Security Issues in Cloud Computing

Dr. A. Askarunisa
Professor and Head
Vickram College of Engineering,
Madurai, Tamilnadu, India

N.Ganesh
Sr.Lecturer
Vickram College of Engineering,
Madurai, Tamilnadu, India

A.Athiraja
Sr.Lecturer
Vickram College of Engineering,
Madurai, Tamilnadu, India

Venkatesh
Sr.Lecturer
Vickram College of Engineering,
Madurai, Tamilnadu, India.

Abstract - Cloud Computing offers a computing model for the organizations to implement the functions related to Information technology with lower Total Cost of Ownership and without investment. Cloud Computing opens door for multiple, unlimited venues from elastic computing to demand provisioning for dynamic storage and computing. Besides the gains of the cloud computing, the security and accessing the resources freely is a big problem which affects the cloud adoption. Security problem is related with the multi-tenancy, elasticity, architecture, layer dependency. This paper gives a detailed analysis about the problems related to the security of the cloud such as characteristic perspective, stakeholder perspective, architecture perspective, delivery model perspective. Also this paper analysis about challenges regarding the research by implementing cloud security solutions which secures the changing and dynamic model of the cloud. Based on these analysis a detailed derived specifications of the problem related to cloud security, key features must be covered by the proposed security solutions for the cloud computing.

Keywords: Cloud Computing, Cloud Security and Challenges, Cloud Security model.

I. INTRODUCTION

Cloud Computing [1] provides resources selected from the resource pool for computing and storage which is the next evolution of distributed computing. When comparing with existing process it is a simple way to access the data's and software's stored in the cloud and defines the way of leveraging the distributed model [4]. Cloud Computing is being used in academia, industry and adopted in business ranges from hosting highly computationally intensive applications to light weighted applications and services. Cloud Computing increases capabilities and reduces the IT cost which results is delivering of efficient services. As per the survey [2] cloud market of worth USD 68 billion will reach 148 billion in future. Tradeoff's deals with computing and resources of the cloud and there is an increase in attacks by the attacker's who are showing interest in attacking cloud surface by using vulnerabilities which are existing on the cloud computing. Besides the advantages of cloud such as getting revenues and benefits potentially, there are some issues which affects the pervasiveness and creditability of the cloud computing as shown in Figure 1. The issues other than mentioned in the Figure 1 are,

Multi-tenancy
SLA management
Portable Services
Securing Cloud

Management of Data securely

Vendor lock-in

are the some of the problems which are identified in implementing the cloud computing model. Between the cloud provider and consumer the security is the major problem that hampers the cloud computing model [3] adoption because of,

Loosing the control [13] – Third party who is managing the security without the knowledge of the persons who are accessing the data and from where those data's has been stored.

Multiple tenants [1, 2, 6] – Within the physical and logical medium different tenants are residing.

SLA [7] – Data risk and is unavailable when needed without the right SLA (Service Level Agreement).

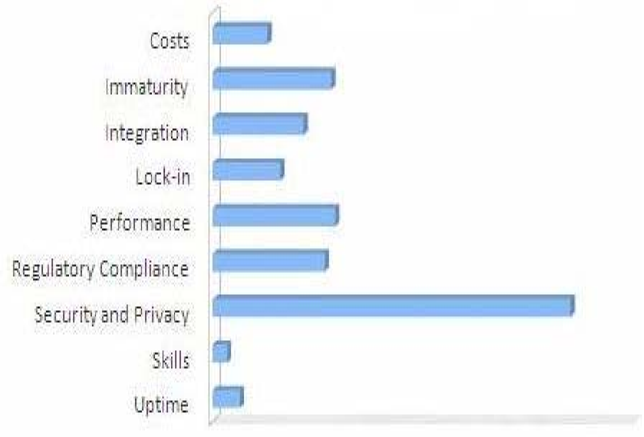


Figure 1 : Cloud computing Concerns

In this paper we analyze about the issues regarding the security in the models of cloud computing. Main objective is to identify different attack vectors, cloud model security issues pertinent. I propose root cause for the weakness in the cloud by a detailed analysis which helps the providers and consumers of the cloud to have an insight in knowing the issues on security of the cloud and how these issues are countered. In Section 2, I have shown the architecture for cloud computing security issues. In Section 3, I have shown the challenges regarding the research in the cloud security in cloud computing model and its implications. In Section 4, I have shown conclusions and the summary of the research. In Section 5, I have given the conclusion with future work and other steps which is to be taken.

II. Issues in the security of Cloud Computing

Cloud Computing contains three service delivery and deployment models as shown in Figure 2. The delivery model[1] are as follows:

Public Cloud: Cloud environment which is available to the cloud users for using the infrastructure by registering in the cloud.

Private Cloud: Cloud platform which is for specific organization.

Hybrid Cloud: Private Cloud which uses the resources of the Public Cloud.

Delivery [1, 2] models are as follows:

Software-as-a-Service (SaaS) : Cloud provider's give's applications to host and implement in cloud infrastructure.

Platform-as-a-Service (PaaS): Cloud provider's delivers platform, tools and business service to develop, deploy and managing the applications.

Infrastructure-as-a-Service (IaaS): Cloud provider delivers storage and network resource computation.

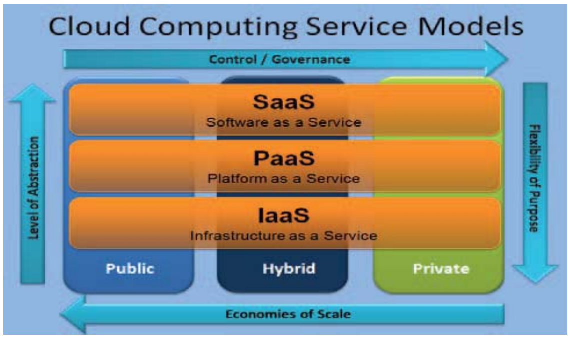


Figure 2: Services and Delivery – Deployment model of the Cloud

Different implementation is done on the service and delivery model of the cloud and it is Complex to develop a service and delivery model which is standard and it is an intangible process. These arguments have lead to the security issues addressed and possible mitigation for the cloud architecture threats which is covered in this paper.

The analysis of the cloud computing issues related to the security, makes the concentration to be done on the following key research area:

Information integrity and privacy
Elasticity
Secure Federation in Cloud
Multi-tenancy
Availability of information regarding Service Level Agreement (SLA)
Management of Secured information

A survey conducted by the International Data Corporation(IDC) which is represented in the following Figure 3 demonstrates the top concerns in the cloud security which is the issue faced by the organization and the difficulties in the merits of the Cloud, because it affects security of information and makes data and the processes in stake. Securing the Cloud is the responsibility which lies between the consumer of the cloud and the provider of the cloud where both of them must have trusted relationship and complement, when to secure information at rest and in transit [12].

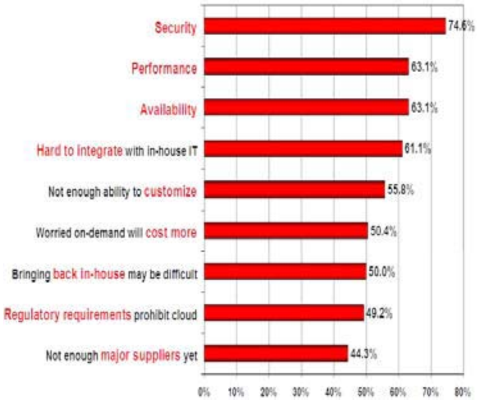


Figure 3: Issues in Cloud Computing

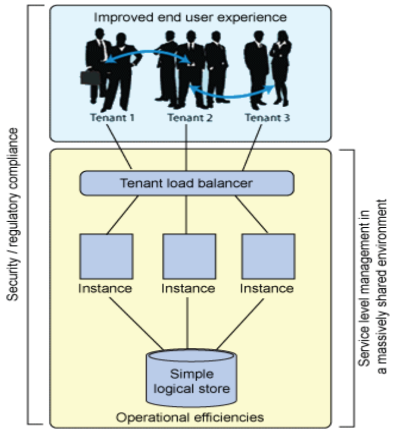
The next section deals with security implications in the cloud which is based on the issues discovered in this section.

III. IMPLICATIONS AND REMEDIATIONS IN THE SECURITY OF CLOUD

A Cloud is dynamic, shifting and complex because of various factors such as multi- threading, computing on demand, elastic computing, multi tenant atmosphere, storage on demand, virtualization requirement, multiprocessing and so on. Due to this restrictions and requirements, it is difficult to apply the security in correct time and in the correct places [5].

A] Multi-tenancy in Cloud

Cloud Computing is built for the shared memory, storage and access resources and for shared computing. Providers of Cloud will deploy multi tenancy as a standard to achieve the efficient utilization of resources with decreasing cost. Increase and decrease of resources is based on the consumer perspective on the real time basis. Cloud Computing meets these demands by two key characteristics such multi-tenancy and elasticity which has serious implications in the cloud security. Multi-tenancy deals with sharing of computational resources, services, storage and applications with other tenants who are residing on physical or logical platform within the provider's premises which is defined on the following Figure 4.


Improved end user experience
Tenant 1
Tenant 2
Tenant 3
Tenant load balancer
Instance
Instance
Instance
Simple logical store
Operational efficiencies
Security / regulatory compliance
Service level management in a massively shared environment

Database recovery by tenant source: IBM

Figure 4: Cloud Multi-tenancy model.

Multi-tenants share the same storage, database, computing, memory, physical or logical access in the cloud environment. Secure multi-tenancy is needed for the assets of the tenant's IT because of the occurrence of violations while sharing of resources [6]. Due to difficulties in analyzing the data which flows between different realms and insecure multi-tenancy model, an isolation between the tenants should be done. Isolation on tenant's data at rest and during the transition, physical location transparency where the tenants are not having knowledge and control over the location where the data and processes (resources) is resident is needed for delivering secure multi-tenancy which makes a way to avoid external and internal attacks that co-locates new malicious data with the assets of the victim's [10]. Isolations of processing, Virtual machine storage, access path network is considered in the IaaS environment. In PaaS environment isolation should cover the operating system level process, API and other running services. In SaaS environment isolation should be provided on the transactions carried out on the same instance of tenant's different data or the information. Isolation of data is done by the organization when they are porting their data and process to the cloud with the security policies and processes to make their data isolation with other tenants data. These processes may vary according to the data retention, rules for the classification of eligible data for sanitization and retention. Data and information should be ported by the organization with the providers of the cloud with mutual understanding which deals with the policies related to the security, control implementation.

B] Elasticity

Consumers can scale up or down their resources assigned to the services based on the demand according to the current situation by the Elasticity aspect which is in the cloud computing as shown in the Figure 5. Scaling up and down of tenant's resource to other tenant's makes the use of the previously assigned resources for the providers and it sometimes leads to the issues because of confidentiality. A tenants scale down and released resources are assigned to another tenants by the providers, may infer the contents of the tenants previous resources.

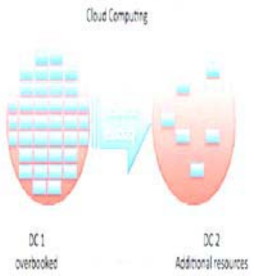


Figure 5: Resource elasticity in Cloud

Service placement engine in the cloud provides a list of resources available from the resource pool which achieves the elasticity in the cloud and these resources can be allocated to the tenants based on the demand. Elastic assignment of resources to the tenants leads to the security issues and the placement engines should incorporate the legal requirements, the security of the cloud consumer's to avoid the physical and logical server resources for the request of the competitors. Data location must be within the boundary of tenant's country. Migration strategy should be included in the placement engine when services are migrated from the physical or logical host to another or from the one cloud provider to another for the efficient resource utilization to meet the demands. Migration should be taken into the account for the security constraints.

C] Information Availability (SLA)

When the process is ported by the organization, services and applications to the cloud, a calculated risk is taken into account in terms of non availability of critical data or process or information due to the various factors. These factors ranges from the country's requirements for data storage in its physical entity to providers storage and resource computing goes offline due to the attack or break line.

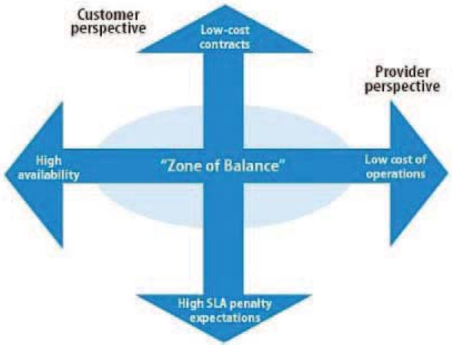


Figure 6: Service Level Agreement of the Cloud

SLA is a trust between the providers of the cloud and consumers and it defines the maximum time the applications (or) resources of the network may not be available to the consumer for use as shown in Figure 6. Maximum time varies between 98% - 99% for the providers [7]. This results in setting expectation by the consumer to have methods for remediation in place to mitigate any issues for non-availability. Mitigation of resource unavailability is to have backup plan to cover an event outage as well as local resources for most crucial information which in sync with secure channel by the cloud provider's. It makes enable to have all critical information by the consumer in off-hand and when needed, even when the resource provider is not available. Consumer must be provided to know about possible or imminent down time by the providers of the cloud.

D] Management of Secure Information

Cloud Management Layer (CML) can be used to incorporate and coordinate different components such as monitoring of service, billing, registry services, and management of security in the cloud. Any vulnerability or breach will results in malicious user ending up in the control having alike an administrator over the cloud platform. API's and services can be used in the integration of client's application and is done in the cloud platform for these layers. Management of Cloud Security is big problem according to the research with the increase in the cloud user base (tenants), stack dependency and large number of security controls for various security requirements delivery. Security requirements are included in the security management and policies which are derived from the organization's of tenants and reviewed to apply in the tenant's specific logical and physical environment and feedback from the environment to the security management and the base of the cloud consumer. Cloud provider must implement security standards realized in the industry [15] when there is a absence of central governing body for cloud security standards. Cloud provider helps consumer with same standards used in house hosting and to safeguard [14] assets of information.

E] Privacy and Integrity of Information

Resource exposure over the internet by the Cloud computing is used for the valid users and malicious attackers [12, 13]. Web browsers and remote connections, SOAP, REST, VPN, XML and RPC Protocols, APIs [8] are used to access the resources of the tenants. Organizations or Business must have trust with the cloud provider when it ports its information in the cloud. Poor cloud infrastructure leads to the design or security architecture [13] flaws in a nutshell and there are various issues which comes with the integrity and confidentiality of the resident information in the environment's of cloud provider. Some of the authentication and privacy issues are

- Absence of authentication, accounting protocols and authorization.
- Key for encryption and decryption is not managed.

Specific issues like mutual trust between the consumer and provider of the cloud is not convenient. Authentication should be done properly, providing Cloud Services by the provider to the consumer with accounting details, such that any attempt of information access is done by multilevel checking and ensures only the tenants who are authorized can have the rights for accessing the information. The Information access should be individual by the credentials, access secured mechanism which ranges from RSA certificate to secure shell (SSH) tunnel based. A key management augments have secure access to the data, and knows about the key availability either with the consumer or provider for the purpose of encryption and decryption Mutual understanding between the cloud provider and organization is done for porting the information/data.

F] Federation for Secure Cloud

Security requirements must be enforced among the clouds when the consumer leverages information's and applications that depends upon the services from different clouds. This produces several issues when there is an integration of multiple clouds to deliver services or bigger pool of resources and the requirement of security must be federated and enforced on logically and physically on various cloud platforms like SaaS, IaaS or PaaS.

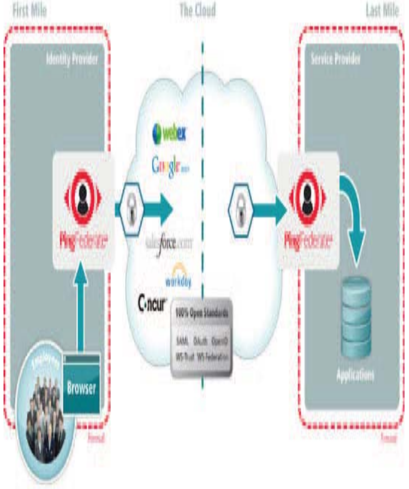


Figure 7: Secure Federation of Cloud with SSO [9]

Identifying user [14] is the main component in any system for the security and it allows the valid and legit – users, servers, services, cloud and other entities which is to be recognized by different systems. An identity contains specific entity composed of set of information like attributed federation and its identity, leveraging identity attributes federation, single sign on (SSO) [9]; authorization and authentication helps in security issued related with federation as shown in Figure 7. Providers of Cloud must adopt standards such as OAuth, XACML, SAML to secure, federate identities among entries identity within different cloud platforms and domains. This ensures application and user data are portable across the cloud and do not present gaps in the security between two or more providers because they adopt and work on same standards.

IV. Conclusion

Facets of cloud may be good or bad and has vibrant, morphing and virtualized milieu [1, 2]. Merits include flexibility for adoption of resources or reduction, pay as you go model, upfront investment and Total cost of ownership and other issues for the organization for prohibiting cloud adoption, information security when ported to the cloud. In this paper the concentration is done on the critical security issues among the other numerous security implications relevant to the cloud model. In this paper the research is based on the security of information/data in cloud computing [1, 2]. I have analyzed the existing issues in cloud model's available today due to integrity loss and confidentiality, elasticity, unsecure management, SLA issues and implications on the federation of cloud. Providers and consumers are incoherence of these issues which leads to the misconception of consumers. For Cloud Consumers and Service Providers, computing model of the cloud is the most promising one. For better utilization of these models, a block is implemented for the security issues which are existing and addressing the security implications/concerns. Cloud Security issues can be summarized as follows:

A. From various technologies security implications are inherited which forms the cloud basis such as virtualization.
B. Maximum attention is implemented on multi tenancy to curb any attacks on the users who are the victims and from malicious users. Isolation of tenant is the major issue in the security problem of the cloud.
C. Control on the management of Cloud security is very critical and the data's faced by the user, provider's infrastructure function either physical or logical is very critical.
D. Holistic security wrapper is on the cloud model as shown in Figure 8, and there is a multilayer security solution for accessing an object on the cloud platform.

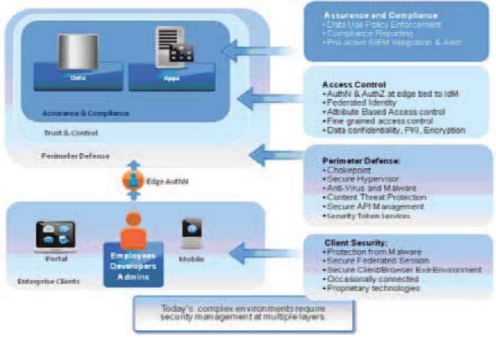

Assurance and Compliance
•Data Use Policy Enforcement
•Compliance Reporting
•Pro-active SIEM integration & Alert
Data
Apps
Assurance & Compliance
Trust & Control
Perimeter Defense
Access Control
•AuthN & AuthZ at edge tied to IdM
•Federated Identity
•Attribute Based Access control
•Fine grained access control
•Data confidentiality, PKI, Encryption
Edge AuthN
Perimeter Defense:
•Chokepoint
•Secure Hypervisor
•Anti-Virus and Malware
•Content Threat Protection
•Secure API Management
•Security Token Services
Portal
Employees
Developers
Admins
Mobile
Enterprise Clients
Client Security:
•Protection from Malware
•Secure Federated Session
•Secure Client/Browser Exe Environment
•Occasionally connected
•Proprietary technologies
Today's complex environments require security management at multiple layers.

Figure 8: Cloud Security Wrapper (Defense in Depth) [13]

Cloud computing security solutions should incorporate the following solution to ensure that the provider, consumer/tenant is assured of its data privacy [15] and integrity:

A. Security interfaces are provided by the mechanisms such as CML and cloud APIs, elasticity engine which is based on the industry encryption and authentication norms.
B. A tenant can see its security and information configurations, data and supporting isolation with multi-tenancy. Logical VM and hypervisor level segregation is carried, and the tenant can access the resource with the elasticity, scale up and down based on the current context for releasing resources to providers pool with privilege of sanitizing the data.
C. Coordination of security policy based on tenant's organization and integration is supported by the providers at different layers to deliver integrated security.

D. For the continuous environmental changes, the providers must be adaptive and ensure to construct security cloud.

V. FUTURE WORK

Various Cloud security issues must be investigated and mitigations can be ported from IaaS to PaaS and to SaaS and private to public and to hybrid cloud models. Collection of various stakeholders data like vendors, providers and consumers and models of the cloud with their merits and restrictions and can be adapted to security issue mitigation technique.

REFERENCES

[1] Cloud Computing – A Practical Approach by Velte, Tata McGraw-Hill Edition (ISBN-13; 978-0-07- 068351-8).

[2] Cloud Computing Bible – by Barrie Sosinsky, Wiley Publishing Inc. (ISBN-13; 978-0470903568)

[3] ENISA, "Cloud computing: benefits, risks and recommendations for information security". www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport/

[4] Cloud Security Alliance (CSA) http://www.cloudsecurityalliance.org/

[5] Bernd Grobauer, Tobias Walloschek and Elmar Stocker, "Understanding Cloud-Computing vulnerabilities," IEEE Security and Privacy, vol. 99.

[6] Microsoft – Multi – Tenant Data Architecture. http://msdn.microsoft.com/en-us/library/aa4709086.

[7] Amazon EC2 SLA. http://aws.amazon.com/ec2-sla/

[8] Z. Wenjun, "Integrated Security Framework for Secure Web Services," in IITSI 2010, pp. 178-183.

[9] Cloud Single Sign-On & Federated Identity, https://www.pingidentity.com/resource-center/SSO-and-Federated-identity.cfm

[10] Users Demand More From Cloud Providers, http://meship.com/Blog/2011/01/18/users-demand-more-from-cloud-providers

[11] It's time to revamp your Defense-in-Depth strategy, http://blogs.mcafee.com/enterprise/data-protection/its-time-to-revamp-your-Defense-in-depth-strategy.

[12] Data Integrity and Availability http://www.mitre.org/work/areas/research/2011iebriefings/05MSR160-JA.pdf.

[13] Research paper – "Security Issues and Solutions in Cloud Computing" http://wolfhalton.info/2010/06/25/security-and-solutions-in-cloud-computing/ISACA (auditor's perspective Journal)

[14] Trusted client to cloud access article http://soaexpressway.wordpress.com/2011/03/01/ trusted-client-to-cloud-access/

[15] IT Regulatory Compliance Programs http://www.systemexperts.com/compliance-programs.html