabled systems regardless of where they may be located or what device they choose to use.

Multitenancy enables sharing of resources and costs among a large pool of users. Chief benefits to a multitenancy approach include:

1. Centralization of infrastructure and lower costs
2. Increased peak-load capacity
3. Efficiency improvements for systems that are often under utilized
4. Dynamic allocation of CPU, storage, and network bandwidth

Another benefit that makes cloud services more reliable is that scalability can vary dynamically based on changing user demands. Because the service provider manages the necessary infrastructure, security often is vastly improved. As a result of data centralization, there is an increased focus on protecting customer resources maintained by the service provider. To assure customers that their data is safe, cloud providers are quick to invest in dedicated security staff. This is largely seen as beneficial but has also raised concerns about a user's loss of control over sensitive data. Access to data is usually logged, but accessing the audit logs can be difficult or even impossible for the customer.

V.Cloud Computing's deep depend enncies Stack

The cloud computing model depends on a deep stack of dependent layers of objects (VMs, A PIs, Services and Applications) where the functionality and security of a higher layer depends on the lower ones. The IaaS model covers cloud physical infrastructure layer (storage, networks and servers), virtualization layer (hypervisors), and virtualized resources layer (VMs, virtual storage, virtual networks). The PaaS model covers the platform layers (such as application servers, web servers, IDEs, and other tools), and APIs and Services layers. The PaaS layer depends on the virtualization of resources as delivered by IaaS. The SaaS model covers applications and services offered as a service for end users. The SaaS layer depends on a layer of platforms to host the services and a layer of virtualization to optimize resources utilization when delivering services to multi-tenant.

This deep dependency stack of cloud objects complicates the cloud security problem as the security of each object/layer depends on the security of the lower objects/layers. Furthermore, any breach to any cloud objects will impact the security of the whole cloud platform. Each cloud layer/object has a set of security requirements and vulnerabilities so it requires a set of security co ntrols to deliver secured service. This results in a huge number of security controls that needs to be managed. Moreover, managing such heterogeneous security controls to meet security needs is a complex task, taking into account conflicts among the security requirements and among security controls at each layer. This may result in an inconsistent security model. Hence, a unified security control management module is required. This module should coordinate and integrate among the various layers' security controls based on security needs

VI.Cloud computing stack holders and security implications

The cloud computing model has different stakeholders stack holders: cloud provider, service provider and the consumer. Each stack container has its own security management systems / processes and each has its own expectations and possibilities from / to other stack holders. This leads to a set of security on a service by different tenants contrary to any security configuration other.So of each service should be maintained and enforced at the service level instances and during implementation, taking into account the possibility of changing requirements based on current limiting consumers. every new risks And consumers to negotiate and agree on the applied security features. However, no standard security specification notations are available that can be used by the cloud containers stack to represent and reason about their offered / required safety features and every stake holder has its own security management processes used to determine their assets, expected risks and consequences, and how to minimize such risks. The adoption of cloud model results in the loss of control of both parties involved, including cloud providers (who are not aware of the content and securing services hosted on their infrastructure) and cloud consumers (who are unable not to check on their ability safety Noron other services with the same resources). Security SLA management frameworks represent a part of the solution with regard to the safety features specification, maintenance and control. However, SLAs not cover security in their specifications. Moreover, SLAs are contracts high level, where the details of the security and safeguards, and how to change during runtime are not included.

On the other side, cloud providers are not able to provide efficient and effective security because they are not aware of the architectures hosted services. Furthermore, cloud providers face many changes to security while having used a variety of security controls to be updated. This further complicates the tasks of the cloud providers' security administrators. Transparency of what security is enforced, what risks exist, and what violations occur on the cloud platform and hosted services must exist between cloud providers and consumers. This is what is called "trust but verify" where consumers must rely on their cloud providers meanwhile cloud providers must provide tools to help monitor the safety of law enforcement and monitor consumers

VII. CLOUD COMPUTING SERVICE DELIVERY MODELS AND SECURITY IMPLICATIONS

We summarize the key security issues/vulnerabilities in each service delivery model. Some of these issues are the responsibility of cloud providers while others are the responsibility of cloud consumers.

A. IaaS Issues

VM security – securing the VM operating systems and workloads from common security threats that affect traditional physical servers, such as malware and viruses, using traditional or cloud-oriented security solutions. The VM's security is the responsibility of cloud consumers. Each cloud consumer can use their own security controls based on their needs, expected risk level, and their own security management process.

Securing VM images repository - unlike physical servers VMs are still under risk even when they are offline. VM images can be compromised by injecting malicious codes in the VM file or even stole the VM file itself. Secured VM images repository is the responsibilities of the cloud providers. Another issue related to VM templates is that such templates may retain the original owner information which may be used by a new consumer.

Virtual network security - sharing of network infrastructure among different tenants within the same server (using v Switch) or in the physical networks will increase the possibility to exploit vulnerabilities in DNS servers, DHCP, IP protocol vulnerabilities, or even the v Switch software which result in network-based VM attacks.

Securing VM boundaries - VMs have virtual boundaries compared with to physical server ones. VMs that co-exist on the same physical server share the same CPU, Memory, I/O, NIC, and others (i.e. there is no physical isolation among VM resources). Securing VM boundaries is the responsibility of the cloud provider.

Hypervisor security - a hypervisor is the "virtualizer" that maps from physical resources to virtualized resources and vice versa. It is the main controller of any access to the physical server resources by VMs. Any compromise of the hypervisor violates the security of the VMs because all VMs operations become traced unencrypted. Hypervisor security is the responsibility of cloud providers and the service provider. In this case, the SP is the company that delivers the hypervisor software such as VMware or Xen.

B. PaaS Security Issues

SOA related security issues – the PaaS model is based on the Service-oriented Architecture (SOA) model. This leads to inheriting all security issues that exist in the SOA domain such as DOS attacks, Man-in-the-middle attacks, XML-related attacks, Replay attacks, Dictionary attacks, Injection attacks and input validation related attacks . Mutual authentication, authorization and WS-Security standards are important to secure the cloud provided services. This security issue is a shared responsibility among cloud providers, service providers and consumers.

API Security - PaaS may offer APIs that deliver management functions such as business functions, security functions, application management, etc. Such APIs should be provided with security controls and standards implemented, such as OAuth , to enforce consistent authentication and authorization on calls to such APIs. Moreover, there is a need for the isolation of APIs in memory. This issue is under the responsibility of the cloud service provider

C. SaaS Security Issues

In the SaaS model enforcing and maintaining security is a shared responsibility among the cloud providers and service providers (software vendors). The SaaS model inherits the security issues discussed in the previous two models as it is built on top of both of them including data security management (data locality, integrity, segregation, access, confidentiality, backups) and network security.

Web application vulnerability scanning - web applications to be hosted on the cloud infrastructure should be validated and scanned for vulnerabilities using web application scanners Such scanners should be up to date with the recently discovered vulnerabilities and attack paths maintained in the National Vulnerability Database (NVD) and the Common Weaknesses Enumeration (CWE) . Web application firewalls should be in place to mitigate existing/discovered vulnerabilities (examining HTTP requests and responses for applications specific vulnerabilities). The ten most critical web applications vulnerabilities in 2010 listed by OWASP are injection, cross site scripting (Input validation) weaknesses.

Web application security miss-configuration and breaking - web application security miss-configuration or weaknesses in application-specific security controls is an important issue in SaaS. Security miss-configuration is also very critical with multi-tenancy where each tenant has their own security configurations that may conflict with each other leading to security holes. It is mostly recommended to depend on cloud provider security controls to enforce and manage security in a consistent, dynamic and robust way.

D. Cloud Management Security Issues

The Cloud Management Layer (CML) is the "microkernel" that can be extended to incorporate and coordinate different components. The CML components include SLA management, service monitoring, billing, elasticity, IaaS, PaaS, SaaS services registry, and security management of the cloud. Such a layer is very critical since any vulnerability or any breach of this layer will result in an adversary having control, like an administrator, over the whole cloud platform. This layer offers a set of APIs and services to be used by client applications to integrate with the cloud platform. This means that the same security issues of the PaaS model apply to the CML layer as well.

E. Cloud Access Methods Security Issues

Cloud computing is based on exposing resources over the internet. These resources can be accessed through web browsers (HTTP/HTTPS), in case of web applications - SaaS; SOAP, REST and RPC Protocols, in case of web services and APIs – PaaS and CML APIs remote connections, VPN and FTP in case of VMs and storage services – IaaS. Security controls should target vulnerabilities related to these protocols to protect data transferred between the cloud platform and the consumers.

VIII. CLOUD COMPUTING SECURITY ENABLERS

A. Identity & Access Management (IAM) and Federation

Identity is a core of any security aware system. It allows the users, services, servers, clouds, and any other entities to be recognized by systems and other parties. Identity consists of a set of information associated with a specific entity. This information is relevant based on context. Identity should not disclose user personal information "privacy". Cloud platforms should deliver or support a robust and consistent Identity management system. This system should cover all cloud objects and cloud users with corresponding identity context information. It should include: Identity Provisioning and deprovisioning, identity information privacy, identity linking, identity mapping, identity federation, identity attributes federation, single sign on, authentication and authorization. Such system should adopt existing standards, *such as SPML, SAML, OAuth, and XACML*, to securely federate identities among interacting entities within different domains and cloud platforms.

B. Key Management

Confidentiality is one of key objectives of the cloud computing security (CIA triad). Encryption is the main solution to the confidentiality objective, for data, processes and communications. Encryption algorithms either symmetric keybased or asymmetric are key-based. Both encryption approaches have a major problem related to encryption key management i.e. how to securely generate, store, access and exchange secrete keys. Moreover, PaaS requires application keys for all APIs and service calls from other applications. The applications' keys must be maintained securely along with all other credentials required by the application to be able to access such APIs.

C. Security Management

Based on the huge number of cloud stakeholders, the deep dependency stack, and the large number of security controls to deliver security requirements, the cloud security management becomes a more complicated research problem. Security management needs to include security requirements and policies specifications, security controls configurations according to the policies specified, and feedback from the environment and security controls to the security management and the cloud stakeholders. Security management should function as a plug-in for CML

D. Secure Software Development Lifecycle

The secure software development lifecycle (SDLC with security engineering activities) includes elicitation of the security requirements, threat modeling, augmentation of security requirements to the systems models and the generated code consequently. The cloud based applications will involve revolution in the lifecycles and tools used to build secure systems. The PaaS provides a set of reusable security enabling components to help developing secured cloud-based applications. Also security engineering of the cloud-based application should change to meet new security requirements imposed on such systems. Applications should support adaptive security (avoiding hardcoded security) to be able to meet vast range of consumers' security requirements. Adaptive application security is based on externalizing/delegating the security enforcement and applications security management to the cloud security management, cloud security services and security controls.

E. Security-Performance tradeoff optimization

The cloud computing model is based on delivering services using SLAs. SLAs should cover objectives related to performance, reliability, and security. SLAs also define penalties that will be applied in case of SLA violation. Delivering high security level, *as one of SLA objectives*, means consuming much more resources that impact on the performance objective (the more adopted security tools and mechanism, the worst the impact on the performance of the underlying services). Cloud management should consider the trade-off between security and performance using utility functions for

security and performance (least security unless stated otherwise). Moreover, we should focus on delivering adaptive security where security controls configurations are based on the current and expected threat level and considering other tradeoffs.

F. Federation of security among multi-clouds

When a consumer uses applications that depend on services from different clouds, he will need to maintain his security requirements enforced on both clouds and in between. The same case when multiple clouds integrate together to deliver a bigger pool of resources or integrated services, their security requirements needs to be federated and enforced on different involved cloud platforms.

IX. CONCLUSION

The cloud computing model is one of the promising computing models for service providers, cloud providers and cloud consumers. Despite the potential benefits derived from the cloud computing, the security model is still the question of where the cloud model adoption.But to make best use of the model we have in the security blocks influences. Existing holes Based on the data explained above, we can summarize the cloud security problem as follows:

• Part of the security to be taken from the technologies such as virtualization and SOA.

• Multi-tenancy and isolation is an important dimension in the cloud security problem that a vertical solution from the SaaS layer to physical infrastructure (to develop physical borders among tenants alike instead of virtual boundaries currently used) is required.

• Safety management is very critical to monitor and manage the number of requirements and controls.

Based on this discussion, we recommend cloud computing security solutions must:

• a focus on the problem abstraction, using model-based approaches to different viewpoints safety record and link with these views in a holistic cloud security model.

• Inherent to the cloud architecture. Where supplied mechanisms (such as elasticity engines) and APIs to provide flexible security interfaces.

.• Support for: multi-tenancy where each user can see only hi security configurations, elasticity, to scale up and down based on the current context.

• Support integration and coordination with other security controls at different layers to deliver integrated security.

• Be adaptive to meet continuous environment changes and stakeholders needs.

X. FUTURE WORK

We are investigating in the cloud security management problem. Our objective is to block the hole arise in the security management processes of the cloud consumers and the cloud providers from adopting the cloud model. To be able to resolve such problem we need to Capture different stakeholders security requirements from different perspectives and different levels of details Map security requirements to the cloud architecture, security patterns and security enforcement mechanisms; and Deliver feedback about the current security status to the cloud providers and consumers. We propose to adopt an adaptive model-based approach in tackling the cloud security management problem. Models will help in the problem abstraction and the capturing of security requirements of different stakeholders at different levels of details. Adaptive-ness will help in delivering an integrated, dynamic and enforceable cloud security model. The feedback loop will measure the security status to help improving the current cloud security model and keeping cloud consumers aware with their assets security status (applying the trust but verify concept).

ACKNOWLEDGEMENT

First I am grateful to God for giving me a chance to complete thiswork. This work is supported by K.Sripath Roy (Assistant Professor), ECE department of KL University. I am thankful to him and KL Universityfor giving me continuous encouragement and great support.

REFERENCES

[1] NIST. October, (2010). *National Vulnerability Database (NVD)*.
Available: http://nvd.nist.gov/home.cfm.

[2] Microsoft. (2006, October, 2010). *Multi-Tenant Data Architecture*.
Available: http://msdn.microsoft.com/en-us/library/aa479086.aspx

[3] IDC, "IDC Ranking of issues of Cloud Computing model," ed, 2009, http://blogs.idc.com/ie/?p=210, Accessed on July 2010.

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

[5] S. Subashini, ,Kavitha, V., "A survey on security issues in service delivery models of cloud computing," *Journal of Network and Computer Applications*, vol. In Press, Corrected Proof. [6] Cloud Security Alliance (CSA). (2010). Available:http://www.cloudsecurityalliance.org/

[6] Balachandra Reddy Kandukuri, Ramakrishna Paturi and Atanu Rakshit, "Cloud Security Issues," in *Proceedings of the 2009 IEEE International Conference on Services Computing*, 2009, pp. 517-520.

[7] Kresimir Popovic , Zeljko Hocenski, "Cloud computing security issues and challenges," in *The Third International Conference on Advances in Human-oriented and Personalized Mechanisms, Technologies, and Services*, 2010, pp. 344-349.

[8] Meiko Jensen, Jörg Schwenk, Nils Gruschka and Luigi Lo Iacono, "On Technical Security Issues in Cloud Computing," in *IEEE ICCC*, Bangalore 2009, pp. 109-116.

[9] Bernd Grobauer, Tobias Walloschek and Elmar Stocker" Understanding Cloud-Computing Vulnerabilities," *IEEE Security and Privacy*, vol. 99, 2010.

[10] D. K. Holstein, , Stouffer, K., "Trust but Verify Critical Infrastructure