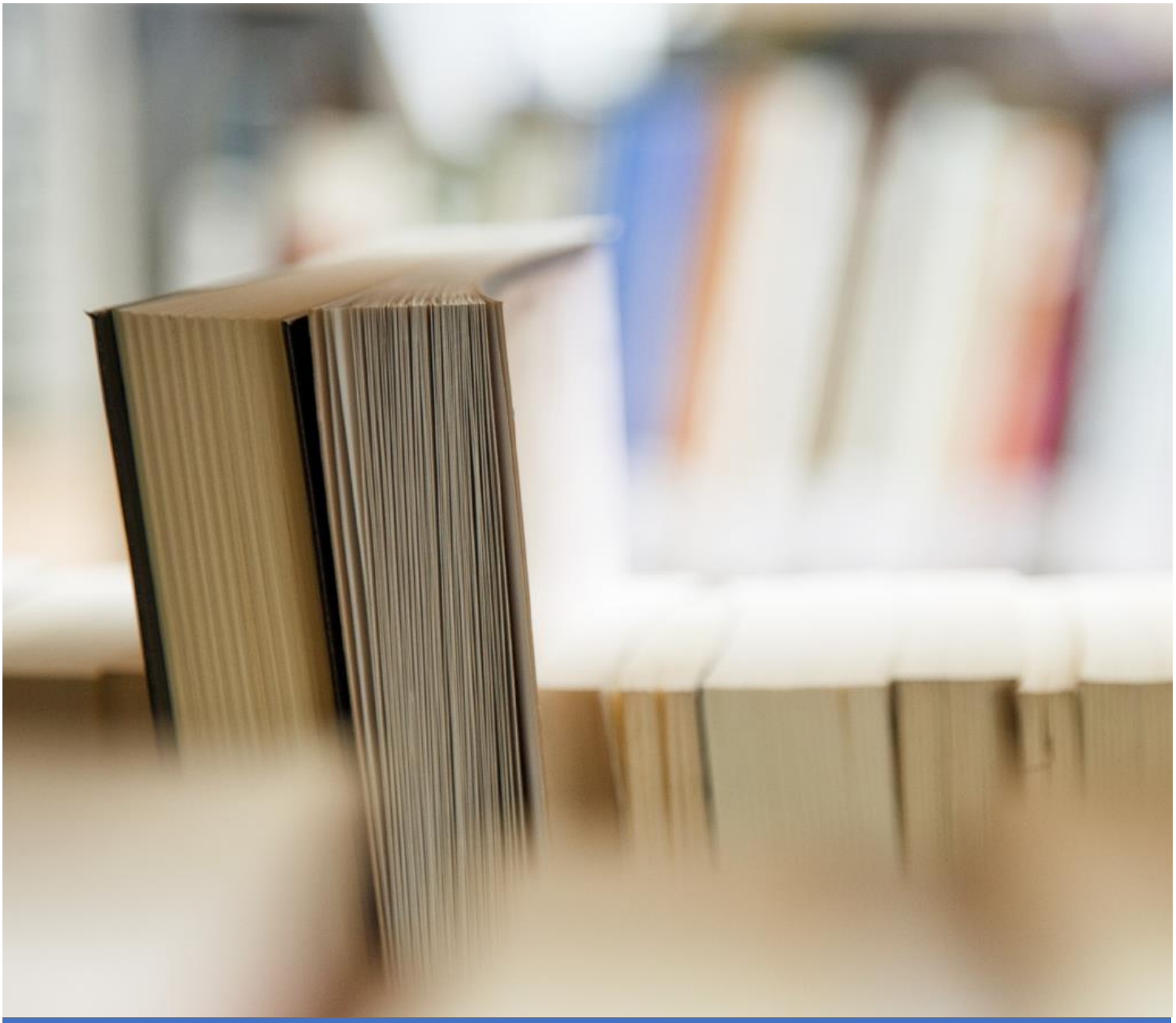

An overview of security concerns in cloud computing

Research Paper

Rajesh Deshpande

Page intentionally left blank

Table of Contents

Page intentionally left blank

An overview of security concerns in cloud computing

Abstract

The modern-day digital business requires scale, speed and agility that is provided by cloud computing. Cloud services are ubiquitously available to a broader set of users through a self-service interface. Ironically, even after a decade of cloud computing being around, it may come as a surprise that the issue of cloud computing is still perplexing to many organizations and individuals. There's good degree of inhibition surrounding Cloud adoption justified by issues like loss of control, dependency on the Cloud Service Provider, unpredictable costs and most importantly data security, privacy, and compliance issues. This paper examines key areas associated with security, risk and governance on the Cloud and provides an insight into the various aspects to be considered while deciding to adopt Cloud computing. Readers who are already using cloud services or those who have already transitioned their workloads to the cloud will also find this paper useful.

Conceptual Preliminaries

Cloud computing is the delivery of computing services like software, digital content, servers, data storage, integrated development environment over the Internet. Cloud is a metaphor for the internet as denoted in network diagrams. Companies offering such services are called as Cloud Service Providers or CSPs. They typically charge a fee for delivering computing services based upon usage just like electricity, gas, and water.

Cloud computing is a disruptive technology that has the potential to enhance collaboration, agility, scaling and availability as well as a possibility to reduce costs through optimized and efficient computing.

Definitions of Cloud computing – The National Institute of Standards and Technology (NIST), US Department of Commerce defines cloud computing as:

"Cloud computing is a model for enabling ubiquitous, 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."

The International Standards Organization (ISO) / International Electrotechnical Commission (IEC) definition is:

"Paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on demand."

NIST further defines Cloud Computing by describing five essential characteristics, four deployment models and three services as follows,

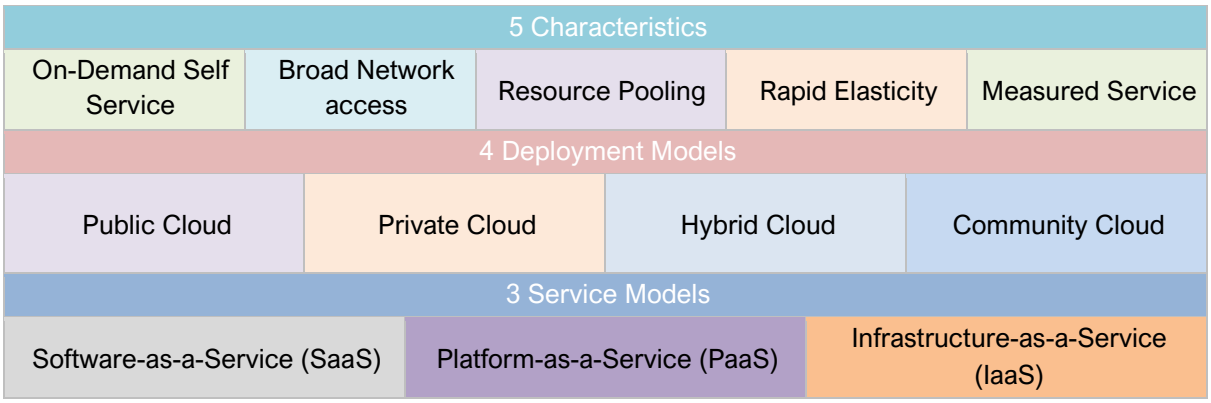

Figure 1 – NIST Cloud Computing Definition

Five Characteristics –

1. On demand self-service – a customer can unilaterally provision computing resources like servers and disk storage as and when required through a web dashboard.

2. Broad network access – ubiquitous access to computing resources over a network or the Internet using endpoints like Laptops, tablets, smartphones and workstations.

3. Resource pooling – a cloud service providers computing resources are pooled to serve multiple tenants by dynamically assigning and reassigning them as per demand. i.e. resources are shared dynamically between multiple tenants (customers).

4. Rapid elasticity – computing resources are scaled-in and scaled-out i.e. elastically provisioned and released as per demand.

5. Measured service – customers are billed as per their usage of computing resources i.e. pay-as-per-use.

Four deployment models –

1. Public Cloud – is owned and operated by a Cloud Service Provider. It is a shared multitenant model. Computing services are delivered over the Internet or a private network.

2. Private Cloud – is owned and operated by a company. It is a single tenant model. It is generally built within the company's own Datacenter. Computing services are delivered over the Internet or a private network.

3. Hybrid Cloud – uses a mix of company owned private cloud and Cloud Service Provider owned public cloud services with orchestration between the two platforms. Computing services are delivered through the Internet or a private network.

4. Community Cloud – is a cloud infrastructure purposefully built to deliver services that are exclusively used by a community of customers. E.g. some banks share core banking services on a community cloud.

Three service models –

The cloud delivers services like software, integrated development environment and hardware. A cloud service model defines the type of service delivered by the cloud.

1. Software – delivers Software-as-a-Service (SaaS) which is charged as a subscription per user. Cloud Service Providers (CSPs) deliver software like Email, CRM, Core Banking, ERP, HRMS. Some well-known examples of SaaS are Gmail, Office365, Facebook, LinkedIn, Twitter, Instagram, Salesforce, SAP.

2. Integrated Development Environment – known as Platform-as-a-Service (PaaS) provides an integrated development environment (IDE) for developing software applications using programming languages and frameworks like Java, PHP, Python, R, Dot Net, Hadoop, NoSQL, MongoDB.

3. Hardware – resources like servers (called as virtual machines), network and storage are provisioned on the Cloud and are charged as a monthly subscription based upon usage. This is called as Infrastructure-as-a-Service (IaaS).

Amazon Web Services (AWS), Microsoft Azure and Google Cloud Platform (GCP) are the world's largest Cloud Service Providers. They provide all the three types of Cloud services enumerated above.

The five characteristics, four deployment models and three service models of cloud computing defined by NIST can be memorized as the 5-4-3 rule.

Cloud Computing Technology Stack – the technology stack for cloud computing is illustrated below.

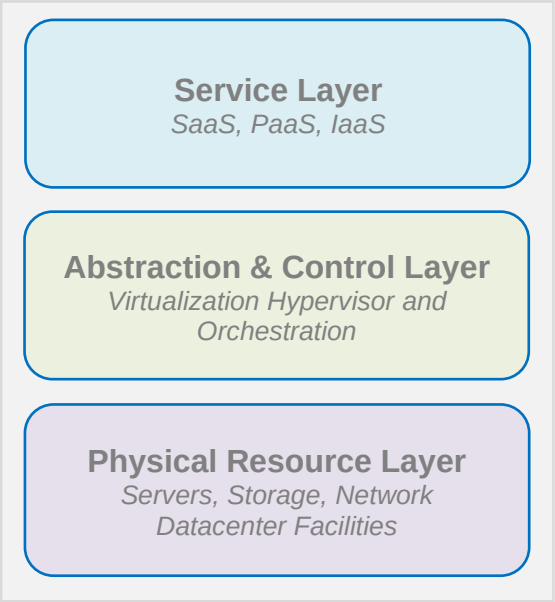

Figure 2 – Cloud Computing Technology Stack

A three-layered model is used to represent cloud computing technology stack, representing the grouping of three types of system components that Cloud Service Providers need to implement to deliver their services.

In the model shown in Figure 2, the top layer is the service layer, this is where Cloud Service Providers define interfaces for Cloud consumers to access the computing services. Access interfaces of each of the three service models are provided in this layer. It is possible, though not necessary, that SaaS applications can be built on top of PaaS components and PaaS components can be built on top of IaaS components.

The middle layer in the model is the resource abstraction and control layer. This layer contains the system components that Cloud Service Providers use to provide and manage access to the physical computing resources through software abstraction. Examples of resource abstraction components include software elements such as hypervisors, virtual machines, virtual data storage, and other computing resource abstractions. The control aspect of this layer refers to the software components that are responsible for resource allocation, access control, and usage monitoring. This is the software fabric that ties together the numerous underlying physical resources and

their software abstractions to enable resource pooling, dynamic allocation, and measured service. Various open source and proprietary cloud software are examples of this type of middleware.

The lowest layer in the stack is the physical resource layer, which includes all the physical computing resources. This layer includes hardware resources, such as computers (CPU and memory), networks (routers, firewalls, switches, network links and interfaces), storage components (hard disks) and other physical computing infrastructure elements. It also includes facility resources, such as heating, ventilation, and air conditioning (HVAC), power, communications, security and other aspects of the physical plant.

As per system architecture conventions, the adjacent layering in a model represents dependency relationships – the upper layer components are dependent on adjacent lower layer to function. The resource abstraction and control layer expose virtual cloud resources on top of the physical resource layer and supports the service layer where cloud services interfaces are exposed to cloud consumers, while cloud consumers do not have direct access to the physical resources.

Cloud computing – key drivers and inhibitors

The cloud is where many start-ups were born, and it continues to be the birthplace of new start-ups. Companies like Netflix, Airbnb and Uber started their journey on the cloud. Cloud computing accelerates launching of new products and services, facilitates ubiquitous access to employees and partners and enhances the customer experience.

Drivers of Cloud Computing –

1. Expense Model – Cloud computing is a move from capital expenditure to operating expenditure. The decision to opt for cloud services entirely depends upon the financial standing of an organization. It is more of a business decision than a choice of the IT Organization. E.g. Start-ups prefer the cloud because it facilitates them to invest their capital into business rather than investing it in technology.

2. Cost – The cloud may be beneficial in terms of cost up to a certain level of usage. As cloud usage grows i.e. no. of seats, no. of VM's and data, the recurring expenditure may grow to a point where the equation may tilt in favour of moving things back home. Many start-ups like Netflix, Uber, and Flipkart began their journey on the Cloud but as they grew, they opted to go home for curtailing operating cost.

3. Agility – SaaS provides the agility by delivering line of business (LOB) applications like ERP, CRM, and HRMS on demand. IaaS and PaaS provide the agility to deliver servers and development platforms on demand.

4. Scalability – SaaS, PaaS and IaaS Cloud service models provide the ability to scale up or scale down resources thus providing a 'pay only as much as you use' pricing model.

Inhibitors of Cloud Computing –

1. Security – being a multitenant system, the cloud is prone to hypervisor attacks, volumetric attacks and hacking which can pose a threat to customer's data. Poor isolation protection may lead to data of one customer being accessible to others. The cloud has become an attractive target of attack for hackers as it provides them a platform to inflict maximum damage.

2. Privacy – Data is at risk on the cloud if the Cloud Service Provider or the customer organization does not protect it enough. Data at rest on the Cloud if not encrypted may be at risk of being stolen by malicious insiders.

3. Compliance – Indian regulators like RBI, SEBI and IRDA have laid down stringent requirements for data locality, right to audit and reporting of security incidents. International regulations like SOX, HIPAA, PCI DSS have stringent requirements related to protection of customer identity information and data privacy. Compliance requirements could be an inhibitor in cloud adoption as Cloud Service Providers may not be compliant with such regulations or may not agree to cooperate for granting specific privileges to customer organizations.

4. Interoperability – Cloud service providers have developed tools for onboarding customer data and VMs to the cloud but there is nothing available to bring it back home. Also, there are challenges with availability of APIs or their integration with other services.

5. Lock-in – In a SaaS model both application and data are under the Cloud Service Provider's custody. The customer has a right to access the application and has ownership of his data. On contract termination, even if the Cloud Service Provider returns the data, it may be of little or no use to the customer due to the absence of an application to render the data usable. Due to this dependency, the customer gets locked into the service.

Cloud computing – benefits and risks

The key techniques to create a cloud are abstraction and orchestration. Computing resources are abstracted from the underlying physical infrastructure to create resource pools, orchestration (and automation) is used to provision a set of resources from the pools to the consumers. These two techniques create all the essential characteristics used to define a "Cloud." This is precisely the difference between cloud computing and traditional virtualization. Virtualization abstracts resources, but it typically lacks the orchestration to pool them together and deliver them to customers on demand, instead it relies on manual processes for provisioning resources.

Business benefits provided by the Cloud –

1. Accelerates business growth by allowing transformation of ideas into marketable products and services.

2. Provides a choice to business between one-time investment and recurring expenditure.

3. Democratization of computing makes ubiquitous availability of computing resources to everyone.

Risks associated with Cloud computing –

1. Security and Privacy – Loss of governance is a key risk with Cloud computing e.g. lack of visibility in vendor's operations processes like vulnerability management, infrastructure hardening, physical security, incident response and change management.

2. Fiscal Management and Tax – Op Ex pricing model of the Cloud impacts budgeting, forecasting, and reporting processes for the customer organization. A shift from fixed to variable cost model and change in character and source of services impacts tax considerations. Outdated Indian tax laws create uncertainty when characterizing the various Cloud transactions. ROI and cost benefit analysis of cloud services are complicated by the need for knowledge of existing cost of delivery and future use of service.

3. Vendor Management – Lack of clarity on ownership responsibilities between Cloud vendor and customer organization may lead to administrative lapses. There is no prevalent standard for interoperability of services between Cloud Service Providers. Cloud services also create a dependency for the customer organization on the Cloud Service Provider.

4. Operational impact – Cloud adoption introduces rapid changes in the organization. Success depends upon organization culture. It may have a significant impact on organizational roles and may require development of new skillsets. The organization Business Continuity / Disaster Recovery plan would undergo a notable change. The role of IT Org. in the customer organization changes from an implementer to a facilitator.

5. Data and Technology – Cloud services may expose the customer organization to shadow IT. Without proper controls, end users may dump data on the cloud. Without proper processes in place, business may bypass the IT Org. to buy apps and services directly. The organization perimeter becomes redundant due to Cloud.
6. Regulatory and Compliance – Lack of visibility in to Cloud Service Provider operations inhibits knowledge of its compliance with pertinent laws and regulations. Lack of industry standards and certifications for Cloud Service Providers is a risk for customer organizations (the only industry certification as on date is CSA Star).

Myths around Cloud computing

The naïve belief that Cloud Service Providers are entirely responsible for the security of customer organization's instance means many organizations are failing to address how their employees use cloud applications and thus leaving them free to share large amounts of classified data with third parties and even the whole Internet at times.

1. *"Security is implied on the cloud"* – a common misconception amongst customer organizations is that security would be taken care of by the Cloud Service Provider and anything that is hosted on the Cloud would inherently and automatically be secured. However, this is not true for Infrastructure-as-a-Service and Platform-as-a-Service. The Cloud Service Provider is responsible only for platform security and not of Guest OS and Apps, which is clearly the responsibility of customer organization.

2. *"Fault tolerance is a default feature"* – Although the Cloud Service Provider would have implemented hardware fault tolerance for host servers, storage and network, the availability of everything above the Virtual Machine (VM) layer must be ascertained. The Cloud Service Provider's responsibility is to ensure availability and uptime of the VM and not of the application and data associated with the VM. For E.g. Guest OS of a VM may crash, an application may crash or VM performance may degrade. A backup VM may be required for failover and

scalability in such situations to keep the application available. Such requirements are additionally charged by Cloud Service Providers.

3. *"Disaster Recovery is not required in the Cloud"* – Yet another misconception which is common amongst customer organizations is that 'they are immune to failures in the Cloud Service Provider Datacenter, and everything would continue to work seamlessly from another site'. This may be true with SaaS to some extent but certainly not with IaaS. The Cloud Service Provider at best would facilitate availability of VM's at a DR site in case if the primary Cloud Datacenter experiences a major failure. However, data replication and application availability could become a challenge for resuming operations. Therefore, a purposefully built DR-as-a-Service is needed for data replication and application failover to a DR site. This service is generally offered by Cloud Service Providers at an additional cost.

4. *"Data backup is not required in the Cloud"* – A Cloud Service Provider has no business to do with customer organization's data. A myth is that since data is always available on the Cloud there is no need to maintain a backup. Data backup captures a state of data at a given time, if backups are not done, the data state on a date would not be known since data would have undergone changes past that date. Responsibility of data backup on the cloud is entirely on the customer organization. Cloud Service Providers offer data backup services at a cost. Customer organizations may choose to subscribe to this service. The customer organization must identify what data needs to be backed up e.g. Databases, Logs, Apps, Files etc. and then decide upon what type of data backup should be implemented.

5. *"Moving to the cloud would increase performance"* – The Cloud is not a magic wand. For a given set of resources like vCPU, vRAM and vDisk, application performance would not increase significantly unless some sort of optimization measure is implemented. Special attention is needed in bandwidth sizing between the Cloud Service Provider DC and the customer organization. Any miscalculation at this stage may degrade performance if not increase it.

6. *"Assumed Value Added Services"* – Customer organizations assume that the Cloud is a turnkey solution that takes care of everything. However, life is not so simple yet. Cloud Service Providers offer a diversity of value-added services like advanced security, VPN gateway, data backup, IP addresses, web application firewall, storage and more. These are chargeable services and are entirely left to the choice of the customer organization.

Cloud Security Concerns

Cloud security includes everything that a security team is responsible for. All the security domains are relevant but the nature of risks, roles and responsibilities, and implementation of controls change dramatically. Cloud computing is a shared technology model where different organizations are responsible for implementing and managing various parts of the stack. As a result, security responsibilities also get distributed across the stack and thus across the organizations involved.

1. Responsibility of security in the Cloud – The most important security consideration is knowing who is responsible for what. In SaaS environments, the security is almost entirely the responsibility of the Cloud Service Provider. In IaaS offerings, while the responsibility of securing the underlying infrastructure and abstraction layers belongs to the Cloud Service Provider, everything else is the customer organization's responsibility. This includes protection of Guest OS, application security, vulnerability scanning, identity and access management, security incident and event management and security of the management plane. PaaS offers a balance somewhere in between where securing the platform is the Cloud Service Provider's responsibility whereas securing the applications developed on the platform is customer's responsibility.

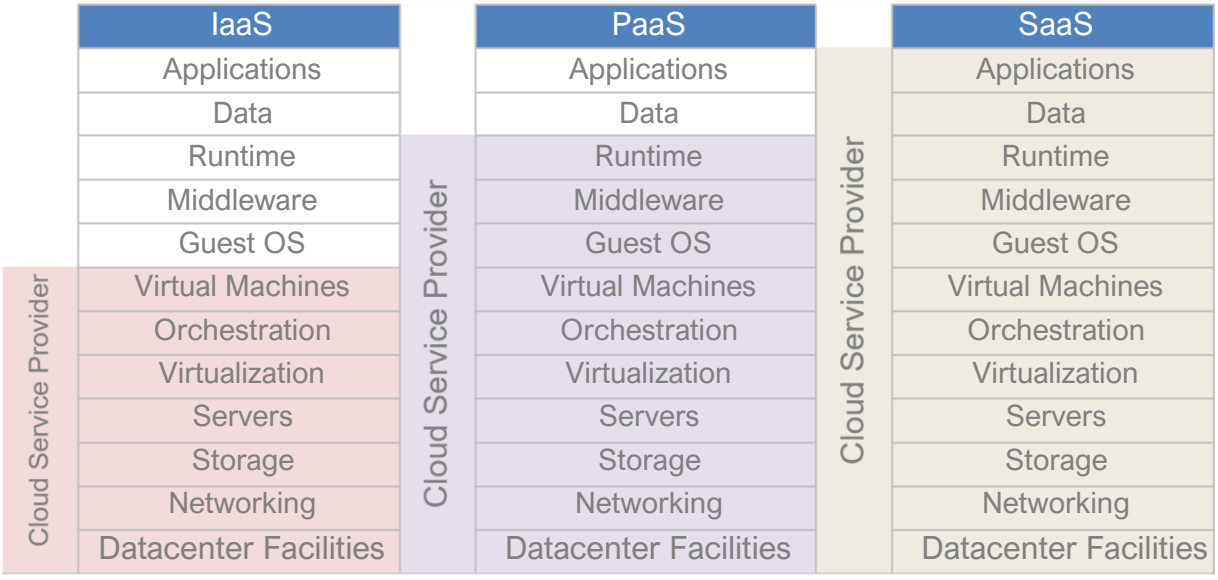

Figure 3 – Responsibility of Cloud Service Provider and Customer Organization

2. Data breach – is a security incident in which sensitive, protected, or confidential data is copied, transmitted, viewed, stolen, or used by an individual unauthorized to do so. An organization's cloud-based data may have value to different parties for several reasons. E.g. organized crime often seeks financial, health and personal information to carry out a range of fraudulent activities. Competitors

and foreign nationals may be keenly interested in proprietary information, intellectual property, and trade secrets. Activists may want to expose information that can cause damage or embarrassment. Data breaches and enabling of attacks can occur because of a lack of scalable identity access management systems, failure to use multifactor authentication, weak password use, and a lack of ongoing automated rotation of cryptographic keys, passwords, and certificates.

3. Identity and Access Management on the Cloud – Identity systems are becoming increasingly interconnected, and federating identity with a Cloud Service Provider is becoming more prevalent to ease the burden of user maintenance. Organizations planning to federate identity with a Cloud Service Provider need to understand the security around the Cloud Service Provider identity solution, including processes, infrastructure, and segmentation between customers (in the case of a shared identity solution). Identity systems must scale to handle lifecycle management for millions of users as well as the Cloud Service Providers. Identity management systems must support immediate deprovisioning of access to resources when personnel changes, such as job termination or role change, occur.

4. Malicious insiders – A malicious insider threat to an organization is a current or former employee, contractor, or other business partner who has or had authorized access to an organization's network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems. A malicious insider, such as a system administrator, can access potentially sensitive information. The Cloud Service Provider must have adequate checks and balances to verify the integrity of its own personnel and contractual personnel coupled with corresponding processes like separation of duties, mandatory leaves, and periodic medical checks. A process to revoke privileged access in the event of any irregularity being detected or during separation of personnel should be present.

5. System vulnerabilities – are exploitable bugs in programs that attackers can use to infiltrate a computer system for stealing data, taking control of the system, or disrupting service operations. Vulnerabilities within the components of the operating system – kernel, system libraries and application tools put the security of all services and data at significant risk. The Cloud Service Provider must have well defined processes for consistently applying patches and updates to hardware, network, and virtualization components. The customer organization must also have corresponding processes for lockdown of Guest OS, Database and Web service components. The customer organization should also have

defined processes for patch management of Guest OS and for updating Antivirus signatures on virtual machine instances.

6. Account hijacking – Customer account on the Cloud Service Provider website is hijacked and a bonafide customer is denied access. Cloud solutions add a new threat to the landscape. If attackers gain access to customer credentials, they can eavesdrop on activities and transactions, manipulate data, return falsified information, and redirect clients to illegitimate sites. The cloud account or service instances may become a new base for attackers. From here, they may leverage the power of customer's reputation to launch subsequent attacks. Customer organizations and Cloud Service Providers must restrict access to the tenant control panel only to authorized named personnel whose actions are traceable. The access control matrix (ACM) must be exchanged periodically.

7. Advanced Persistent Threat (APT) – are a parasitical form of cyber-attack that infiltrates systems to establish a foothold in the computing infrastructure of target companies from which they smuggle data and intellectual property. APTs pursue their goals stealthily over extended periods of time, often adapting to the security measures intended to defend against them. Spear phishing, direct hacking systems, delivering attack code through USB devices, penetration through partner networks and use of unsecured or third-party networks are common points of entry for APTs. Once in place, APTs can move laterally through Datacenter networks and blend in with normal network traffic to achieve their objectives. The Cloud Service Provider and customer organizations must consider implementing artificial intelligence (AI) based threat intelligence controls for effectively counteracting the risk.

8. Data Loss – Data stored in the cloud can be lost for reasons other than malicious attacks. An accidental deletion by the Cloud Service Provider, or worse, a physical catastrophe such as a fire or earthquake, can lead to the permanent loss of customer data unless the provider or customer organization takes adequate measures to backup data and possibly off-site storage. Furthermore, the burden of avoiding data loss does not fall solely on the Cloud Service Provider's shoulders. If a customer encrypts his or her data before uploading it to the cloud but loses the encryption key, the data will be lost as well.

   Customer organizations should review the contracted data loss provisions, ask about the redundancy of a provider's solution, and understand which entity is responsible for data loss and under what conditions. Some providers offer solutions for geographic redundancy, data backup within the cloud, and premise-to-cloud backups. The risk of relying on the provider to store, backup

and protect the data must be considered against handling that function inhouse, and the choice to do both may be made if data is extremely critical.

9. Inadequate diligence – An organization that rushes to adopt cloud technologies and choose Cloud Service Provider without performing due diligence exposes itself to a myriad of commercial, financial, technical, legal and compliance risks that jeopardize its success. This applies whether the company is considering moving to the cloud or merging with or acquiring a company that has already moved to the cloud or is considering doing so.

10. Cloud service abuses – Poorly secured cloud service deployments, free cloud service trials and fraudulent account sign-ups via payment instrument fraud expose cloud computing models such as IaaS, PaaS, and SaaS to malicious attacks. Malicious actors may leverage cloud computing resources to target users, organizations, or other cloud providers. Examples of misuse of cloud service-based resources include launching DDoS attacks, Email spam and phishing campaigns; “mining” for digital currency; large-scale automated click fraud; brute-force compute attacks of stolen credential databases; and hosting of malicious or pirated content.

11. Service Denial – Denial-of-service (DoS) attacks are volumetric attacks meant to prevent users of a service from being able to access their data or their applications. By forcing the targeted cloud service to consume inordinate amounts of finite system resources such as processor power, memory, disk space or network bandwidth, the attackers, as is the case in distributed denial of-service (DDoS) attacks — causes an intolerable system slowdown and leaves all legitimate service users confused and angry as to why the service is not responding. The customer organization should ascertain that the Cloud Service Provider has implemented adequate DDoS protection controls for its overall infrastructure.

12. Shared technology vulnerabilities – Cloud service providers deliver their services scalability by sharing infrastructure, platforms, or applications. Cloud technology divides the “as a Service” offering without substantially changing the off the-shelf hardware / software—sometimes at the expense of security. Underlying components (e.g., CPU caches, RAM, GPUs, etc.) that comprise the infrastructure supporting cloud services deployment may not have been designed to offer strong isolation protection for a multitenant architecture (IaaS), re-deployable platforms (PaaS) or multi customer applications (SaaS). This can lead to shared technology vulnerabilities that can potentially be exploited in all delivery models. A defence in depth strategy is recommended and should include compute, storage, network, application and user security enforcement

and monitoring, whether the service model is IaaS, PaaS, or SaaS. The key is that a single vulnerability or misconfiguration can lead to a compromise across an entire provider's cloud.

13. Security of the management plane – The management plane is a set of tools and graphical user interfaces which are accessible remotely over a network or the Internet to manage the customer instance of infrastructure, platform or software as a service i.e. partition of the Cloud allotted to a customer organization. The management plane abstracts and centralizes administrative management of resources. Instead of controlling a Datacenter configuration with boxes and wires, it is now controlled with application programming interface (API) calls and user interfaces (UI). A malicious intruder gaining access to the management plane would also gain unfettered access to the Cloud Datacenter, unless proper security controls are put in place to limit who can access the management plane and what they can do within it. To think about it in security terms, the management plane consolidates many things that were previously managed through separate systems and tools, and then makes them internet accessible with a single set of authentication credentials. Securing the management plane is key to a robust security policy implemented by the Cloud Service Provider and by the customer organization. As a minimum, the management plane should facilitate multi-factor authentication and random encryption keys for gaining access to the Cloud ecosystem.

14. Application Security – Websites and web applications are the primary target of attack for hackers. With cloud computing, the customer organization is left vulnerable in many ways. Firstly, the security team of customer organization loses visibility into the network security infrastructure. If the Cloud Service Provider makes a change to its infrastructure, it naturally changes the risk profile of the customer organization's application. However, the customer organization is most likely not informed of these changes and therefore unaware of the ultimate impact. Secondly, customer organizations view application security as an unnecessary cost. The corporate focus is on revenue, and often that means frequently pushing new code. Even with rigid acquisition, development, and quality assurance (QA) processes, there will be differences between QA and actual production applications. This was not as critical when the applications resided behind the customer organization firewall, but in the cloud, customer organizations must consider the value of data stored in an application residing in the cloud.

    Customer organizations should inventory their cloud (and existing Web) application deployments. Based upon a meaningful impact analysis, adequate security controls must be applied to each application. An application

vulnerability assessment should be performed on all applications periodically or after each major change.

Once the customer organization has accurate and actionable vulnerability data about all its websites, it can then create a mitigation plan. Urgent issues can be "virtually patched" with a Web Application Firewall (WAF); less serious issues can be sent to the development queue for later remediation. Instead of facing the undesirable choice between shutting a website down or leaving it exposed, customer organizations armed with the right data can be proactive about security, reduce risk and maintain business continuity.

15. Incident Response – To avoid a security incident in the cloud, customer organizations must have an incident response plan. the most practical first step is to establish a joint response process. Responsibilities and roles should be clearly defined and contact information for primary and secondary contacts should be exchanged. The customer organization should obtain a detailed explanation of what triggers the provider's incident response and how the provider will manage different issues. For an effective response on security issues related to cloud infrastructure, it is important for the customer organization to understand what kind of monitoring and security measures are made available by the Cloud Service Provider. If the tools or security services are insufficient, the customer organization should look out at ways to deploy a supplemental solution.

    The customer organization should decide whether recovery will be necessary in the event of a provider outage. It should create a recovery plan that defines whether to use an alternate provider or on-premises DC as well as a procedure to collect and move data. The customer organization should find out what tools are available from the cloud service provider or from other sources for conducting forensics in case of an incident. If the incident involves PII information, it might turn into a legal and compliance challenge, so having appropriate tools which can help with forensics and evidence tracking is essential.

Cloud Governance and Risk management

Governance includes the policy, process and internal controls that comprise how an organization is run. Cloud computing affects governance since it introduces a third party – the Cloud Service Provider into the process. Even if Cloud computing is an outsourcing model, the customer organization can never outsource responsibility for governance. The management tools for Cloud governance are enumerated below.

Contracts – are the primary tool between the Cloud Service Provider and a customer organization. A cloud services contract guarantees service uptime and performance, information non-disclosure and extends governance to the Cloud Service Provider.

Supplier Assessment – is done by the potential customer organization of the Cloud Service Provider on various dimensions like,

- Financial solvency, investors, and sources of funding.
- Contracts with OEMs, insurance policies and their validity.
- Operations Processes – incident management, BC/DR, change management and asset management processes of the Cloud Service Provider.
- Frequency of assessment of certifications e.g. ISO27001, PCI DSS, HIPAA, SOX, UPI etc.)
- Level of sub-contracting done by Cloud Service Provider.

Compliance Reporting – includes all the documentation on a Cloud Service Providers internal and external compliance assessment. They are audit reports of the Cloud Service Provider as assessed by a third-party auditor. Cloud Service Provider may be assessed for existing standards like the SSAE 16 and for compliance with extant laws and regulations, compliance with international standards and frameworks E.g. ISO27001, PCI DSS, HIPAA, SOX. The scope may also include software licensing compliance.

Conclusion

Cloud security is more of a shared responsibility between a Cloud Service Provider and the customer organization. It is a matter of identifying security roles and responsibilities, re-aligning security processes and implementing an adequate governance structure based upon the policies and procedures laid down by the customer security organization.

The cloud business model provides huge market incentives for cloud service providers to place a higher priority on security than is typical for customer organizations. Cloud service providers can afford to hire experienced system and InfoSec specialists, and their economies of scale make it practical to provide round-the-clock security monitoring and response. Even though, customer organizations should not assume that using a cloud service means that whatever they do within that cloud will be secure. The characteristics of the cloud stack under customer control can make it easy for inexperienced users to adopt poor cloud practices, which can lead to widespread security or compliance failures. Ultimately the responsibility lies with the customer organization to exert control over cloud. Secure and regulatory-compliant use of public clouds requires that enterprises implement and enforce clear policies on usage

responsibility and cloud risk acceptance processes. Customer organizations that don't take a strategic approach to the secure use of cloud computing could find themselves in an unsecure, unfavourable or uncompetitive situation.

References –

1. Cloud Security Alliance – Security Guidance for Critical Areas of Focus in Cloud Computing v3.0

2. National Institute of Standards and Technology – NIST Cloud Computing Reference Architecture NIST SP 500-292.

3. Gartner eBook – Cloud Strategy Leadership, Chapter 2 – Securing the Cloud.

4. ISACA Mumbai Chapter Meeting – Cloud Security Fundamentals, excerpts from speaker presentation.

========