Assignment - 1

Q1. List and explain in detail types of risks on CC.

Ans. Types of risk on CC:

1. Misuse and illicit use of cloud computing:-
- Unregistered individuals may take advantage of the befitting registration, straightforward methods and somewhat anonymous access to cloud services to launch diverse attacks.
- eg: DDOS, password and key breaking.

2. Insecure interfaces and APIs:-
- Customers organize and combine with cloud services through interfaces or APIs.
- Targets are Iaas, Paas, Saas.

3. Vicious insiders:-
- Vicious insiders represent a larger risk on a cloud computing environment, since clients manage not have a clear outlook of providers principles and procedures.

4. Issues related technology sharing:-
- Iaas is based on distributed infrastructure, which is often not conceived to accomodate a multi-tenant architecture.

5. Data loss or leakage:-
- Compromised data may encompass deleted or changed data without producing a backup.
- eg: review (AAA) controls, authorization

CLASSMATE
Date :
Page :

6. Hijacking (Account / Service)
- Account or service hijacking is generally carried out with pilfered credentials.
- Targets are: IaaS, PaaS, SaaS

Q2. Write a short note on data security advantages, disadvantages and challenges on CC.

Ans.

→ Advantages:-

1. Data centralization:-
- In a cloud atmosphere, the service provider takes responsibility of storage and small organizations need not spend more money for personal storage devices.

2. Incident response:-
- IaaS providers contribute dedicated logical server which can be used on demand.

3. When there is a server, a backup of the environment can be effortlessly made and put up on the cloud without affecting the usual course of business.

4. Forensics or image verification time:
- Some cloud storage implementations reveal a cryptographic assertion addition or hash.

5. Logging:
- In a cloud, storage requirement for benchmark logs is mechanically solved.

→ Disadvantages:-

1. Investigation:-
- Investigating an illegal undertaking may be unrealistic on cloud environments.

2. Data segregation:
- ~~Data~~ Some clients may not decide to encrypt data because there may be a case when encryption misleads can decimate the data.

3. Long-term viability:-
- Service providers should double-check the data security on altering enterprise positions, such as mergers and acquisitions.

4. Compromised servers:-
- If a server is compromised, we require to shut down the servers down until they get a backup of the data.

5. Recovery:
- Cloud service providers should double-check the data security in natural and man-made disasters.

→ Challenges:-

1. Data breaches:-
- Resulting from misconfigurations, week access controls, or inadequate encryption.

2. Poor identity and access management (IAM):-

- Inadequate IAM, practices including weak passwords, insufficient monitoring, etc.

3. Weak cloud configurations :-
- Misconfigured cloud environments, such as public access to private data or failing to configure network settings.

4. Cloud misconfigurations :-
- Misconfigurations, such as public access to cloud storage buckets.

5. Insider Threats :-
- The risk of malicious or accidental actions by employees, contractors, or third-party vendors.

Q 3. Explain in brief cloud digital persona.

Ans. Cloud computing supports rapid, cost-effective app. deployment but introduces concerns about security, privacy, and compliance.
- Data protection must be enforced across all platforms with layered security.

→ Security Levels for cloud data:

1. Level 1:
- Encrypt data during transmission using secure protocols (eg: HTTPS).

2. Level 2:
- Restrict access to documents, but content is not encrypted.

3. Level 3:

CLASSMATE
Date :
Page :

- Add content encryption along with access control to secure sensitive data.

4. Level 4:

- Includes all level 3 protections plus advanced controls like admin rights, watermarking and content redaction.

→ Data protection needs:-

- Data must be protected across all environments - desktops, networks, mobile devices, and cloud platforms.
- As data often flows through collaborative and complex workflows, consistent security across all touchpoints is essential.

Q4. Discuss secure cloud software requirements and examples of tools / platforms for cloud software testing.

→ ~~Cloud software requirements~~

Ans. When enterprises take up cloud computing and establish databases on virtual environments, they run the risk of revealing highly-sensitive data to internal and external attacks.

- The outsourced environment of the cloud and inherent lors of control proceeds along and hence perceptive data should be mind fully supervised to double-check that it is inherently protected.
- To further complicate things, ensuring double check that it is inherently protected.
- Virtualization and cloud computing lend larger flexibility and effectiveness by giving you the proficiency

to proceed reviews and add or eliminate assets.

→ Software testing tools / platforms for computing:-

- ~~New open~~ with ~~goog~~ google documents, Flickr, Buzzword and Zoho as examples of general purpose applications that use cloud computing technology it is only a matter of time before cloud computing is seen as the most viable option for application development and deployment.
- Visual Testers Tools for open source software testing tools and accepts encompassing a dedicated cloud computing testing tools
- CloudTools and PushToTest are the test methods which comprises of products that will help the future of evolved cloud-based software testing ~~&~~ functions.