ASSIGNMENT 2 FRONT SHEET

Qualification	**BTEC Level 5 HND Diploma in Computing**		
Unit number and title	Unit 9: Cloud Computing		
Submission date	10/05/2019	**Date Received 1st submission**	
Re-submission Date		**Date Received 2nd submission**	
Student Name	Nguyen Phuong Thao	**Student ID**	GCH17640
Class	GCH0701	**Assessor name**	Do Quoc Binh

Student declaration

I certify that the assignment submission is entirely my own work and I fully understand the consequences of plagiarism. I understand that making a false declaration is a form of malpractice.

Student's signature	

Grading grid

P5	P6	P7	P8	M3	M4	D2	D3

This page is intentionally left blank

Contents

1. Most common problems of cloud computing platform and solutions

1.1 Network issues of cloud

Cloud networking is the basic foundation for providing cloud services and the reason for the shift in how users are provided with IT services. This part focuses on a number of issues facing cloud networking.

Availability

One of the difficult challenges facing an organization of a cloud provider is to provide maximum uptime for the services provided to users. Even a few seconds of downtime can cause the organization to end up losing reputation and impact the business as a whole. Furthermore, downtime may result in a breach of service-level agreements (SLAs) between the cloud user and the cloud provider, affecting the revenues of the cloud provider to a large extent. (Chandrasekaran, 2014).

=> Solution: Replicating the data and taking regular backups is the most widely adopted approach to achieving high availability and reduce the recovery time.

Poor Network Performance

High burst tolerance, low latency, and high throughput are the three basic performance requirements of a Cloud Network. This is because trafficking in a data center includes a mix of all three types of trafficking: mice trafficking, cat trafficking, and elephant trafficking, each with a different performance requirement.

The main challenge is that the traditional Transmission Control Protocol / Internet Protocol (TCP / IP) stack, designed primarily for Internet-like scenarios, does not deliver optimum performance in Cloud Networks (Chandrasekaran, 2014).

=> Solution: The primary objective of TCP with GIP. This can enhance network performance in terms of great performance by reducing the total number of timeouts. Timeouts lead to serious network performance destruction and affect the perceived lag of the user. TCP publishers with GIP concentrate on preventing two types of network timeouts: timeouts due to the loss of full packet window, full window loss timeouts (FLoss-TOs), and timeouts due to the absence of ACKs, lack of ACKs timeouts (LAck-TOs).

Advantages: In a wide variety of scenarios, including with and without the background UDP traffic, TCP with GIP achieves nearly zero timeouts and higher quality. In addition, TCP's scalability with GIP is much more than any TCP variant, it scales well up to 150 worker nodes in parallel.

1.2 Less control and flexibility

Because the cloud infrastructure belongs to CSP, customers have a limited control with their system.

The cloud computing system is developed by developers from CSP, so any function or implementation of the service depends on CSP and customers will find it difficult to fully customize and monitor the system(Larkin, 2018).

=> Solution:

- Customers should spend time on studying basic knowledge of their cloud system so that they can detect problems by themselves and minimize their dependences on CSP.
- Customers and CSP must understand clearly their own responsibilities so that when there is any failure in the system, they don't have to wasting time to blame for and shifting the responsibilities onto each other.

2. Most common security issues in the cloud environment and solutions

2.1 Physical security risks

Firewalls and encryption are not enough for protecting the CSC data because data loss still happens if the unauthorized onsite access attacks the physical location of cloud data centers (Worlanyo, 2015).

=> Solution: This can be reduced by enhance the physical security protection such as bodyguards, cameras, alarm systems, smart lock, biometric scans to make sure all access to the physical assets are authorized.

2.2 Technological Security risks

This includes failures relating to hardware, technologies, and services provided by CSPs (Worlanyo, 2015).

=> Solution: According to Worlanyo (2015), CSP can use 'an Advanced Cloud Protection system (ACPS) to ensure the security of guest virtual machines and of distributed computing middleware. Behaviour of cloud components can also be monitored by logging and periodic checking of executable system files'.

2.3. Compliance and audit risks

These are risks relating to laws including lack of jurisdiction information and adhering to regulatory guidelines (Worlanyo, 2015).

=> Solution: Both CSP and CSC need to have the thorough insights into legal and regulatory obligations so that any contracts between them are all legal and meet these obligations.

2.4 Organizational risks

There are two main types of these risks. First, there could be malicious personnel in the organization who want to do harm to CSC's data. Second, if a CSP are no longer in the business or controlled by other business, its CSPs may be affected badly because SLA

of these CSPs may be changed and have to be migrated to another CSP that is closer to their needs (Worlanyo, 2015).

=> Solution: This risk mainly comes from the malicious people in the organization, so it can be reduced by enacts more strict rules and principles when a company hires new staff. Moreover, there could be a third party that is responsible for assessing and monitoring the CSP, as well as the usage of security breach notification process.

2.5 Data security risk

- Privacy: because database is on cloud and can be accessed over the internet, there is a high likelihood that personal information from CSC is taken by attackers. This risk is the most important especially with CSC that stores sensitive data. This is also a difficult problem because of multitenency. Most service providers use virtualization, thereby, multiple users access to the same database hardware. In the result, it is easier for attackers to access to host and virtual machine to get data (Worlanyo, 2015).
- Integrity: there is a risk of data being changed by unauthorized users, which can causes unexpectedly harm to CSC (Worlanyo, 2015).
- Availability: CSC can be banned from accessing their data because of some attacks such as DDos or simply the errors in system provided.
  => Solution:
    - ✓ Authentication: authorizing carefully any access can considerably minimize the risk of data theft. This could be implemented by both CSP and the third parties. These are some methods of authentication such as SAP or IBHMCC.
    - ✓ Encryption technique: this is an algorithm used to transform plain text into encrypted text (cipher text) so hacker and unauthorized users can not view the information. A key is created to decrypt the cipher text. This is one of effective algorithm:
        - ➢ Caesar Cipher: this is a classical encryption where each letter in plaintext is replaced with a letter whose position is moved ahead or aback that letter by fixed times. For example, a fixed shift number is 3, so D is now A, Z is now W, Q is now M and so on.

3. Security problems and solutions to ATN

- Limited control: Not ATN, CSP owns technology, hardware, and services of cloud computing. Moreover, ATN has never had a cloud expert in their organization, so the performance of this cloud service depends a lot on CSP that. Therefore, anytime there is a failure of system or downtime, ATN has to rely on CSP to fix.

=> Solution:

- ✓ ATN should hire a cloud expert or even third-party company to regularly monitor their cloud's working.
- ✓ ATN needs to have a back-up plan for any expected disaster or failure caused by CSP's technology.

- Technology Security Risks: this problem mainly comes from CSP because CSP provides technology, hardware, and service, etc. used to build this system.

  => Solution:

  - ✓ ATN has to ensure that the CSP that they work with is professional and reputable for their technology.
  - ✓ Moreover, ATN can also require CSP to monitor their system's activities daily and separate domains name for providers and customers. There will be a trust agent – a third party that collects security information used to verify at endpoint for each domain.

- Compliance and Audit Risks: this is the first time that ATN integrates cloud computing with current system, so this company doesn't have experiences in regulation. Therefore, ATN may not see clearly problems hidden in their contract with CSPs.

  => Solution:

  ATN must study thoroughly the regulation of security (data privacy, technology, etc.) and consult carefully with CSP. During their consultation ATN can hire the third party to monitor and make a judgment for terms and conditions in the contract.

- Physical security risks: physical infrastructure could be still damaged by natural disaster or malicious attackers (both inside and outside the company).

  =>Solution:

  ATN should enhance its physical location by hiring armed body-guards, adding smart key lock, or tighten the principles of recruiting new employees (to prevent *malicious people from attacking physical location)*.

4. References

Chandrasekaran, K., 2014. *Essentials of Cloud Computing*.

Larkin, A., 2018. *Disadvantages of Cloud Computing*. [Online] Available at: https://cloudacademy.com/blog/disadvantages-of-cloud-computing/ [Accessed 2019].

Worlanyo, E., 2015. *A Survey of Cloud Computing Security: Issue, Challenge and Solutions*. [Online] Available at: https://www.cse.wustl.edu/~jain/cse570-15/ftp/cld_sec.pdf.

❒ **Summative Feedback:**	❒ **Resubmission Feedback:**	
Grade:	**Assessor Signature:**	**Date:**

Internal Verifier's Comments:
Signature & Date: