SECURITY ISSUES IN CLOUD COMPUTING SERVICE MODEL

Mrs. Neeraj Sharma

Department of Computer Science, Punjab Technical University (India)

ABSTRACT

Cloud Computing provides a very flexible way to allocate valuable resources within a shared network, bandwidth, software's and hardware's in a cost effective manner and limited service provider dealings (The NIST Definition of Cloud Computing).Many people carry their portable devices when not on their desk and they can easily access their documents, media and pictures on cloud storage via the Internet. It is very easy to set up and decommission server instances in cloud computing. Using this cloud computing technology consumers can get benefit in the form of on-demand self services , cost saving and can access broad network and boosting their infrastructure resources with reduced capital expenses but as everything come with some drawback this also put the business world into a more risky environment. As user used to put their private data on cloud and expects that data is in the secured condition, second main concern is about loss of control over certain sensitive data. From above situation we can say security and data integrity are the very important aspect in cloud computing which has to be taken in deep considerations. In this paper, we will discuss present security issue in cloud computing service model IaaS,PaaS,SaaS and purposed a solution for these issues.

Keywords: Cloud Computing, Security Issues In Service Model, Solution For Security And Privacy Issue

I. INTRODUCTION

Despite the many benefits, cloud computing produces many open security issues which are the main reason for slowing down its acceptance even the leading and famous cloud providers such as Amazon, Google etc are facing many security related challenges and are yet working to stabilize them. Finding a complete solution for all the security, integrity related issues are still a very big task. In this present work we discuss different security issues with enterprise and the associated challenges in the cloud service delivery models and organized this paper in 3 section where Section 2 will describes the common security issues that are due to cloud service delivery models (SaaA,PaaS,IaaS) ,section 3 will cover the solutions for security related challenges and Section 4 provides conclusions derived out from this survey.

II. PRESENT SECURITY ISSUE IN CLOUD COMPUTING SERVICE MODELS

2.1 Software as a Service (SaaS)

Software as a Service is a software distribution model. In which application are hosted by vendor or service provider and delivered to multiple clients on demand via a client browser over the Internet. Typical examples are Google Docs and Salesforce.com .The cloud provider replicate the data of various enterprise at multiple locations across world for maintaining high availability. In business world there is a great deal of discomfort

with the lack of control over data and knowledge of how enterprise data is being stored and either it's secured or not. In Fig 2 we illustrated the layered stack for a typical SaaS vendor and all the aspects that must be covered in designing and developing, deployment process in order to ensure security of the data. Following are the key points:

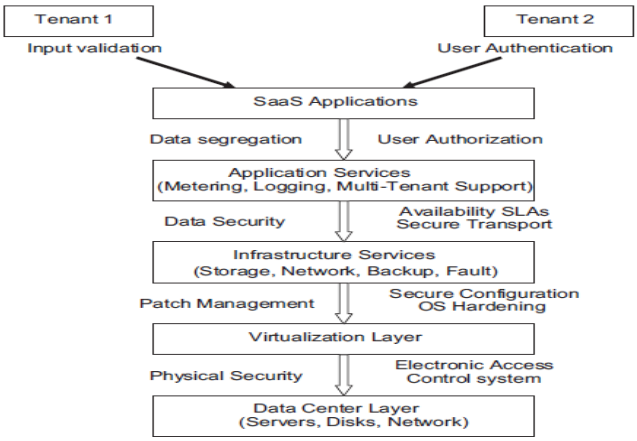

Fig. 2 Structure of SaaS Stack

2.1.1 Data Security

In the SaaS model, the data is stored outside the enterprise location, at the SaaS vendor end. That's why, the SaaS vendor must adopt some security checks point to ensure data security and prevention due to various security vulnerabilities. For that good encryption techniques and fine authorization technique to control access to data can be to use. In cloud vendors like Amazon, the Elastic Compute Cloud (EC2) administrators even not any have access to the customer instances and they cannot even log as Guest .In EC2 administrators is required to use their own cryptographically strong Secure Shell (SSH) keys to gain any access to a host. All users need to encrypt their data before it is uploaded to Amazon S3, so that they are not accessed or tampered by any unauthorized party. Malicious users always seeking for knowing the weakness in security system to gain access over unauthorized data

Counter Measure:-By performing below assessments test we can validate the security of the enterprise data stored at the SaaS vendor: Insecure Configration, Cookie Manipulation, OS and Cross-site scripting, SQL injection flaws, Cross-site request forgery, Access control weaknesses,Hidden manipulation and Insecure storage. If any type of vulnerability detected during these test, it can lead to gain access to sensitive data and which may lead to big loss.

2.1.2 Network Security

In SaaS deployment model, sensitive data of enterprises is processed by the SaaS application and stored at the SaaS vendor environment. Then data transfer over the network needs to be secured in order to prevent leakage of any type of sensitive information. For that we need some strong network encryption techniques for Transport Layer Security and Secure Socket Layer (SSL) for security. In Amazon for network security SSL encrypted endpoints use which are accessible from both the side, Internet and within Amazon EC2, which ensuring that data is safely transferred. But we need to aware from malicious users

Counter Measure: Performing below assessments test we can validate the network security of the SaaS vendor by Proper Session management, Network penetration and Packet data analysis, Insecure SSL trust configration.

If find any vulnerability performing these tests we need to review the security measure as malicious user can hijack active sessions, can gain access to user sensitive data.

2.1.3 Data Locality/Physical Security

In a SaaS model the consumers use the applications which are provided by the SaaS vender and process their business data online. Without knowing where the data actually stored, Regulations like the Federal Information Security Management Act (FISMA) says customers need to keep sensitive data within the country, but cloud vendors often not give any such guarantee. In some highly virtualized systems, data and virtual machines can move dynamically from one country to another in order to load balancing needs and for some other factors. E.g. like in Google if a user live in California goes on a business trip to London, it's better for that user's data to be served up by a data center in Europe. The typical SaaS vendors have held the view that it doesn't matter where the servers are, he continues. "We understand your laws, but the Internet doesn't work that way." Symantec, which has data centers in 14 countries, even not offer an in-country guarantee. But if data stays within a country, customers should be able to verify the data's location in order to meet regulatory requirements.

Counter measure: For this some integration requires between EMC, VMware and Intel products to find actual location of data. As right now, there's nothing that help to verifiability of where a virtual machine lives .There's nothing stopping you from moving a VM from one place in the world to somewhere else, and more importantly, there's no way to audit that at any sort of scale."

2.1.4 Data Integrity

In Cloud computing the problem of the data integrity is a big issue, as there are mix of on-premise and SaaS multi-tenant applications hosted by third party. SaaS applications expose their functionality by XML based Application Program Interfaces (APIs). But the biggest challenges is with web services at the protocol level, as Hyper Text Transfer Protocol (HTTP) does not give any guarantee of delivery, so the only option is to implement these at the API level as any lack of control over integrity lead to big problems.

Counter Measure: One method to deal with is all the transactions must be handled carefully in safe manner. Another method is to use hash value as hash value is derived by condensing a set of data into a single unique value by way of a pre-defined algorithm.

2.1.5 Data Segregation

As Multi-tenancy are the major characteristics of CC's, which helps multiple users to store their data using the applications provided by SaaS. Although, data of many users will reside at the same location which may lead to intrusion of data of one user by another user becomes possible. This can be done by injecting client code into the SaaS system. If the application executes this code without any verification, it leads to problem.

Counter Measure: The following are the assessments test to validate the data segregation is Data validation check, inserting SQL injection flaws and insecure storage check. If any vulnerability detected while performing these test, it can be exploited to gain access to sensitive enterprise data of other tenants. Some security policies must be follow by the cloud provider to avoid intrusion of data from unauthorized users The SaaS model must be able to provide boundary within the cloud not only at the physical level but also at the application as multiple enterprise deploying their business processes within a single cloud environment.

2.2 Infrastructure as a Service (IaaS)

In an IaaS model, a third-party provider hosts hardware, software, servers, storage and other infrastructure components on behalf of its clients and host users applications and handle tasks including system maintenance, backup and resiliency planning and offer highly scalable resources that can be adjusted on-demand. In IaaS customers pay- as-use basis, which eliminates the capital expense of deploying in-house hardware and software's example of these are Amazon Web Services (AWS), Windows Azure, Google Compute Engine, Rackspace Open Cloud, and IBM Smart Cloud Enterprise.

Security issues in Infrastructure-as-a-service IaaS

2.2.1 Platform Virtualization

In IaaS model of CC's the resources are shared and rented to the different customers. One single physical machine can be shared by many of different customers. Thus if virtualization become weak and it can easily lead to major attacked.

Counter measure: We propose a solution for this type of problem which is Virtualization-Aware Security Solution, which will help to examine volatile memory to detect and prevent kernel data rootkits also some new control objective for virtualization management are needs for more data protection and so that Virtual machines will help to managed and control all the information from internal and external threats.

2.2.2 Denial of Service (DoS)

DoS attacks in virtual environment are a critical threats .This type of attack is mainly happens when a great amount of non-sense requests sended and system start working against these requests due to that system consume all recourses and not able to supply any service to another users. However, Hypervisors is there to prevent VM from gaining 100% usage of any shared hardware resources, like CPU, RAM, network bandwidth.

Counter measure: For this type of attack we need appropriate hypervisor's configuration which detect extreme resource consumption, filter the malicious requests either by installing firewall or provide some solution for this of type issue and inform the administrator.

2.2.3 Networks & Internet Connectivity

In order to maintain availability and performance of cloud infrastructure multiple geographical sites use to reduce the load. Each of these site connected locally as local area network also connected with the other sites by high speed Internet. These sites compose the whole cloud infrastructure Thus, Cloud can use better conventional of vulnerabilities of Internet and computer networks.

Counter Measure: IaaS model is vulnerable to IP Spoofing, DDOS, MITM, and Port Scanning. For that some traffic encryption technique require to access the resources on the clouds, as VPNs use Layer 2 Tunneling Protocol (L2TP) and Point-to-Point Transfer Protocol (PPTP) and the WSSecurity help to maintain a secure context over a multi-point message but WS-Security need all the entities within the cloud to support the web services and for communicate using SOAP messages.

2.2.4 Network Monitoring

In IaaS model network monitoring is done by some site which are able to notify the events to selected users or groups and also use some technique to fix network problems automatically Eg MapCenter and NetSaint, in

NetSaint, the INFN-Testbed use, but more research need to show more feasibility and performance of cloud environment.

2.3 Platform as a Service (PaaS)

In a PaaS provider hosts the hardware and software on its own infrastructure and make users free from any type of installation typical examples are Google App Engine Mendix, Amazon Web Services (AWS) Elastic Beanstalk, Google App Engine and Heroku.

Security issues in Platform-as-a-service (PaaS)

2.3.1 Third-Party Relationships

As PaaS provide third-party web services components such as mashups . Mashups[9] is which combine more than one source element into a one single integrated unit. Thus, PaaS models also inherit some security issues related to mashups such as data and network security Also, in PaaS users have to depend on both the security of web-hosted development tools and third-party services.

Counter measure: In internet many web services available which providing QoS (Quality of Service). Therefore services mashup have to search for an optimal set of services to construct a composite service [6]

2.3.2 Underlying Infrastructure Security

In PaaS model, developers do not have any access to the underlying layers, so service providers are responsible for security infrastructure as well as for the applications services.

2.3.3 Development Life Cycle

Software Development Life Cycle (SDLC) is main and difficult phase of any application development .In which all the future issue related to security and privacy should examine carefully, if at single step of security measure fail to discuss, application can easily hack also SDLC should be design in such a way that any type of updation have no any effect on Data loss, Deletion, Security and Privacy

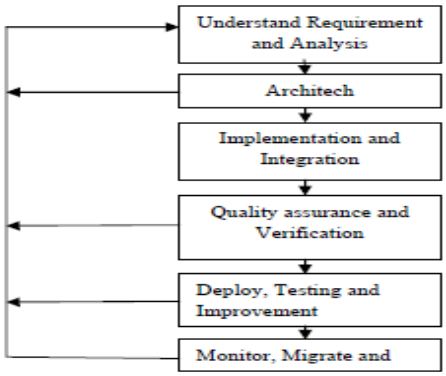

Fig 2: Cloud Development Life Cycle

In conclusion, we can say there is less material in the literature about security issues in PaaS rather than reality

III. PURPOSED SOLUTION FOR SECURITY AND PRIVACY ISSUE

In order to provide high security and privacy of enterprise data, some areas should be reconsidered. These areas are Governance Domains and Operational Domains [5]. As Governance domains deal with all strategic and

policy issues in Cloud environment, whereas the operational domains addresses to all different type of security concerns and there right implementation

3.1 Governance Domains

3.1.1Governance and Enterprise Risk Management

A good risk management system is need to redesign which deal with issues like legal precedence for agreement, ability of different organizations to adequately assess risk of a cloud provider and it should be responsible to protect and handle sensitive data and all aspect related to international boundaries should cover in this.

3.1.2 Legal Formality

Some process need to assign which deal with the legal issues when enterprises adopt Cloud Computing eg like protection of information and computer systems, security breach disclosure laws, regulatory requirements, privacy requirements, international laws etc.

3.1.3 Information Lifecycle Management

Information lifecycle management need to introduced which deal with issue like where data resides in the cloud and how to control the data also which and what type of compensations need to controls the loss of physical control, and who will responsible for data confidentiality, integrity and availability.

3.1.4 Service Level Agreement (SLA)

As cloud user have no control over the underlying computing resources, which means when consumers have migrated their core business to entrusted cloud provider no any surety about Quality, performance, availability are provided. In other words, it is vital for consumers to obtain guarantees from providers. This can provided through Service Level Agreements.SLA can negotiate between the providers and consumers.SLA specifications must be redefine in such a way that has an appropriate level of granularity, between expressiveness and complicatedness, so that they can cover most of the consumer expectations .For different cloud offerings (IaaS, PaaS, SaaS) we need to define different SLA specifications. For that advanced SLA mechanisms need to constantly incorporate user feedback and customization features into the SLA evaluation framework.[4]

3.2 Operational Domains Consist of

3.2.1Data Center Operations

Detailed study need to discuss on the provider's data center and its architecture, In order to make it stable for long terms.

The entire item should be discuses in detailed at provider side and user levels to ensure proper incident handling and forensics.

3.2.2 Application Security

We also need to guide all the client about how to secure the application software, and Client should know in detail how cloud work ,how to move from one cloud to another cloud ,which they should to adopted and what are their benefits.

3.2.3 Encryption and Key Management

A proper encryption key and scalable key management should used in all level both for protecting access to resources as well as for protecting data in cloud from leakage and unauthorized access.

3.2.4 Identity and Access Management

It discusses the management of identities and leveraging directory services to provide access all the control and also takes into account the assessment of an enterprise's readiness to conduct cloud based Identity and Access Management (IAM).

3.2.5 Fragmentation Redundancy Scattering Technique for Data Leakage

Using this technique we can secure the storage and intrusion tolerance, this technique first breaking down sensitive data into irrelevant different fragments, so that any fragment does not have any significant information by itself. Then, these fragments are transfer across different sites of the distributed system to protect data from leakage.

3.2.6 Digital Signatures

Use of digital signatures can also protect data from any type of unwanted access when data being transferred from one place to another, this always work with RSA algorithm to as RSA is the most recognizable algorithm .

3.2.7 Web Application Scanners

we can scans the web applications through web scanner in front-end to identify security vulnerabilities. This may also help to routes all web traffic through the web application firewall which inspects specific threats.

3.2.8 Protection Aegis for Live Migration of VMs ,VNSS

A secure live migration framework is needed which preserves integrity and privacy protection during and after migration of data from any type of threat and provide more security framework with customizes security policies for each virtual machine.

***3.2.9* Virtual Network Security**

[8] Presents a virtual network framework that secures the communication among virtual machines. This framework is based on Xen which offers two configuration modes for virtual networks: "bridged" and "routed". The virtual network model is composed of three layers: routing layers, firewall, and shared networks, which can prevent VMs from sniffing and spoofing. An evaluation of this approach was not performed when this publication was published.

Furthermore, web services are the largest implementation technology in cloud environments. However, web services also lead to several challenges that need to be addressed. Security web services standards describe how to secure communication between applications through integrity, confidentiality, authentication and authorization. There are several security standard specifications [6] such as Security Assertion Markup Language (SAML), WS-Security, Extensible Access Control Markup (XACML), XML Digital Signature, XML Encryption, Key Management Specification (XKMS), WS-Federation, WS-Secure Conversation, WS-Security Policy and WS-Trust. The NIST Cloud Computing Standards Roadmap Working Group has gathered high level standards that are relevant for Cloud Computing.

IV. CONCLUSION

In this paper security considerations in cloud computing services model SaaA,PaaS,IaaS are highlighted . As we Know, the threats in CC's are numerous, and each of them requires an in-depth analysis in last we purposed a solution for various issue we faced in cloud computing like governance and risk management to monitor the cloud protection in terms of information and security breach disclosure laws, regulatory requirements, privacy requirements, international laws, and FRS technique for secure storage, digital signature to protect data. There is no doubt that CC's has the potential to become a frontrunner in promoting a secure, virtual and economically viable IT solution in the future. For that new security techniques are needed as well as redesigned traditional solutions that can work with cloud architectures.

REFERENCES

[1.] Cloud Security Alliance (2011) Security guidance for critical areas of focus in Cloud Computing V3.0. Available: https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf
[2.] https://cloudsecurityalliance.org/wp-content/uploads/.../Domain-2.doc
[3.] C. Weinhardt, A. Anandasivam, B. Blau, and J. Stosser. "Business Models in the Service
[4.] World." IT Professional, vol. 11, pp. 28-33, 2009.
[5.] S. Ramgovind, M. M. Eloff, E. Smith. "The Management of Security in Cloud Computing" In
[6.] PROC 2010 IEEE International Conference on Cloud Computing 2010.
[7.] Wu H, Ding Y, Winer C, Yao L (2010) Network Security for virtual machine in Cloud Computing,IEEE Computer Society Washington. pp 18-21
[8.] http://www.hadmernok.hu/2012_1_kovacsz.pdf
[9.] Xu K, Zhang X, Song M, Song J (2009) Mobile Mashup: MASS'09. Washington, DC, USA: IEEE Computer Society. pp 1