INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH & DEVELOPMENT

ISSN: 2278 – 0211 (Online)

Security Issues In Cloud Computing And Associated Mitigation Techniques

ParasYadav
Dronacharya College of Engineering, India
Purnendu Mishra
Dronacharya College of Engineering, India
Tarun Sharma
Dronacharya College of Engineering, India
Vishal Sharma
Dronacharya College of Engineering, India

Abstract:
Cloud computing is a new computational paradigm that offers an innovative business model fororganizations to adopt IT without upfront investment. It promises to provide a flexible IT architecture, accessible through internet from lightweight portable devices. This would allow multi-fold increase in the capacity and capabilities of the existing and new software. In a cloud computing environment, the entire data resides over a set of networked resources, enabling the data to be accessed through virtual machines. Despite the potential gains achieved from the cloud computing, the model security is still questionable which impacts the cloud model adoption.The security problem becomes more complicated under the cloud model as new dimensions have entered into the problem scope related to the model architecture, multi-tenancy, elasticity, and layers dependency stack. In this paper, we discussed security issues for cloud computing. We investigated the problem from the cloud architecture perspective, the cloud offered characteristics perspective, the cloud stakeholders' perspective, and the cloud service delivery and deployment model models perspective. Based on this analysis, weelaborate the numerous unresolved issues threatening the cloud computing adoption and diffusion affecting the various stake-holders associated with it.

Key words: *cloud computing; cloud computing security; cloud computing security management, Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS)*

1.Introduction

Internet has been a driving force towards the various technologies that have been developed since its inception. Cloud computing provides the next generation of internet-based, highly scalable distributed computing systems in which computational resources are offered 'as a service.

A visible mass of data floating in the network, typically present on the server. In information technology, a server is a computer program that provides services to other computer programs (and their users) in the same or other computers(basically a cloud). The discipline of computing is the systematic study of algorithmic processes that describe and transform formation: their theory, analysis, design, efficiency, implementation, and application (basicallya computing).

A plethora of definitions have been given explaining the cloud computing. The most widely used definition of the cloud computing model is introduced by NIST [1] as " a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. ".

Cloud computing is defined as a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage devices and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction [2] In such an environment users need not own the infrastructure for various computing services. In fact, they can be accessed from any computer in any part of the world. This integrates features supporting high scalability and multi-tenancy, offering enhanced flexibility in comparison to the earlier existing computing methodologies. It can deploy, allocate or reallocate resources dynamically with an ability to continuously monitor their performance [2]..

Multi-tenancy and elasticity are two key characteristics of the cloud model.MultiTenancy 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 advantages of using cloud computing include:

- Reduced hardware and maintenance cost,
- accessibility around the globe, and
- Flexibility and highly automated processeswherein the customer need not worry about mundane concerns like software up-gradation [3, 4].

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 [5] because:

• Enterprises outsource security management to a third party that hosts their IT assets (loss of control).

• 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.

• Hosting this set of valuable assets on publicly available infrastructure increases the probability of attacks

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. Our objective is to identify the weak points in the cloud model. We present a detailed analysis for each weakness to highlight their root causes. 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 2.0, we explore previous efforts in defining cloud security problems and challenges. Sections 3 explore the cloud computing security problem from different perspectives. Section 4.0 summarizes our conclusions and what we believe are the key dimensions that should be covered by any cloud security solution. Finally, in section 5.0.we discuss the future work focusing on one of the discussed security enablers (cloud security management).

2.Literature Review

Cloud computing security challenges and issues discussed various researchers. The Cloud Computing Use Cases group [6] discusses the different use case scenarios & related requirements that may exist in the cloud computing model. They consider use cases from different perspectives including customers, developers and security engineers. ENISA [7] investigated the different security risks related to adopting cloud computing alongwith the affected assets, the risks likelihood, impacts, and vulnerabilities in cloud computing that may lead to such risks. . Similar efforts discussed in" TopThreats to Cloud Computing" by CSA [8}Balachandra et al[9] discuss the security SLA's specifications and objectives related to data locations, segregation and data recovery. Kresimir et al [10] discuss high level security concern in the cloud computing model such as data integrity, payment, and privacy of sensitive information. Bernd et al [11] discussthe security vulnerabilities existing in the cloud platform. The authors grouped the possible vulnerabilities into technology -related, cloud characteristics -related, security controls- related. Subashini et al [12] discuss the security challenges of the world service delivery model, focusing on the SaaS model.

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 & delivery solutions.

3. Architecture& security

The Cloud Computing model has three service delivery models and main three deployment models [1] models are: 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 cloud are the most vulnerable deployment model because for public users to host their services who may be malicious users.

According to the differenttypes of services offered, cloud computing can be consideredto consist of three layers. Infrastructure as a Service (IaaS)isthe lowest layer that provides basic infrastructure supportservice. Platform as a Service (PaaS)layer is the middle layer,which offers platform oriented services, besides providing theenvironment for hosting user's applications. Software as a Service (SaaS)is the topmost layer which features a completeapplication offered as service on demand [13, 14].

SaaS ensures that complete applications are hosted on theinternet and users use them. The payment is made on a pay per-use model. It eliminates the need to install and run theapplication on the customer's local computer, thus alleviatingthe customer's burden for software maintenance. In SaaS,there is the Divided Cloud and Convergence coherencemechanism whereby every data item has either the "ReadLock" or "Write Lock" [15]. Two types of servers are used bySaaS: the Main Consistence Server (MCS) and DomainConsistence Server (DCS). Cache coherence is achieved bythe cooperation between MCS and DCS [16]. In SaaS, if theMCS is damaged, or compromised, the control over the cloudenvironment is lost. Hence securing the MCS is of greatimportance.

In the Platform as a Service approach (PaaS), the offeringalso includes a software execution environment. For example,there could be a PaaS application server that enables the lonedeveloper to deploy web-based applications without buyingactual servers and setting them up. PaaS model aims to protectdata, which is especially important in case of storage as aservice. In case of congestion, there is the problem of outagefrom a cloud environment. Thus the need for security againstoutage is important to ensure load balanced service. The dataneeds to be encrypted when hosted on a platform for securityreasons. Cloud computing architectures making use ofmultiple cryptographic techniques towards providingcryptographic cloud storage have been proposed in [17].

Infrastructure as a Service (IaaS)refers to the sharing ofhardware resources for executing services, typically usingvirtualization technology. Potentially, with IaaS approach,multiple users use available resources. The resources caneasily be scaled up depending on the demand from user andthey are typically charged on a pay-per-use basis [18]. Theyare all virtual machines, which need to be managed. Thus aGovernance framework is required to control the creation and Usage of virtual machines. This also helps to avoiduncontrolled access to user's sensitive information.

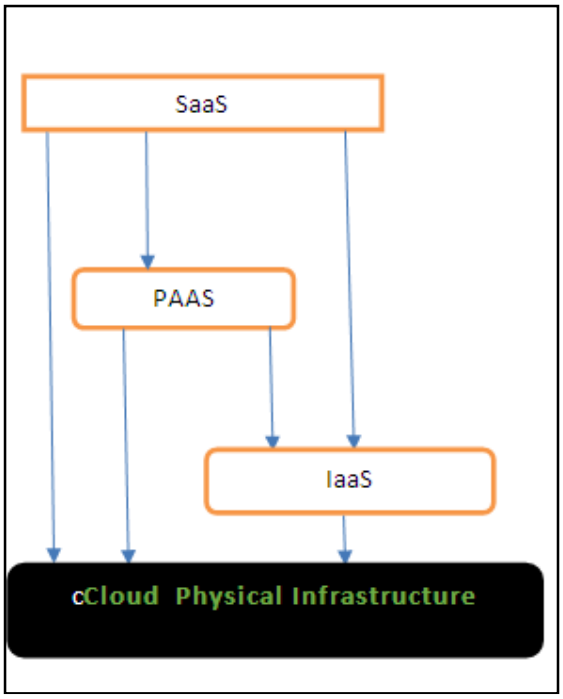

Figure 1

Each service delivery model has different possible implementations, as in figure 1, which complicates the development of standard security model for each service delivery model. Moreover, these service delivery models may exist in one cloud platform leading to further complication of the security management process.

3.Characterstics And Security

3.1.Implications

To achieve efficient utilization of resources, cloud providers need to increase their resource utilization while decreasing cost. At the same time consumers need to use resources as far as needed while being able to increase or decrease resources consumption based on actual demands. Cloud computing models provide Multi-tenancy and Elasticity to achieve efficient utilization of resources. . Both characteristics turn out to have serious implications on the cloud model security.

Multi-tenancy implies sharing of computational resources, storage, services, and applications with other tenants. Multi- tenancy has different realization approaches as shown in figure 2. In approach 1, each tenant has their own dedicated instance with their own customizations (customization may include special development to meet customer

needs).In approach 2, each tenant uses a dedicated instance, like approach 1, while all instances are the same but with different configurations (adjustment of application parameters or interfaces) .In approach 3, all tenants share the same instance with runtime configuration (the application is divided into core application component and extra components that are loaded based on the current tenant requests – similar to SalesForce.com).). In approach 4 tenants are directed to a load balancer that redirects tenants requests to a suitable instance based on current instances load.Approaches 3 and 4 are the most risky as tenants are coexisting on the same process in memory and hardware. This sharing of resources violates the confidentiality of tenants' IT assets which leads to the need for secure multi-tenancy. To deliver secure multi-tenancy there should be isolation among tenants' data (at rest, processing and transition) and location transparency where tenants have no knowledge or control over the specific location of their resources (may have high level control on data location such as country or region level), to avoid planned attacks that attempt to co-locate with the victim assets [19].]. In IaaS, isolation should consider VMs' storage, processing, memory, cache memories, and networks. In PaaS, isolation should cover isolation among running services and APIs' calls. In SaaS, isolation should isolate among transactions carried out on the same instances by different tenants and data.

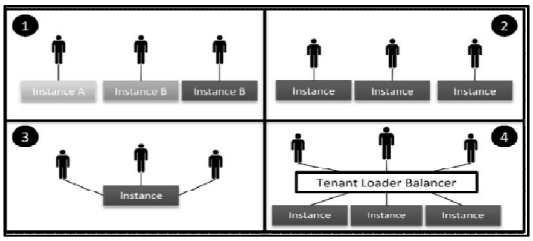

Figure 2

Elasticity implies being able to scale up or down resources assigned to services based on the current demand. Scaling up and down of tenant's resources gives the opportunity to other tenants to use the tenant previously assigned resources. This may lead to confidentiality issues. Moreover, Elasticity includes a service placement engine that maintains a list of the available resources from the provider's offered resources pool. This list is used to allocate resources to services. Such placement engines should incorporate cloud consumers' security and legal requirements such as avoid placing competitors services on the same server, data location should be within the tenants'

country boundaries. Placement engines may include a migration strategy where services are migrated from physical host to another or from cloud to another in order to meet demands and efficient utilization of the resources. This migration strategy should take into account the same security constraints. Furthermore, security requirements defined by service consumers should be migrated with the service and initiates a process to enforce security requirements on the new environment, as defined by cloud consumers, and updates the current cloud security model.

3.2.Cloud Computing'sdeep Dependenncies Stack

The cloud computing model depends on a deep stack of dependent layers of objects (VMs, APIs, 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 SaaSmodel covers applications and services offered as a service for end users, as shown in figure 3. The SaaSlayer 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 controls 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.

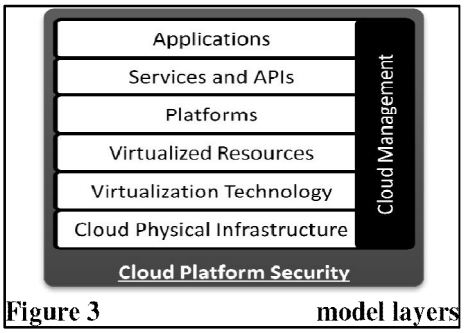

Figure 3

3.3.Stakeholders And Security Implications

The cloud computing model has different involved stakeholders: cloud provider (an entity that delivers infrastructures to the cloud consumers), service provider (an entity that uses the cloud infrastructure to deliver applications/services to end users), and service consumer (an entity that uses services hosted on the cloud infrastructure). Each stakeholder has their own security management systems/processes and each one has their own expectations (requirements) and capabilities (delivered) from/to other stakeholders. This leads to: (1) A set of security requirements defind on a service by different tenants that may conflict with each other. So security configurations of each service should be maintained and enforced on the service instances level and at runtime taking into account the possibility of changing requirements based on current consumers' needs to mitigate new risks; (2) Providers and consumers need to negotiate and agree on the applied security properties. However, no standard security specification notations are available that can be used by the cloud stakeholders to represent and reason about their offered/required security properties; and (3) Each stakeholder has their own security management processes used to define their assets, expected risks and their impacts, and how to mitigate such risks. Adopting cloud model results in losing control from both involved parties,includingcloud providers (who are not aware of the contents and security requirements of services hosted on their infrastructures) and cloud consumers (who are not able to control The cloud computing model has different involved stakeholders: cloud provider (an entity that delivers infrastructures to the cloud consumers), service provider (an entity that uses the cloud infrastructure to deliver applications/services to end users), and service consumer (an entity that uses services hosted on the cloud infrastructure). Each stakeholder has their own security management systems/processes and each one has their own expectations (requirements) and

capabilities (delivered) from/to other stakeholders. This leads to: (1) A set of security requirements defined on a service by different tenants that may conflict with each other. So security configurations of each service should be maintained and enforced on the service instances level and at runtime taking into account the possibility of changing requirements based on current consumers' needs to mitigate new risks; (2) Providers and consumers need to negotiate and agree on the applied security properties. However, no standard security specification notations are available that can be used by the cloud stakeholders to represent and reason about their offered/required security properties; and (3) Each stakeholder has their own security management processes used to define their assets, expected risks and their impacts, and how to mitigate such risks. Adopting cloud model results in losing control from both involved parties,includingcloud providers (who are not aware of the contents and security requirements of services hosted on their infrastructures) and cloud consumers (who are not able to control neither on their assets security nor on other services sharing the same resources). Security SLA management frameworks represent part of the solution related to security properties specification, enforcement and monitoring. However, SLAs still don't cover security attributes in their specifications [20]. Moreover, SLAs are high level contracts where the details of the security policies and security control and how to change at runtime are not included.

On the other side, cloud providers are not able to deliver efficient and effective security controls because they are not aware of the hosted services' architectures. Furthermore, cloud providers are faced with a lot of changes to security requirements while having a variety of security controls deployed that need to be updated. This further complicates the cloud providers' security administrators' tasks. Transparency of what security is enforced, what risks exist, and what breaches occur on the cloud platform and the hosted services must exist among cloud providers and consumers. This is what is called "trust but verify" [21], where cloud consumers should trust in their providers meanwhile cloud providers should deliver tools to help consumers to verify and monitor security enforcements.

3.3.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.

3.3.1.Security Issues In SaaS

Following key security element should be carefully considered as an Integral part of the SaaS deployment process:

Data Security, Network Security, Data locality, Data integrity, Data access, Data Segregation, Authorization and Authentication Data Confidentiality, Web Application security Data Breaches, Virtualization vulnerability, Availability, Backup, Identity Management on sign-on process

3.3.2.Security Issues In PaaS

- In PaaS, the provider might give some control to the people to build applications on top of the platform. But any security below the application level such as host and network intrusion prevention will still be in the scope of the provider.
- Applications sufficiently complex to leverage an Enterprise Service Bus (ESB) need to secure the ESB directly, leveraging a protocol such as Web Service (WS) Security (Oracle, 2009).The ability to segment ESBs is not available in PaaS environments. Metrics should be in place to assess the effectiveness of the application security programs.
- Hackers are likely to attack visible code, including but not limited to code running in user context. They are likely to attack the infrastructure and perform extensive black box testing. The vulnerabilities of cloud are not only associated with the web applications but also vulnerabilities associated with the machine-to-machine Service Oriented Architecture (SOA) applications.

3.3.3.Security Issues In IaaS

- Taking virtual machines, which contain critical applications and sensitive data, off premise to public and shared cloud environments creates security challenges for organizations that have relied on network perimeter defence as the main method to protect their data centre. It may also revoke compliance and breach security policies. OS Security issues also alive in IaaS . Following are the points which are considered in IaaS.[22]

3.3.4.Cloud Access Methods Security Issues

Cloud computing is based on exposing resources over the internet. These resources can be accessed through (1) web browsers (HTTP/HTTPS), in case of web applications - SaaS; (2) SOAP, REST and RPC Protocols, in case of web services and APIs – PaaS and CML APIs; (3) 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.

3.3.5.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.

3.5.Security Issues In The Cloud Deployment Models

Each of the three ways in which cloud services can be deployed has its own advantages and limitations. And from the security perspective, all the three have got certain areas that need to be addressed with a specific strategy to avoid them.

3.5.1. Security Issues In A Public Cloud

In a public cloud, there exist many customers on a shared platform and infrastructure security is provided by the service provider. A few of the key security issues in a public cloud include:

The three basic requirements of security: confidentiality, integrity and availability are required to protect data throughout its lifecycle. Data must be protected during the various stages of creation, sharing, archiving, processing etc. However, situations become more complicated in case of a public cloud where we do not have any control over the service provider's security practices [23].

In case of a public cloud, the same infrastructure is shared between multiple tenants and the chances of data leakage between these tenants are very high. However, most of the

service providers run a multitenant infrastructure. Proper investigations at the time of choosing the service provider must be done in order to avoid any such risk [23, 24].

In case a Cloud Service Provider uses a third party vendor to provide its cloud services, it should be ensured what service level agreements they have in between as well as what are the contingency plans in case of the breakdown of the third party system.

Proper SLAs defining the security requirements such as what level of encryption data should undergo, when it is sent over the internet and what are the penalties in case the service provider fails to do so.

Although data is stored outside the confines of the client organization in a public cloud, we cannot deny the possibility of an insider attack originating from service provider's end. Moving the data to a cloud computing environment expands the circle of insiders to the service provider's staff and subcontractors [25]. An access control policy based on the inputs from the client and provider to prevent insider attacks has been proposed in [26]. Policy enforcement implemented at the nodes and the data-centres can prevent a system administrator from carrying out any malicious action. The three major steps to achieve this are: defining a policy, propagating the policy by means of a secure policy propagation module and enforcing it through a policy enforcement module.

3.5.2.Security Issues In A Private Cloud

A private cloud model enables the customer to have total control over the network and provides the flexibility to the customer to implement any traditional network perimeter security practice. Although the security architecture is more reliable in a private cloud, yet there are issues/risks that need to be considered:

- Virtualization techniques are quite popular in private clouds. In such a scenario, risks to the hypervisor should be carefully analysed . There have been instances when a guest operating system has been able to run processes on other guest VMs or host. In a virtual environment it may happen that virtual machines are able to communicate with all the VMs including the ones who they are not supposed to. To ensure that they only communicate with the ones which they are supposed to, proper authentication and encryption techniques such as IPsec [IP level Security] etc. should be implemented [26].
- The host operating system should be free from any sort of malware threat and monitored to avoid any such risk . In addition, guest virtual machines should not be

able to communicate with the host operating system directly. There should be dedicated physical interfaces for communicating with the host.

- In a private cloud, users are facilitated with an option to be able to manage portions of the cloud, and access to the infrastructure is provided through a webinterface or an HTTP end point. There are two ways of implementing a web-interface, either by writing a whole application stack or by using a standard applicative stack, to develop the web interface using common languages such as Java, PHP, Python etc. As part of screening process, Eucalyptus web interface has been found to have a bug, allowing any user to perform internal port scanning or HTTP requests through the management node which he should not be allowed to do. In the nutshell, interfaces need to be properly developed and standard web application security techniques need to be deployed to protect the diverse HTTP requests being performed .
- While we talk of standard internet security, we also need to have a security policy in place to safeguard the system from the attacks originating within the organization. This vital point is missed out on most of the occasions, stress being mostly upon the internet security. Proper security guidelines across the various departments should exist and control should be implemented as per the requirements .

Thus we see that although private clouds are considered safer in comparison to public clouds, still they have multiple issues which if unattended may lead to major security loopholes as discussed earlier.

The hybrid cloud model is a combination of both public and private cloud and hence the security issues discussed with respect to both are applicable in case of hybrid cloud. A trust model of cloud security in terms of social security has been discussed in [103]. Social insecurity has been classified as multiple stakeholder problem, open space security problem and mission critical data handling problem. All these issues have been considered while proposing a cloud trust model also known as “Security Aware Cloud”. Two additional layers of trust: internal trust layer and contracted trust layer have been proposed to enhance security in a cloud computing environment

4.CONCLUSION

The cloud computing model is one of the promising computing models for service providers, cloud providers and cloud consumers. But to best utilize the model we need to

block the existing security holes. Based on the details explained above, we can summarize the cloud security problem as follows:

- Some of the security problems are inherited from the used technologies such as virtualization and SOA.
- Multi-tenancy and isolation is a major dimension in the cloud security problem that requires a vertical solution from the SaaS layer down to physical infrastructure (to develop physical alike boundaries among tenants instead of virtual boundaries currently applied).
- Security management is very critical to control and manage this number of requirements and controls.
- The cloud model should have a holistic security wrapper, as shown in figure 3, such that any access to any object of the cloud platform should pass through security components first.

Based on this discussion we recommend that cloud computing security solutions should:

- Focus on the problem abstraction, using model-based approaches to capture different security views and link such views in a holistic cloud security model.
- Inherent in the cloud architecture. Where delivered mechanisms (such as elasticity engines) and APIs should provide flexible security interfaces.
- Support for: multi-tenancy where each user can see only his 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.

5.Future Aspects

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: (1) Capture different stakeholders security requirements from different perspectives and different levels of details; (2) Map security requirements to the cloud architecture, security patterns and security enforcement mechanisms; and (3) 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.

6.Reference

1. Peter Mell, and Tim Grance, "The NIST Definition of Cloud Computing," 2009, http://www.wheresmyserver.co.nz/storage/media/faq-files/cloud- def-v15.pdf , Accessed April 2010.
2. Peter Mell, Timothy Grance, "The NIST Definition of Cloud Computing", Jan, 2011.http://docs.ismgcorp.com/files/external/Draft-SP-800-145_cloud-definition.pdf
3. R. Maggiani, Communication Consultant, SolariCommunication, "Cloud Computing is Changing Howwe Communicate", 2009 IEEE International ProfessionalConference, IPCC, pp. 1-4, Waikiki, HI, USA, July 19-22, 2009. ISBN: 978-1-4244-4357-4.
4. Harold C. Lin, ShivnathBabu, Jeffrey S. Chase, Sujay S.Parekh, "Automated Control in Cloud Computing:Opportunities and Challenges", Proc. of the 1st Workshop on Automated control for data centres andclouds, New York, NY, USA, pp. 13-18, 2009, ISBN:978-1-60558-585-7
5. IDC, "IDC Ranking of issues of Cloud Computing model," ed, 2009, http://blogs.idc.com/ie/?..
6. Cloud Computing Use Case Discussion Group, "Cloud Computing Use Cases Version 3.0," 2010.
7. ENISA, "Cloud computing: benefits, risks and recommendations for information security,"2009,http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing- risk-assessment ,
8. Cloud Security Alliance (CSA). Available:http://www.cloudsecurityalliance.org/
9. BalachandraReddy Kandukuri, Ramakrishna Paturi and AtanuRakshit, "Cloud Security Issues," in Proceedings of the 2009 IEEE International Conference on Services Computing , 2009, pp. 517-520.
10. KresimirPopovic , ZeljkoHocenski, "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
11. Bernd Grobauer, Tobias Walloschek and ElmarStöcker, "Understanding Cloud-Computing Vulnerabilities," IEEE Security and Privacy, vol. 99, 2010.

12. 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.
13. Meiko Jensen, JorgSchwenk, Nils Gruschka, Luigi LoIacon, “On technical Security Issues in CloudComputing”, Proc. of IEEE International Conference onCloud Computing (CLOUD-II, 2009), pp. 109-116,India, 2009.
14. B.P. Rimal, Choi Eunmi, I. Lumb, “A Taxonomy andSurvey of Cloud Computing Systems”, Intl. JointConference on INC, IMS and IDC, 2009, pp. 44-51,Seoul, Aug, 2009. DOI: 10.1109/NCM.2009.218
15. Gaoyun Chen, Jun Lu and Jian Huang, Zexu Wu,“SaaAS - The Mobile Agent based Service for CloudComputing in Internet Environment”, Sixth InternationalConference on Natural Computation, ICNC 2010, pp.2935-2939, IEEE, Yantai, Shandong,China, 2010. ISBN: 978-1-4244-5958-2.
16. SangeetaSen, RituparnaChaki, “Handling Write LockAssignment in Cloud Computing Environment”,Communications in Computer and Information Science,vol. 245, issue. 7, pp. 221-230, 2011. DOI: 10.1007/978-3-642-27245-5_27
17. SenyKamara, Kristin Lauter, “Cryptographic cloudstorage”, Lecture Notes in Computer Science, FinancialCryptography and Data Security, pp. 136-149, vol. 6054,2010.DOI: 10.1007/978-3-642-14992-4_13
18. S. Bhardwaj, L. Jain, and S. Jain, “Cloud computing: Astudy of infrastructure as a service (IAAS)”,International Journal of engineering and informationTechnology, 2(1):60–63, 2010.
19. Thomas Ristenpart, EranTromer, HovavShacham, Stefan Savage, "Hey,you, get off of my cloud: exploring information leakage in third-partycompute clouds," presented at the Proceedings of the 16th ACMconference on Computer and communications security, Chicago, Illinois,USA, 2009.
20. Amazon .October, 2010).Amazon EC2 SLA.Available: http://aws.amazon.com/ec2-sla/
21. [21]D. K. Holstein, , Stouffer, K., "Trust but Verify Critical Infrastructure Cyber Security Solutions," in HICSS 2010, pp. 1-8.

22. PankajArora,RubalChaudhryWadhawan, Er. Satinder Pal Ahuja ,on Cloud Computing Security Issues in Infrastructure as a Service, International Journal of Advanced Research in Computer Science and Software Engineering , 2012
23. A. Verma and S. Kaushal, "Cloud Computing Security Issues and Challenges: A Survey", Proceedings of Advances in Computing and Communications, Vol. 193, pp. 445-454, 2011.DOI: 10.1007/978-3-642-22726-4_46
24. P. Sharma, S. K. Sood, and S. Kaur, "Security Issues in Cloud Computing", Proceedings of High Performance Architecture and Grid Computing, Vol. 169, pp. 36-45, 2011.DOI: 10.1007/978-3-642-22577-2_5
25. Wayne Jansen, Timothy Grance, "NIST Guidelines on Security and Privacy in Public Cloud Computing", Draft Special Publication 800-144,2011. http://csrc.nist.gov/publications/drafts/800-144/Draft- SP-800-144_cloud-computing.pdf
26. SudharsanSundararajan, Hari Narayanan, VipinPavithran, KaladharVorungati, KrishnashreeAchuthan, "Preventing Insider attacks in the Cloud", Communications in Computer and Information Science, vol. 190, issue. 5, pp. 488-500, 2011.DOI: 10.1007/978-3-642-22709-7_48
27. Thomas W. Shinder, "Security Issues in Cloud Deployment models", TechNet Articles, Wiki, Microsoft, Aug, 2011.http://social.technet.microsoft.com/wiki/contents/articles/security-issues-in-cloud-deployment-models.aspx