


<b>Module Code</b>	School of Computing University of Leeds	 <b>UNIVERSITY OF LEEDS</b>
<b>COMP5850M</b>	<b>Coursework 2 – Report</b>	

Full Name: Fanhui Meng  
Coursework Title: Research Paper Review

Username: sc19fm  
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 its appendixes, describes 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 directions. At first, it addresses existing issues. 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 cloud computing. It's kind of like cloud computing instruction book, it tells people that we do make significant progress, but in many aspects, including data management, heterogeneity and so on, they are worth to do further study and improve.

2. 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 challenges 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 cloud computing. This phenomenon is because security cannot show the advantages when it compares to other computing, and also it cannot attract more customers to use cloud computing. However, as more and more people are enjoying the cloud nowadays, the issue of security has become crucial. The crisis of trust in computer network and customers' information security caused by cloud computing problems has also intensified. Thus, developers have come up with some ideas about making the cloud more secure. For example, on the cloud service provider side, the existing solutions 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, this solution is not perfect. If the encryption is too sophisticated, 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 encrypt, it's also likely to be cracked 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 an emphasis on data or resource sharing; others care more about confidentiality. Therefore, the cloud provider should come up with different strategies for different needs. There are other exciting aspects of security, including effective privacy-preserving techniques, better hardware-based ARM TrustZone techniques and policy for punishing hackers who try to access cloud illegally. And I'm very looking forward to seeing how the war is going between the cloud protectors and hackers.

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

First of all, there is no universal standard for cloud computing's interoperability at present. Different cloud providers, such as Amazon, Google, Alibaba may use different standard or API for their clouds. And lack of interoperability can lead to limited its ability to connect to cloud resources. Application migration or matching data with alternative cloud services can also be expensive and time-wasting. Besides, 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 address this problem, people need to develop all kind of standards, include standard interfaces, portable data formats, applications, and internationally recognized standards for service quality and security. However, pure standardization 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 universal open-source cloud operation system can also be another solution. But, to achieve complete interoperation is still an immense challenge, and it has not fixed so far.

4. The paper identifies seven 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 its security and other features, including transparency and the record is unchangeable. Blockchain becomes a 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 blockchain technology. Cloud data centre is always a centralized institution. However, the decentralized blockchain is also capable of cloud storage and provide decentralization cloud storage solution, which makes things possible and useful.

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

People use to develop an application to adapt the infrastructures, which can lead to a more complicate long period of software development. Serverless architecture allows developers to run code in the back-end or a container, while they are no longer need to manage their service system or application. Then it appears in two forms: Back-end 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 to implement multiple tasks. Serverless architecture also increases the level of decentralization of the computation. With the help of decentralization, software-defined infrastructures can efficiently allocate the pooled virtualized resources and recombined them on demand. In this way, the 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.

6. 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 constantly evolved. And many service providers have increased 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 the operating system. Heterogeneity always exists, 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.

7. 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 in 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 fields, 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 requests and access. This helps develop adaptability to respond to violation attacks and becomes more automatic detection and response to the 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 responsibility to tackle massive security issues. And the developer should do regular offensive and defensive drills to test if AI can react well to 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 these things to happen again.