

COMP 7530 Writing assessment Part 2

Seminar topic: “The Evolution of Data Centers in Digital transformation”

Student Number: _____ 15451682 _____

Student Name: _____ CHEUNG Saiho _____

Program: _____ MSc AIS _____

In the September of 2011, the cloud computing model has proposed by the U.S. National Institute of Standards and Technology (NIST). It is a huge evolution for changing the traditional datacenter infrastructure model, this evolution has involved in the data transformation of the traditional business model.(Mell &Grance, 2011) There has disrupted all the existed business processes to transform the new e-commerce model when they have entered for the digital generation.

In this seminar, the speaker is Mr. Eric HUI who is the director of business development in emerging ecosystems, Equinix Asia Pacific. The topic of speech is 'The Evolution of Data Centers in Digital transformation'. The speaker has mainly focused on talking about the four main benefits of using the cloud computing technology to compare with building the traditional datacenter for companies, including on-demand network access, scalability, availability and minimal IT management effort for internal.(Armbrust et al., 2010) There have elaborated some idea of the cloud computing security issues and the development trend of Internet Of Things (IoT) in the future. Basically, the speaker has explained the fundamental concept of three mainstream cloud computing models, including Software as a service (SaaS), Infrastructure as a service (IaaS) and Platform as a service (PaaS). The SaaS is providing software service for customers used, for example, Gmail service. The IaaS is providing software development tools and application programming interface (API) for customers used, for example, Google Apps engines. The PaaS is provided to allocate the hardware resources for customers used, for example, Rackspace. (Liu et al., 2011)

For the part of digital transformation in existing business model, the speaker has given some successful cases for using the cloud computing platform and expand their market share to the global, such as Pizza Hut, Food Panda and Uber. As the fast food restaurants have launched the mobile apps, they do not need to walk into the food store to make an order, because the mobile apps must be retrieved the food menu and online payment system by the cloud service provider. Thus, the restaurants can reduce the cost in physical restaurants and manpower resources of operational staff. In this case, there can be fulfilled the two main benefits for using cloud services which is followings the on-demand network access and scalability. As the cloud computing platform is shared the pool of servers and internet lease line connection, the restaurants can expand or reduce the usage of IT hardware resources during the different period of time, it is more flexible to fulfil the business needs. For example, the restaurants must need to increase the network capacity and processing power for amount of customer order requests during the

lunch and dinner time, instead of increasing the number of restaurants only. Moreover, the company has released the web service or mobile apps, the traditional datacenter is needed to add the new service manually, it is a high cost for the configuration of IT system. However, the cloud computing can scale this service on-demand. (Garrison, Kim, & Wakefield, 2012)

The main advantage of Uber app is matching customers and taxi drivers in the shortest distance via GPS location which provides the Google map. There can be reduced the idle time and petrol fee by every taxi, it has increased the income for each driver. Certainly, the matching system has analysed a large volume data of GPS location for the customer and taxi driver which is according to the shortest distance. It has involved a huge data processing power in the datacenter and appropriated for using the cloud computing platform, instead of purchased the single server can fulfil all network requests. In this case, there can be fulfilled the other two main benefits for using cloud services which is followings the availability and minimal IT management effort. According to the Uber is an international taxi calling service company, it has used the cloud computing service to reduce the system downtime and maintenance cost during IT infrastructure failure, it can be automated recovery to the multiple datacenters by the service provider. Thus, the availability is a higher than the traditional datacenter, because the companies need to invest an amount of money for updating IT infrastructure and hiring IT teams support frequently when they have built the datacenter in different cities. However, the rental cost of cloud computing service is paid the fixed annals fee, it can be terminated the service contract when the companies do not need.

For the part of cloud service security issues, most of business companies have used the cloud service for business growth more elastically. However, the speaker has concerned the security issues of data protection when the data has stored in cloud servers. As these system providers have not promised the customer's data in safety, there can be stolen, duplicated and modified by the hackers illegally, it seems like the case of Apple iCloud, this platform provides the web storage for the customers when they can upload their digital media files. Unfortunately, the hackers have stolen the amount of famous international movie star's photographs and system login account information for triggering DDoS attacks for the past years ago. Hackers have sold these photos to the entertainment media when they have made a huge of money, but no one need to be responsible for the customers' data leakage.

Certainly, the speaker has suggested that everyone should have thought about which kind of images

can be uploaded in iCloud, especially private life images. As this platform belongs to the public cloud service, every user can access it and easy to leakage the storing data by the hackers during network attacks. In this case, the Apple company should consider using the hybrid cloud service model for increasing the security level. It seems like the Netflix company which is providing the online video playing service. The hybrid cloud service model is separated in two parts, the private cloud server is processing all the sensitive data which is including the membership and billing payment system, the public cloud server is providing the online video service for customers. As the private cloud server should not be accessed by the public network and need to connect it via VPN, the hackers cannot steal this sensitive data easily, including customer personal and bank account information. (Carroll, van derMerwe, &Kotze, 2011)

Consequently, the author has agreed with the speaker's viewpoints. The cloud computing service can be reduced the IT infrastructure investment for business expanding by the companies. However, it is not appropriated in all cases exactly, especially software development company. On the other hand, most of people have used the smart phone for their daily life, such as bank service, business activities. Thus, the security issues of mobile computing are the most important topic in IT security. (Bahl, Han, Li, &Satyanarayanan, 2012) The author has proposed four suggestions for improvement which is shown as below:

Firstly, users should not install the untrusted apps in the third parties website, some people want to download the mobile apps in the apps store without paid money when they have installed the backdoor program to unlock some functions in the kernel of mobile operating system. It is the extremely high risk for their phone, because this program must be embedded some malicious code or malware by the hackers. They can steal the victim data in silence which is including the phonebook, Apple iCloud login account and message records. On the other hand, users should need to keep updated the latest version of anti-virus software and operating system. (Suo, Liu, Wan, &Zhou, 2013)

Secondly, many people have used the free wireless network access point (Wifi hotspot) for public area in Hong Kong, they can watch the movie, play game and interact with the social network platform which is reduced their usage of mobile data capacity in 4G network plan. The hackers can easy to capture the other people network transmission data when the hotspot has not implemented the data encryption technique during data transmission, such as Wi-Fi Protected Access (WPA). Besides, users should need to turn off the

functions of blue tooth connection and file sharing, it can be prevented easy to leakage their storing data in smart phone by hacker.

Thirdly, the software development company is focused on producing the different kinds of software, mobile apps and system integration projects, such as R&D development of Microsoft company. It must not be appropriated to rent the hybrid cloud system model for replacing their existed datacenters. As no any cloud service providers can be provided the latest version of Microsoft development tool and API libraries, it is not fulfilled for the whole system development stage. For example, Relations database management system cannot be adopted by Google NoSQL database system, this is a typical system compatibility problem. On the other hand, most of cloud service providers is provided the virtual machine to the clients without special request, instead of physical server. It may involve some system vulnerable, but the clients cannot complain as they are not a system owner. (Zhang, Cheng, &Boutaba, 2010)

Fourthly, the cloud service providers are lack of well define the service layer agreement and clear description of system security performance for the clients. For example, how to destroy the client's data when they have terminated the service contract, how to propose the data recovery plan when the cloud system has suffered from hacker attacks or natural disasters. Besides, the client data is very difficult to move the other providers, it may be enforced for using the existing cloud service.

Therefore, the critical and developing systems are not appropriated for running in the cloud system, it has a very high risk. In this case, the author is suggested for using the traditional computing model when the company has implemented for these kinds of systems.

For the part of development trend IoT, the speaker has proposed some examples for IoT devices, such as health care alarm for elderly, smart wearable devices and smart car. These devices have collected some useful data from the users and sent to the back-end servers for doing some tasks of data analysis, the purpose is made the best of decision which is implemented the big data technique. (Riahi, Challal, Natalizio, Chtourou, &Bouabdallah, 2013)

According to the IoT devices have embedded the network sensors for data transmission, the author has concerned for data privacy and encryption during data collection, otherwise the data may be used in the wrong way or leakage to the third party for using in the illegal purpose. As these devices have collected a huge amount of data from time to time, users may not agree with it, or even do not know what kind of

information has sent it out to the back-end cloud systems via wireless network. Thus, the author has proposed two suggestions for the issues of data security and privacy in smart car chase.

The most of smart cars have embedded the automatic guidance system when the driver does not need to control their car in the highway, it can be prevented many car accidents and protected the human life in safety by the system. However, the guidance system has not encrypted the car routes information during data exchanging with servers. The hackers can easily sniff the information which is including the GPS location and car speed, or even remote control the car when the hackers have hacked the systems via wireless network. The system company must consider how to enhance the security level in this device for avoiding of the extremely dangerous cases.

Firstly, the car of IoT device has connected to synchronize GPS location in the remote system of automatic guidance functions via virtual private network (VPN), it has used the security tunnel for data encryption on both sides. As the network packets have been encrypted during network transmission, the hackers cannot capture and read them more easily. In addition, the devices should have set the session key or password for the users, they have a responsibility of changing password frequently and must do not use the default password only.

Secondly, users should need to read the terms of use in the devices very carefully when they have determined to purchase and use it before. They should focus on whether has collected too much privacy, data without necessary and keep it in confidentiality from the servers. (U.Farooq, Waseem, Khairi, &Mazhar, 2015) For example, the automatic guidance system should not be captured the photographs of inside car and driving record of the system company. Users should make a right choice for their actual needs, instead of just for fun.

In conclusion, the cloud computing service is very critical the key success factor for business growth. However, the companies should need to consider the security issues and system risks when they have stored data on it, otherwise it may be becoming a time bomb.

Bibliography:

- Armbrust, M., Stoica, I., Zaharia, M., Fox, A., Griffith, R., Joseph, A. D., ...Rabkin, A. (2010). A view of cloud computing. *Communications of the ACM*, 53(4), 50. <http://doi.org/10.1145/1721654.1721672>
- Bahl, P., Han, R. Y., Li, L. E., &Satyanarayanan, M. (2012). Advancing the state of mobile cloud computing. *Proceedings of the Third ACM Workshop on Mobile Cloud Computing and Services - MCS '12*, 21. <http://doi.org/10.1145/2307849.2307856>
- Carroll, M., van derMerwe, A., &Kotze, P. (2011). Secure cloud computing: Benefits, risks and controls. *2011 Information Security for South Africa*, 1–9. <http://doi.org/10.1109/ISSA.2011.6027519>
- Garrison, G., Kim, S., &Wakefield, R. L. (2012). Success factors for deploying cloud computing. *Communications of the ACM*, 55(9), 62. <http://doi.org/10.1145/2330667.2330685>
- Liu, F., Tong, J., Mao, J., Bohn, R., Messina, J., Badger, L., &Leaf, D. (2011). NIST Cloud Computing Reference Architecture Recommendations of the National Institute of Standards and. *NIST Special Publication 500-292*, 292(9), 35. Retrieved from http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909505
- Mell, P., &Grance, T. (2011). The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology. *National Institute of Standards and Technology, Information Technology Laboratory*, 145, 7. <http://doi.org/10.1136/emj.2010.096966>
- Riahi, A., Challal, Y., Natalizio, E., Chtourou, Z., &Bouabdallah, A. (2013). A systemic approach for IoT security, 351–355. <http://doi.org/10.1109/DCOSS.2013.78>
- Suo, H., Liu, Z., Wan, J., &Zhou, K. (2013). Security and privacy in mobile cloud computing. *2013 9th International Wireless Communications and Mobile Computing Conference (IWCMC)*, 655–659. <http://doi.org/10.1109/IWCMC.2013.6583635>
- U.Farooq, M., Waseem, M., Khairi, A., &Mazhar, S. (2015). A Critical Analysis on the Security Concerns of Internet of Things (IoT). *International Journal of Computer Applications*, 111(7), 1–6. <http://doi.org/10.5120/19547-1280>
- Zhang, Q., Cheng, L., &Boutaba, R. (2010). Cloud computing: State-of-the-art and research challenges. *Journal of Internet Services and Applications*, 1(1), 7–18. <http://doi.org/10.1007/s13174-010-0007-6>