|  |  |  |
| --- | --- | --- |
| **Module Code**  **COMP5850M** | School of Computing  University of Leeds  **Coursework 2 – Report** | University of Leeds logo |

Full Name: Fanhui Meng Username: sc19fm

Coursework Title: Research Paper Review Deadline Date: 29/03/2020

***Note:*** *the report should not exceed 3 pages in single-spaced typescript. Arial 11pt font recommended.*

1. What did you like about this research paper? **(2 marks).**

This paper, along with it’s appendixes are describe the challenges and future trends in detail. I’m kind of enjoy this paper’s structure. The 13 challenges are one to one correspondence to their future trends. It addresses existing issues and challenges. Then talking about people do making progress for the last decade, and come up with some useful solutions, but there are still limitations. Finally, showing different aspects of future trends and the exciting future for the cloud computing. It’s kind of like cloud computing instruction book, it tells people that we do make big progresses, but in many aspects, including data management, heterogeneity and so on, they are worth to do futher study and improve.

1. The paper identifies 13 different challenges. Which one did you find the most exciting? Explain why. **(5 marks).**

I found the security and privacy are the most exciting chanellenges for me. Most people would care more about the scalability and the performance of cloud computing. And the aspect of security has always been ignored, especially during the early stage of the cloud computing. This is because security cannot show the advantages when it compare to other computing and also it cannot attract more customers to use cloud computing. However, as more and more people are enjoying cloud nowadays, the issue of security has become crucial. The crisis of trust in computer network and customers’s information security caused by cloud computing problems has also intensified.

Thus, developers have come up some ideas about making cloud more secure. For example, on the cloud service provider side, the existing solutions is encrypt the data before storing them at external cloud providers, using Mix&Slice approach to provide complete mixing of the resource, or increase the computational complexity for retrieving data. However, these solution are not perfect. If the encryption are too complex, it would take much more time and consume more energy to encrypt and decode data for both service and client side. If the data are easy to decode, it’s also likely to be crack easily. So I think the security issue can be turned into a trade-off problem in a way, which is very interesting. Some of the companies and their application are emphsis on data or resource sharing, others are care more about confidentiality. Therefore, cloud provider should come up with different strategies for different needs.

There are other interesting aspect of security, including effective privacy-preserving techniques, better hardware-based ARM TrustZone techniques and policy for punish hackers who tries to access cloud illegally. And I’m very looking forward to see how the war is going between the cloud protectors and hackers.

1. Why is interoperability an issue in cloud computing and how can it be addressed? **(5 marks).**

First of all, there are no common standard for cloud computing’s interoperability at present. Different cloud providers, such as Amazon, Google, Alibaba may use different standard or API for their own clouds. And lack of interoperability can lead to limited it’s ability to connect to cloud resources. Application migration or matching data with alternative cloud services can also be expensive and time wasting. In addition, the API that those providers provide can be very different, such as SOAP and REST API. Some of the providers may also not support other providers’ API or their type of data.

To addressed this problem, people need to develop all kind of standards, include standard interfaces, portable data formats, applications, and internationally recognised standards for service quality and security. However pure standardisation is not enough. Developers also need to use software adapters, libraries, practical methods or useful broker for achieving interoperation. For example, some of the libraries can hide the differences between cloud provider APIs, making it possible to manage different cloud resources through a unified API. Develop a common open source cloud operation system can also be another solution. But, to achieve complete interoperation is still a huge challenges and it’s has not been addressed so far.

1. The paper identifies 7 different emerging trends and impact areas. Which one did you find the most exciting? Explain why. **(5 marks).**

The emerging trends of blockchain are the one that I found is the most exciting. The blockchain adopts a decentralized distributed accounting method. Each node in the system participates in the data change record at the same time. And this makes blockchain vastly secure, even the destruction of a single node will not affect the integrity of the entire ledger and records. Because of it’s security and other features, including transparency and the record is unchangeable. Block chain becomes an useful technology in digital business, which is the future trends. Nowadays, people are using this technology anytime, anywhere. For example, online transaction and the popular bitcoin are based on block chain technology. Cloud data centre is always a centralized institution. However, the decentralized block chain is also capable of cloud storage and provide decentralization cloud storage solution, which make things possible and useful.

1. Are there any benefits combining serverless architectures with Software Defined Infrastructures? Explain. **(5 marks).**

People use to develop application to adapt the infrastructures, which can lead to more complicate long period of software development. Serverless architecture allow developers run code in the back-end or in a container, while they are no longer need to manage their service system or application. Then it appears in two forms: Backend as a Service (BaaS) and Function as a Service (FaaS). Without considering the infrastructures, it can reduce the running complexity of applications. And it’s reducing packaging and deployment complexity, which enable software developers implement multiple tasks. Serveless architecture also increase the level of decentralisation of the computation. With the help of decentralisation, software defined infrastructures can easliy allocate the pooled virtualized resources and recombined them on demand. In this way, software may define and manage all kinds of resources, and make it from the core of hardware resources to the core of software platforms. And once the infrastructure can be defined by software, it can get elasticity, automation and other benefits.

1. Heterogeneity has been identified as an important direction for future research. Why does it span over the entire cloud stack? **(2 marks)**

Because the cloud infrastructure is not changeless, it has constantly evloved. And many service providers have incresed their offerings and update their hardware, such as CPU, GPU, FPGA, to meet customer demands and improve performance. And different provider may use different hardware as well as operate system. Heterogeneity always exist and people are trying to use cloud computing to solve this problem. With heterogeneity, it can use co-processor and achieve data parallelism, low latency processing and low power consumption capabilities.

1. The paper identifies 13 different future research directions. Which one did you find the most exciting? Write a short research proposal explaining HOW you will tackle such research direction. **(6 marks)**

The aspect of security and privacy is still the most exciting future directions for me. However, security and privacy are not easy to tackle with, they are involved massive technologies, such as networks, databases, virtualizations, resource scheduling and so forth. And I believe we can achieve these with the help of artificial intelligence. AI is the future trend in many field, and we can also use it in cloud computing to cope with the challenge of security. Researchers can work on machine learning or some predict model to handle with requests and access. This helps develop adaptability to respond to violation attacks and becomes more automatic detection and response to vicious assault, such as web vulnerabilities, Ddos attack and so on. Due to the large scale of the cloud, the harm caused is also greater and wider range. Therefore, AI should take responsibililty to tackle with massive security issues. And developer should do regular offensive and defensive drills to test if AI is able to react well to the most of the conditions.

In addition, it’s also related to other non-technology issues, like ethical issues and legal provision. I’m not a law school student, but researchers still need to set up rules and boundary to punish vicious assaults and prevent this things happen again.