MET's Institute of Engineering

Bhujbal Knowledge City, Adgaon, Nashik.

Department of Computer Engineering

"Security in Cloud Computing"

Prepared By

Prof. Anand N. Gharu

(Assistant Professor)

Computer Engineering Departement

CLASS : TE COMPUTER 2019

SUBJECT : CC (SEM-II)

UNIT : V

08 June 2022

SYLLABUS

- **Risks in Cloud Computing:** Risk Management, Enterprise-Wide Risk Management, Types of Risks in Cloud Computing.
- **Data Security in Cloud:** Security Issues, Challenges, advantages, Disadvantages, Cloud Digital persona and Data security, Content Level Security.
- **Cloud Security Services:** Confidentiality, Integrity and Availability, Security Authorization Challenges in the Cloud, Secure Cloud Software Requirements, Secure Cloud Software Testing.

Risk in Cloud Computing

Risk in Cloud Computing

Introduction to Risks of Cloud Computing :

Being an on-demand availability of system resources, like computing power and data storage, cloud computing involves various types of risks that are grouped in different categories like privacy (involves risk like controlled Access, Segmentation, Risk with Sub letting services and ownership claim), availability (involves risk like service disruption), changes (involves risk like Changes in service and return of investment) and compliance(involves risk like Audit, storage location, and notification).

Risk Management

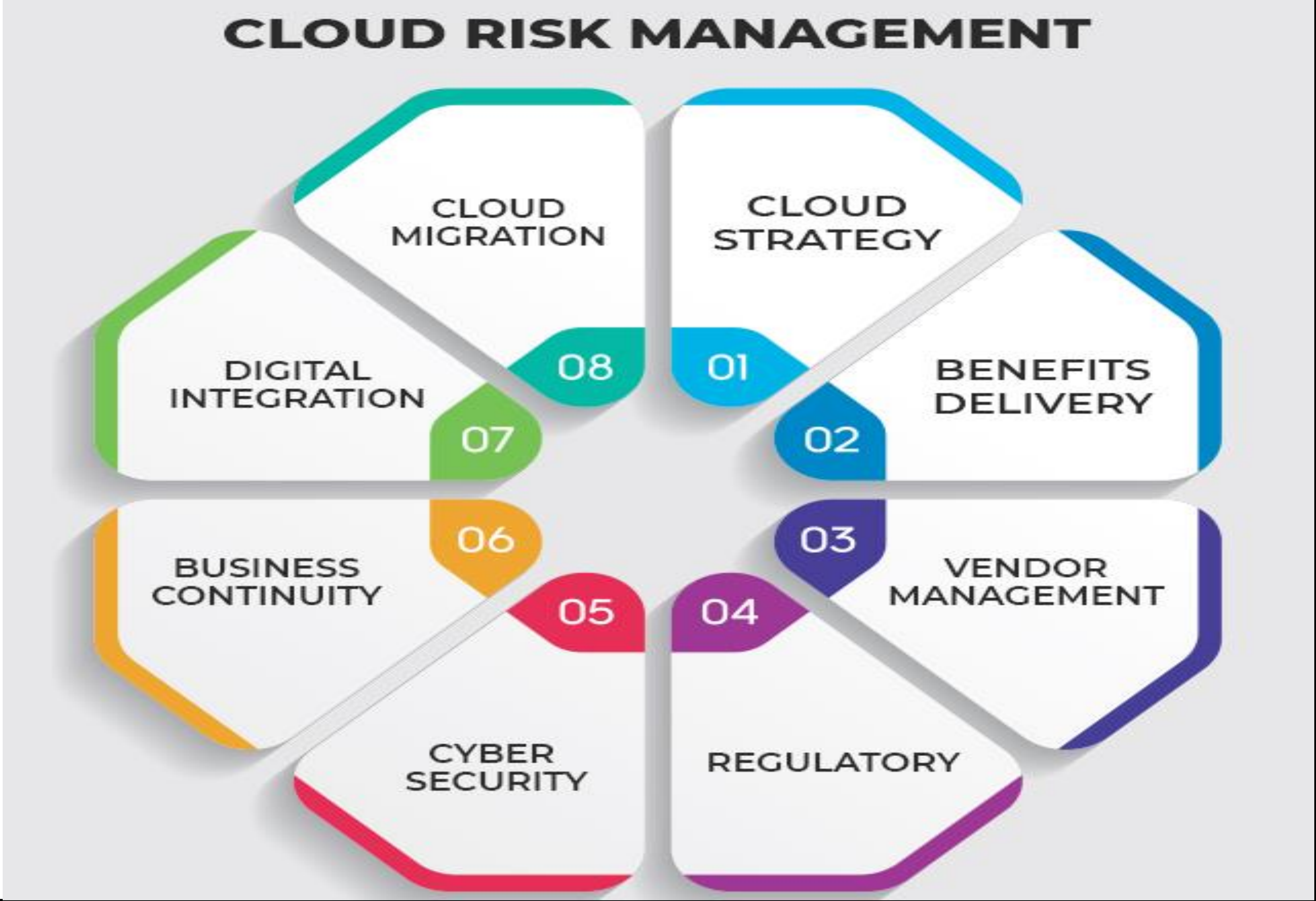
1. Comprehensive Risk Management :

Comprehensive risk management would, of course, begin with a comprehensive risk management framework, which would include everything from detecting and assessing cyber risk to factoring cyber risk into the institution's total risk appetite.

Furthermore, minimizing the risks associated with cloud migration necessitates incorporating cyber risk management within the institution's enterprise risk management operations.

When understanding the risks to the enterprise, it may give top management better insight into hazards and essential data

Risk Management



Risk Management

2. Cybersecurity :

As the complexity and frequency of cyber threats rise, organizations should create a comprehensive cybersecurity program.

They should concentrate on finding vulnerabilities, deploying solutions to protect important business data, detecting potential threats that have infiltrated the infrastructure, and assisting essential business applications and systems in responding to and recovering from incidents.

Given that executives at financial institutions are under enormous pressure to maintain the integrity of their data, keep their customers' sensitive information safe, be fully versed on evolving threats and challenges, and prepare for threats they have not yet seen, it is critical for an institution to establish an aggressive, analytics-driven solution to identify, manage, and mitigate threats.

Risk Management

3. Regulatory compliance :

In light of these problems, authorities all over the world are continuing to act by releasing and updating recommendations on cloud computing and how to avoid and respond to cyber-attacks. Without automation, the expenses of maintaining a risk staff to remain on top of these rules will skyrocket.

Risk Management

4. Backup and recovery :

Almost every company does frequent backups. However, very few businesses actually undertake frequent restoration to ensure the functionality and sufficiency of backups, resulting in unpleasant shocks at the last minute.

Cloud companies have this step-down path since the consequences of a blunder will be devastating to their business. Again, this is a two-edged sword that is depending on the cloud provider's rules, which may or may not be sufficient for your organization's needs.

Risk Management

5. Instituting an end-to-end cyber risk framework :

While keeping your company's goals in mind at all times, there are a few key fundamental measures to take while creating a good cloud-security plan.

It all starts with creating a high-level strategic approach to risk assessment and management that is tailored to your company's needs – there is no one-size-fits-all solution.

This involves developing a budget that is reasonable, practical, and attainable, as well as a deployment plan.

.

Risk Management

6. Platform support :

Many companies are unable to roll out patches on time, or even discover the appropriate patches, for a variety of reasons such as a lack of a suitable knowledge base, time, or testing infrastructure.

Most cloud providers do not have these weaknesses, guaranteeing that the platforms and apps you use on such cloud settings are properly up to date.

This is a two-edged sword because vulnerabilities are found in several cloud providers. Organizations with reasonably developed procedures ensure things such as timely internal system changes and sufficient testing.

The same cannot be true for cloud providers owing to a lack of visibility and openness.

Risk Management

6. Platform support :

Many companies are unable to roll out patches on time, or even discover the appropriate patches, for a variety of reasons such as a lack of a suitable knowledge base, time, or testing infrastructure.

Most cloud providers do not have these weaknesses, guaranteeing that the platforms and apps you use on such cloud settings are properly up to date.

This is a two-edged sword because vulnerabilities are found in several cloud providers. Organizations with reasonably developed procedures ensure things such as timely internal system changes and sufficient testing.

The same cannot be true for cloud providers owing to a lack of visibility and openness.

Risk Management

7. Vendor Management :

The inclusion of third-party suppliers in cloud business models has raised security issues. Many cloud providers are undergoing official third-party security assessments, such as the International Organization for Standardization (ISO), Service Organization Control (SOC) 2, and the Federal Risk Authorization and Management Program (FedRAMP).

To prevent security problems, you should concentrate on establishing a corporate public cloud strategy that includes security guidelines on approved SaaS usage.

You will need to understand how to include procurement and sourcing solutions into this approach. You may also establish and enforce policies on use responsibility and risk acceptance processes in the cloud.

It is important to employ a life-cycle governance model that stresses ongoing operational management of your public cloud utilization

Risk Management

7. Vendor Management :

The inclusion of third-party suppliers in cloud business models has raised security issues. Many cloud providers are undergoing official third-party security assessments, such as the International Organization for Standardization (ISO), Service Organization Control (SOC) 2, and the Federal Risk Authorization and Management Program (FedRAMP).

To prevent security problems, you should concentrate on establishing a corporate public cloud strategy that includes security guidelines on approved SaaS usage.

You will need to understand how to include procurement and sourcing solutions into this approach. You may also establish and enforce policies on use responsibility and risk acceptance processes in the cloud.

It is important to employ a life-cycle governance model that stresses ongoing operational management of your public cloud utilization

Risk Management

8. Cloud Migration :

The process of transferring apps, data or even the whole corporate IT infrastructure to distant server facilities and a virtual environment is known as cloud migration.

The benefits of cloud migration are numerous. The cloud architecture allows for the acceptance of any workload, and the simplicity with which new services may be added allows for rapid response to changing business demands.

Risk Management

8. Cloud Migration :

The process of transferring apps, data or even the whole corporate IT infrastructure to distant server facilities and a virtual environment is known as cloud migration.

The benefits of cloud migration are numerous. The cloud architecture allows for the acceptance of any workload, and the simplicity with which new services may be added allows for rapid response to changing business demands.

Best Practices for Cloud Computing Risk Management

1. Carefully select your cloud service provider (CSP). Conduct supplier risk evaluations for contract clarity, ethics, legal liability, viability, security, compliance, availability, and business resilience, among other things.

Determine whether or not the CSP itself has service providers it can rely on to deliver its solutions and adjust the scope accordingly.

2. Establish adequate controls based on the risk treatment. After measuring the risks and determining the risk appetite, the resulting risk treatment solutions will drive the program in a reasonable, pragmatic and prioritized manner.

An essential aspect of risk management is to build robust data classification and lifecycle management methods. It’s also a good idea to incorporate processes in your service-level agreements (SLAs) for safeguarding, and even erasing, data hosted in the public cloud.

Best Practices for Cloud Computing Risk Management

3. Deploy technical safeguards. Technical safeguards, such as a cloud access security broker (CASB), can be cloud or on-premises security policy enforcement points between cloud service users and providers. It serves as an enforcement point for enterprise security policies when users access cloud-based resources.

4. Vendor management. Third-party suppliers' presence in cloud business models has generated security concerns. Many cloud services are subject to third-party security audits, such as those specified by the International Organization for Standardization (ISO).

Consider building a public cloud strategy that includes security criteria for suitable SaaS usage to avoid security risks.

Best Practices for Cloud Computing Risk Management

5. Implement a comprehensive ERM framework. The Committee of Sponsoring Organizations (COSO) offers a comprehensive ERM framework to help you succeed, as does the International Organization for Standardization (ISO).

Governance, risk management, and compliance (GRC) software can help you track and automate many of your risk management tasks to ensure compliance with various frameworks.

Enterprise Wide-Risk Management

As defined in COSO's 2004 Enterprise Risk Management – Integrated Framework: "Risk is the possibility that an event will occur and adversely affect the achievement of objectives."

The types of risks (e.g., security, integrity, availability, and performance) are the same with systems in the cloud as they are with non-cloud technology solutions.

An organization's level of risk and risk profile will in most cases change if cloud solutions are adopted (depending on how and for what purpose the cloud solutions are used). This is due to the increase or decrease in likelihood and impact with respect to the risk events (inherent and residual) associated with the CSP that has been engaged for services.

Types of Enterprise Risks in Cloud Computing

Cloud Computing provides recommended risk responses for the following major risks relating to Cloud Computing :

-Unauthorized cloud activity

-Lack of transparency

-Security, compliance, data leakage, and data jurisdiction

-Transparency and relinquishing direct control

-Reliability, performance, high-value cyber-attack target

-Vendor lock-in

-Non compliance with disclosure requirements

-Non compliance with regulations

Types of Enterprise Risks in Cloud Computing

1. Unauthorized Access to Business Data :

Cloud computing services manage data from thousands of companies. Each company using a cloud service, however, increases the value of that service as a potential target for cyber attackers – and the risk is concentrated at a single point of failure (the cloud service provider). As a result, a cyber attack at a cloud provider could affect all of its customers.

No business is safe in this scenario. Attackers may target small businesses because those companies typically have weaker controls and may be easier to breach. Alternatively, some attackers prefer to target larger companies because of the lure of hefty payouts.

Types of Enterprise Risks in Cloud Computing

2. Cloud Vendor Security Risks :

Using cloud providers exposes you to additional third-party risks. Doing business with any vendor that experiences business challenges such as bankruptcy, lawsuits, regulatory investigations, or other threats could inadvertently harm your organization’s reputation and goodwill.

Many small businesses know little about the technology behind the cloud services they use. As a result, your reputation no longer depends only on the integrity of your company: it now also relies on the integrity of the cloud provider’s company. And that’s a risk of cloud computing.

Due to the ease of access to IaaS (infrastructure as a service), there has been a proliferation of innovative SaaS (software as a service) startups providing cloud services. Some offer unique features that traditional providers have left unmet.

Some of these providers, however, may lack the expertise required to meet stringent control requirements. Their products may also be unsustainable for large organizations that need to exchange increasing amounts of data.

Types of Enterprise Risks in Cloud Computing

3. Compliance Risks :

Legal or compliance risks arise from non-compliance with various industry regulations or regulatory requirements, such as the Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley Act (SOX), Gramm-Leach-Bliley Act (GLBA), or the European Union’s General Data Protection Regulation (GDPR).

When a data breach in a cloud service provider exposes personal data, your company may be held accountable if it does not have proper protections in place. In other words, a cloud service provider suffers a breach of your data, and you will still suffer the consequences. Proper legal contracts to place as much of that responsibility back upon the cloud provider are vital.

Types of Enterprise Risks in Cloud Computing

4. Operational Control :

When an organization manages its own IT infrastructure such as enterprise tools, documents, computing resources, and processes, it has direct control over these elements (along with responsibility for their care). When outsourcing to a vendor cloud environment, the control resides with the cloud provider – not you.

Types of Enterprise Risks in Cloud Computing

5. Availability Risks :

If your Internet access is lost, you will be unable to access your provider’s cloud service. You’ll have to wait until the Internet is back up and running if you need to use the cloud service to process customer payments or access sensitive data. You don’t have this problem when operating on a local server.

Another risk associated with the cloud is that the service provider may fail. The service can become unresponsive due to various factors, including adverse weather, distributed denial of service (DDoS) assaults, or some other system breakdown.

Downtime of cloud environments, platforms, or infrastructure can significantly affect companies that rely primarily on cloud computing technologies for their day-to-day operations and corporations that provide user services.

Types of Enterprise Risks in Cloud Computing

6. Lack of transparency – A CSP is unlikely to divulge detailed information about its processes, operations, controls, and methodologies. For instance, cloud customers have little insight into the storage location(s) of data, algorithms used by the CSP to provision or allocate computing resources, the specific controls used to secure components of the cloud computing architecture, or how customer data is segregated within the cloud.

7. Reliability and performance issues – System failure is a risk event that can occur in any computing environment but poses unique challenges with cloud computing. Although service-level agreements can be structured to meet particular requirements, CSP solutions might sometimes be unable to meet these performance metrics if a cloud tenant or incident puts an unexpected resource demand on the cloud infrastructure**.**

Types of Enterprise Risks in Cloud Computing

8. Vendor lock-in and lack of application portability or interoperability – Many CSPs offer application software development tools with their cloud solutions. When these tools are proprietary, they may create applications that work only within the CSP’s specific solution architecture. Consequently, these new applications (created by these proprietary tools) might not work well with systems residing outside of the cloud solution. In addition, the more applications developed with these proprietary tools and the more organizational data stored in a specific CSP’s cloud solution, the more difficult it becomes to change providers.

Types of Enterprise Risks in Cloud Computing

9. High-value cyber-attack targets – The consolidation of multiple organizations operating on a CSP’s infrastructure presents a more attractive target than a single organization, thus increasing the likelihood of attacks. Consequently, the inherent risk levels of a CSP solution in most cases are higher with respect to confidentiality and data integrity.

10. Risk of data leakage – A multi-tenant cloud environment in which user organizations and applications share resources presents a risk of data leakage that does not exist when dedicated servers and resources are used exclusively by one organization. This risk of data leakage presents an additional point of consideration with respect to meeting data privacy and confidentiality requirements.

11. IT organizational changes – If cloud computing is adopted to a significant degree, an organization needs fewer internal IT personnel in the areas of infrastructure management, technology deployment, application development, and maintenance. The morale and dedication of remaining IT staff members could be at risk as a result.

Types of Enterprise Risks in Cloud Computing

12. Cloud service provider viability – Many cloud service providers are relatively young companies, or the cloud computing business line is a new one for a well- established company. Hence the projected longevity and profitability of cloud services are unknown. At the time of publication, some CSPs are curtailing their cloud service offerings because they are not profitable. Cloud computing service providers might eventually go through a consolidation period. As a result, CSP customers might face operational disruptions or incur the time and expense of researching and adopting an alternative solution, such as converting back to in-house hosted solutions.

Types of Risk in Cloud Computing

Types of Risks of Cloud Computing :

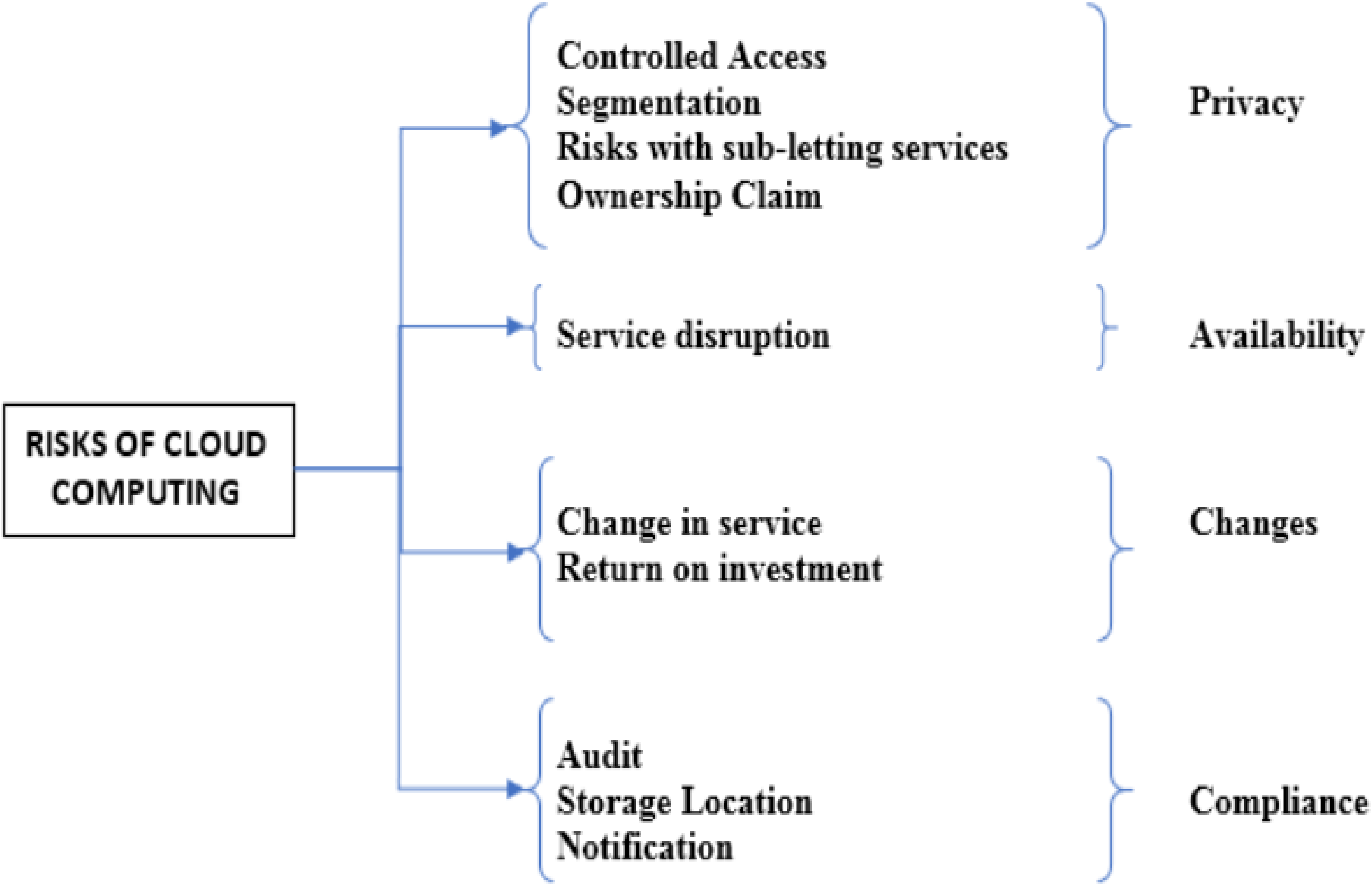
1. Privacy

All of the below risks may result from malicious activities intended for attacking private data.

Controlled Access: If the people/organization tries to store confidential data onto the cloud, the cloud’s true nature provides access to the service provider organization.

Analogous Situation: The government of Gotham city has all data as well as access.

Types of Risk in Cloud Computing



RISKS OF CLOUD COMPUTING

Controlled Access
Segmentation
Risks with sub-letting services
Ownership Claim

Privacy

Service disruption

Availability

Change in service
Return on investment

Changes

Audit
Storage Location
Notification

Compliance

Types of Risk in Cloud Computing

Segmentation: By the true nature of the subscription policy of cloud computing, there would be many subscribers, thus making the data of one organization prone to another organization.

Analogous Situation: The Gotham government's data is not properly secured, which can lead to a situation where people can know about someone else's health issues (not good to be displayed in public).

Risks with Sub-letting Services: With the growing popularity of service providing cloud computing genre, the organization's cloud services' layers are built from other service provider organizations. Thus, the contractual agreement may not be fully transparent to end customers, leaving them in blind spots.

Analogous Situation: The government of Gotham has an MoU (Memorandum of Understanding) with some other governing body, which the citizens are not aware of, thus turning a blind eye to their data usage.

Types of Risk in Cloud Computing

Ownership Claim: If the agreement is not well-read, the data's ownership can be unknowingly transferred to the service-providing organization.

Analogous Situation: If citizens don't give a careful read to the agreement, someone can have access to personal data, and there are chances that this data can be used for unlawful activities.

2. Availability

Service Disruption: This can be attributed to any fault in the internet connection as all cloud computing transactions are done over the internet. This can be either service quality degraded or outage as a whole.

Analogous Situation: The citizens depend on electricity for all their regular needs. And if there is no electricity in Gotham, the whole idea of growing the city is foiled.

Types of Risk in Cloud Computing

3. Changes :

Change in Service: Due to the volatile market, there may be acquisition or closure of a service provider, thus leading to unavailability of the service within short notice.

Analogous Situation: The government may come and go, and when they go, the data might not be available temporarily or permanently depending on the next government's plan.

Return on investment: The whole intuition behind cloud computing is to be cost-effective. But due to unforeseen circumstances, the cost of the subscription is high; it might jeopardize the whole purpose of cloud computing.

Analogous Situation: The cost of subscribing to the service is so high that the budget allocated by each citizen for these services is ending up be non-cost effective.

Types of Risk in Cloud Computing

4. Compliance

Audit: The service provider organization might not follow the external audit process, thus leading to a vulnerable position for the end customers.

Storage Location: Since the data for the services resides in hardware, and the location of that storage device is unknown, it might risk the country’s sensitive data getting leaked by rival countries.

Notification: Proper and transparent communication regarding the lack of breach to the end customer puts them at risk as they might not be aware of the havoc caused due to the same.

Data Security in Cloud

Data Security in Cloud Computing

Cloud data security is the combination of technology solutions, policies, and procedures that you implement to protect cloud-based applications and systems, along with the associated data and user access.

The core principles of information security and data governance—data confidentiality, integrity, and availability (known as the CIA triad)—also apply to the cloud:

1. **Confidentiality:** protecting the data from unauthorized access and disclosure
2. **Integrity:** safeguard the data from unauthorized modification so it can be trusted
3. **Availability:** ensuring the data is fully available and accessible when it’s needed

Data Security in Cloud Computing

Cloud computing which is one of the most demanding technology of the current time, starting from small to large organizations have started using cloud computing services. Where there are different types of cloud deployment models are available and cloud services are provided as per requirement like that internally and externally security is maintained to keep the cloud system safe. Cloud computing security or cloud security is an important concern which refers to the act of protecting cloud environments, data, information and applications against unauthorized access, DDOS attacks, malwares, hackers and other similar attacks.

Community Cloud : These allow to a limited set of organizations or employees to access a shared cloud computing service environment.

Security issues in Cloud Computing

1. Data Loss –

Data Loss is one of the issues faced in Cloud Computing. This is also known as Data Leakage. As we know that our sensitive data is in the hands of Somebody else, and we don’t have full control over our database. So if the security of cloud service is to break by hackers then it may be possible that hackers will get access to our sensitive data or personal files.

2. User Account Hijacking –

Account Hijacking is the most serious security issue in Cloud Computing. If somehow the Account of User or an Organization is hijacked by Hacker. Then the hacker has full authority to perform Unauthorized Activities.

Security issues in Cloud Computing

3. Interference of Hackers and Insecure API's –

As we know if we are talking about the cloud and its services it means we are talking about the Internet. Also, we know that the easiest way to communicate with Cloud is using API. So it is important to protect the Interface's and API's which are used by an external user. But also in cloud computing, few services are available in the public domain. An is the vulnerable part of Cloud Computing because it may be possible that these services are accessed by some third parties. So it may be possible that with the help of these services hackers can easily hack or harm our data.

4. Lack of Skill –

While working, shifting o another service provider, need an extra feature, how to use a feature, etc. are the main problems caused in IT Company who doesn't have skilled Employee. So it requires a skilled person to work with cloud Computing.

Security issues in Cloud Computing

5. Changing Service Provider –

Vendor lock In is also an important Security issue in Cloud Computing. Many organizations will face different problems while shifting from one vendor to another. For example, An Organization wants to shift from AWS Cloud to Google Cloud Services then they ace various problem's like shifting of all data, also both cloud services have different techniques and functions, so they also face problems regarding that. Also, it may be possible that the charges of AWS are different from Google Cloud, etc

6. Denial of Service (DoS) attack –

This type of attack occurs when the system receives too much traffic. Mostly DoS attacks occur in large organizations such as the banking sector, government sector, etc. When a DoS attack occurs data is lost. So in order to recover data, it requires a great amount of money as well as time to handle it.

Types of Cloud Computing Security Control

There are 4 types of cloud computing security controls i.e.

1. **Deterrent Controls :** Deterrent controls are designed to block nefarious attacks on a cloud system. These come in handy when there are insider attackers.
2. **Preventive Controls :** Preventive controls make the system resilient to attacks by eliminating vulnerabilities in it.
3. **Detective Controls :** It identifies and reacts to security threats and control. Some examples of detective control software are Intrusion detection software and network security monitoring tools.
4. **Corrective Controls :** In the event of a security attack these controls are activated. They limit the damage caused by the attack.

Importance of Cloud Security

Cloud security has a lot of benefits –

Centralized security : Centralized security results in centralizing protection. As managing all the devices and endpoints is not an easy task cloud security helps in doing so. This results in enhancing traffic analysis and web filtering which means less policy and software updates.

Reduced costs : Investing in cloud computing and cloud security results in less expenditure in hardware and also less manpower in administration

Reduced Administration : It makes it easier to administer the organization and does not have manual security configuration and constant security updates.

Reliability : These are very reliable and the cloud can be accessed from anywhere with any device with proper authorization.

Challenges of Cloud Security

Some cloud security challenges are :

1. Control over cloud data
2. Misconfiguration
3. Ever changing workload
4. Access Management
5. Disaster recovery

Advantages of Cloud Security

1. Efficient recovery –

Cloud computing conveys quicker and more exact recoveries of applications and information. With less downtime, it is foremost productive recuperation arrange.

2. Openness –

Get to your data wherever, at whatever point. A Web cloud framework increases benefit and commerce capability by ensuring that your application is constantly accessible. This takes under consideration basic participation and sharing between clients in different regions.

3. No material required –

Since everything will be encouraged within cloud, a physical stockpiling community is never once more critical. In any case, it might justify considering a support in case of a calamity that seem moderate down your business' effectiveness.

Advantages of Cloud Security

4. Preferred position –

Straightforward execution – Cloud encouraging grants an organization to keep up comparative applications and trade shapes without managing with specialized parts of back-end. Easily managed over Web, a cloud establishment is viably and quickly accessible to organizations.

5. Cost per head –

Advancement overhead is kept to a base with cloud encouraging organizations, allowing organizations to utilize additional time and resources to make strides trade system. Versatility for improvement. The cloud is successfully versatile with objective that organizations can include or subtract resources as demonstrated by their necessities. As organizations create, their system will development with them.

Disadvantages of Cloud Security

1. Bandwidth issues –

For perfect execution, clients need to arrange in like manner and not pack expansive sums of servers and capacity gadgets into a little set of information centers.

2. Without excess –

A cloud server is not one or other overabundance nor reinforced. Since development can bomb to a awesome degree, go without from getting seared by buying an overabundance course of action. Whereas this can be an additional cost, much of time it is defended, in spite of all inconvenience.

3. Data transfer capacity issues –

For idealize execution, clients ought to plan moreover and not gather colossal amounts of servers and capacity contraptions in a small course of action of server ranches.

Disadvantages of Cloud Security

4. More control –

At the point once you move organizations to cloud, you move your data and information. For organizations with insides IT staff, they won't have choice to bargain with issues all alone. Be that because it may, Stratosphere Systems has an all day, each day live helpline that can address any issue right absent.

5. No Redundancy –

A cloud server isn't excess nor is it supported up. As innovation may fall flat here and there, maintain a strategic distance from getting burned by obtaining a excess arrange. In spite of fact that it is an additional taken a toll, in most cases it'll be well worth it.

Cloud Digital Pesonas and Data Security

Here are four areas where personas are important in optimizing your digital strategy.

1. Sharing knowledge between teams

Consistency is key. For consumers, every interaction is all one experience with your brand, online or offline. Every part of your business needs to be singing from the same song sheet – and personas can help you do that.

From marketing to sales, customer service to stakeholders, having a shared understanding of who you’re engaging with, and in what way, can make sure marketing and digital efforts work toward common goals.

Cloud Digital Pesonas and Data Security

2. Enabling design and testing

It’s not just your messaging that can benefit. User experience and design can be improved with persona research and effective testing.

A brand that has a clear picture of their target personas can ensure sites, experiences, landing pages, and direct communications are designed in a way that helps move the customer through their journey. If you know your personas are often on-the-go, for example, you’ll want to take a mobile-first approach to design.

When it comes to testing the accuracy of your personas, you could A/B test a range of interaction designs across certain persona groups. Consider the mobile-using persona example above. You could test various responsive website designs and see whether or not how consumers interact in real-life really reflects your understanding. If this testing reveals something unexpected, you can then adapt the experience.

Cloud Digital Pesonas and Data Security

4. Supporting campaign creation

You’re starting a new campaign. You know the audience you want to target. How can you make sure your content resonates? And where should you place ads to get the most “bang for your buck”? Having detailed personas will help you answer these questions.

Content that engages will speak to your customers’ needs or pain points. It will answer the different questions your target audience has as they move through their buying journey. Look to your personas to discover and focus on those needs. For example, you may have one persona that outlines an IT buyer. They are aware of your products, understand the industry, and are looking to lead the way when it comes to innovative technology.

Alternatively, you may have another graphic designer persona that is currently at the discovery stage of the customer journey. The content you create for the IT buyer won’t be relevant for this second persona

Cloud Digital Pesonas and Data Security

3. Supporting segmentation and targeting

You’ve created your messaging and tailored your designs. You’ll also want to use personas to map your segmentation and targeting.

While we know that every customer has a unique journey and they’ll have landed on your site from various routes and for different reasons, having clear personas helps you first identify and then refine different segments. Showing content to your target audience based on specific behaviors and intentions that you’ve mapped out helps you deliver appropriate messages to the right people.

Content Level Security

Message content is a significant attack vector used by malicious API consumers. API Services provides a set of Policy types to mitigate the potential for your backend services to be compromised by attackers or by malformed request payloads.

Content-based security, also known as asset-based security, is a gerneral term for security features that are embedded

Cloud Security Services

Cloud Security Services

1. Identity and access

You are provided with control for secured management of identities and access. It includes people, processes and systems used for managing access to your enterprise resources. It is managed by making sure that the identity of the user is verified and the access rights are provided at the correct level.

2. Data loss prevention

This service offers protection of data by providing you with pre-installed data loss prevention software, along with a set of rules deployed.

Cloud Security Services

3. Web security

Web security is provided as an additional protection against malware from entering the enterprise through web browsing and other such activities. This cloud service is provided either by installing a software or an appliance or through the cloud by redirecting your web traffic over to the cloud provider.

4. E-mail security

It provides control over the in-bound and out-bound e-mails to protect your organization from malicious attachments and phishing. This cloud service helps enforce corporate policies such as acceptable use, spam and in providing business continuity options. One of the solution adopted by many cloud e-mail security services is digital signatures, which allows identification and non-repudiation.

Cloud Security Services

5. Security assessment

There are various tools implemented for the users of the SaaS delivery model, such as variant elasticity, low administration overhead, negligible setup time and pay-per use with low investment in the initial stage.

6. Intrusion management

It is the process that uses pattern recognition for detection and reaction to events that are statistically unusual and unexpected.

It may also require reconfiguration of your system components in real time so as to prevent an intrusion.

7. Security information and managing events

Your system gathers information related to log and events. This information is used in correlating and analyzing, to provide you with real time reporting and alerts on events that require intervention.

Cloud Security Services

8. Encryption

There are typical algorithms that are computationally difficult or nearly impossible to break.

9. Disaster management

This cloud service helps in continuing your business and managing disasters by providing flexibility and reliable failover for services that are required in case of service interruptions.

10. Network security

The network security services provides you with address security controls, which in a cloud environment is generally provided through virtual devices

Secure Cloud Software Requirements

(1)The method of access to the cloud

(2)The architecture of the cloud, and

(3) The features of the multi-tenant environment.

Secure Cloud Software Requirements

1. The method of access to the cloud :

First, usually cloud environments are accessed by the CSUs through a web application in which often is deemed the weakest point of CC. This is because the current browser based authentication protocols for the cloud are not secure, due to browsers' inability to issue XML based security tokens by itself. In technical solutions to overcome those obstacles are proposed, e.g. by encrypting data, while it is stored under the custody of a cloud service provider or while it is transmitted to a CSU

Secure Cloud Software Requirements

Second, regarding the architecture of the cloud, one of biggest challenges is that of virtual machine (VM) instance interconnectivity. A key concern in virtualization is isolation, which guarantees that one VM cannot affect another VM running in the same host. When multiple VMs are present on the same hardware (which is common for clouds), one VM could be illegally accessed through another VM. A solution to prevent this is the Virtual Network Framework which consists of three layers (routing layer, firewall and shared network) and aims to control the intercommunication among VMs deployed in physical machines with higher security

Secure Cloud Software Requirements

Third, requirements should be aligned to the specific context of the multi-tenant environments in order to avoid the possible problems caused by role name conflicts, cross-level management and the composition of tenants' access control. Solutions that address these requirements are the SaaS Role Based Access Control (S-RBAC) model, the reference architecture defined in, and the reference architecture encompassing the concept of “interoperable security”. These solutions help one to differentiate between a 'home cloud' and a 'foreign cloud'. The 'home cloud' is a CSP which is unable to meet demand with its current resources and, therefore, forwards federation requests to ‘foreign clouds’ with the purpose to exploit their virtualization infrastructures.

Cloud Based Software Testing

Cloud Testing is one type of software testing in which the software applications are tested by using cloud computing services. Cloud testing intends to test the software based on functional and non-functional requirements using cloud computing services that ensure faster availability, scalability, and flexibility that saves time and cost for software testing.

Cloud Based Software Testing

Cloud-based software testing is a set of procedures, tools, and processes that are leveraged by testers inefficiently and precisely testing software. With the utilization of Cloud service models, enterprises can implement testing as a service, without the need to completely invest in testing labs, tools, or infrastructure. Cloud services deal with not just testing but also everything from cloud security, software development, resource utilization, etc.

Without a proper test, the software will always be vulnerable to threats, errors, security breaches, and many more factors that will significantly affect customer experiences. Therefore, while selecting a test tool, infrastructure, or automation service from the cloud, testers must completely understand its platform compatibility, resource support, flexibility, and service cost. Completely ingraining QA, at multiple phases of cloud adoption and administration, must be an overriding mandate.

Cloud Based Software Testing

This means enterprises must carry out robust QA planning and stipulation to guarantee that the Cloud services cover the entire test automation process successfully. Moreover, enterprises must be keenly conscious of the growing levels of regulatory scrutiny of Cloud technology. Clients anticipate seeing proof that enterprises have fully completed and implemented cloud-based software testing strategies for data, flexibility, and application exit.

Benefits of Cloud-Based Software Testing

1. It significantly reduces the expenses and the process cycles by sharing the resources when the testing strategy is performed. This is because cloud-based Testing as a Service (TaaS) enables IT and software developers to initialize practical experimental tests on cloud platforms without the necessity to possess licenses or purchasing the resource. This reduces the expenses of testing and improves sharing of resources and the use of services.

2. Better testing environment of testing and virtual infrastructures. The flexibility of cloud technology enables enterprises to leverage TaaS from any part of the globe as long as the place has a good internet connection. Also, the cloud provides a better virtual environment for testing and SaaS solutions that support the entire testing life cycle, including development. With these virtual infrastructures, enterprises will not have to spend a lot on real labs or traffic generators but just lease the resources from the cloud.

Benefits of Cloud-Based Software Testing

3. The Pay per use policy of cloud services is the most notable factor for enterprises. As opposed to traditional software testing, in cloud-based software testing, enterprises can choose the resource, tools, or technologies for just the time they need. They will have to only pay for the service based on the utilization time and can stop leveraging cloud services once the testing is complete.

Note : The majority of the IT companies and software developers are now migrating their legacy systems to a cloud ecosystem for better test automation services. With cloud-based testing, their applications are scalable, flexible, and easily adaptable. Here are some reasons why enterprises are adopting cloud-based software testing over traditional or manual application testing.

REFERENCES

1. https://www.educba.com/risks-of-cloud-computing/

2. analyticssteps.com/blogs/8-pillars-risk-management-cloud-computing

3. https://www.researchgate.net/publication/307899076_Risk_Management_Framework_for_Cloud_Computing_A_Critical_Review

4. https://reciprocity.com/blog/enterprise-risk-management-for-cloud-computing/

5. https://www.consultia.co/wp-content/cache/page_enhanced/www.consultia.co/enterprise-risk-management-for-cloud-computing/_index.html_gzip

6. https://www.sitecore.com/knowledge-center/blog/2020/11/the-importance-of-personas-for-digital-experience

7. https://www.rishabhsoft.com/blog/10-categories-of-security-services-offered-over-the-cloud

8. https://www.researchgate.net/publication/261038126_Cloud_computing_security_requirements_A_systematic_review

9. https://blog.thundra.io/what-is-cloud-based-software-testing-and-how-can-it-enhance-testing-services

THANK YOU!!!

My Blog : https://anandgharu.wordpress.com/

Email : gharu.anand@gmail.com