**CSW105 – PARALLEL AND DISTRIBUTED COMPUTING**

**Hiquiana, Al Cedric S.**

**BSCS 4A**

**20180397-C**

**Cloud Computing**

1. Suggest two hardware mechanisms and software schemes to secure the application cloud (SaaS), the infrastructure cloud (IaaS), and the platform cloud (PaaS). Discuss their specific requirements and difficulties and limitations that may be encountered.

* **SaaS**

SaaS (software as a service) is a cloud computing service that gives consumers access to a vendor's cloud-based software. The program does not need to be installed on the user's PC. Instead, the program is accessed via the web or an API that is hosted on a distant cloud network.

**Security issues and solutions in SaaS:**

* Mechanism to allow users to utilize a single set of credentials - this technique saves money by lowering the amount of support required from IT help desks. Furthermore, if a new user enters or quits the organization, there is only one password to activate or deactivate, as opposed to dealing with several passwords.
* Different instances operating on the same physical system must be segregated from one another. This necessitates the deployment of Reconfigurable distributed virtual machines.
* **IaaS**

IaaS (Infrastructure as a Service) is a cloud computing service that gives consumers access to computational resources such as storage, networking, and servers. Users employ their own platforms and applications within the infrastructure of the service provider.

**Security issues and solutions in IaaS:**

* **Data Encryption and Network Encryption** : IaaS providers must never be able to gain access to virtual machines and customer data.
* **Vulnerability Control**: Implementing and using vulnerability control, together with regular software updates, can significantly reduce the risks associated with information security,​​​​​​​
* **Cloud access security broker (CASB)** : it provides a variety of security services, such as monitoring unauthorized cloud services, enforcing data security policies, data loss prevention and many others.
* **Cloud security gateway (CSG) :** It provides visibility and control over cloud resources . It also provides auditing and monitoring of security settings and configurations
* **PaaS**

Platform as a service is a cloud computing offering that provides customers with a cloud environment in which they may build, manage, and distribute web applications. This strategy is used to enable the efficient and speedier creation of Web applications by lowering the complexity of software and infrastructure.

**Security issues and solutions in PaaS:**

* **Cloud security posture management (CSPM) :** A security posture manager continuously audits the cloud environment for security and compliance issues
* **Cloud workload protection platforms (CWPP) :** CWPP services also apply malware protection and simplify security management across multiple PaaS environments.
* **Cloud access security broker (CASB) :** it provides a variety of security services, such as monitoring unauthorized cloud services, enforcing data security policies, data loss prevention and many others.

2. Consider two cloud service systems: Google File System and Amazon S3. Explain how they achieve their design goals to secure data integrity and to maintain data consistency while facing the problems of hardware failure, especially concurrent hardware failures.

* To ensure the integrity and consistency of the data, such cloud services always incorporate a recovery and backup strategy in their architecture. They backup the data on a regular basis, and if there is a hardware failure or concurrent hardware failure, the restoration is done using the backed up data. As the backups that are saved are likewise encrypted, it does not impair the service to the users and also protects the integrity and consistency of the data.

3. Describe the following techniques or terminologies used in cloud computing and cloud services.

**a. Virtualized data center**

* A virtual data center has the same capabilities as a regular data center, but it uses cloud-based resources instead of physical resources. It enables a company to deploy new infrastructure resources as needed without the requirement for obtaining, deploying, configuring, and managing physical appliances.

**b. Green information technology**

* Green IT (green information technology) is the practice of computing that is ecologically friendly. Green IT seeks to reduce the negative environmental effect of IT operations by designing, producing, running, and disposing of computers and computer-related items in an ecologically responsible manner.

**c. Multitenant technique**

* Multi-tenant architecture, often known as multi-tenancy, is a software architecture in which many instances of the same software operate on a single physical server. Following that, the server serves numerous tenants.