Global Journal of Computer Science and Technology: B
Cloud and Distributed
Volume 15 Issue 4 Version 1.0 Year 2015
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

A Review on Progress and Problems of Quantum Computing as a Service (Qcaas) in the Perspective of Cloud Computing

By Mijanur Rahaman & Md. Masudul Islam
Bangladesh University of Business and Technology (BUBT), Bangladesh

Abstract- Cloud computing is a global established system. Quantum computing is hypothetical model which is still in tentative analysis. Cloud system has some weakness in security, processing, backup and vicinity. Somehow quantum computing illustrates some revolutionary solution to overcome cloud weakness. Most researchers are optimistic in quantum computing that it will improve cloud system. It is not easy to combine these two different systems along. We will show two quantum approaches; quantum cryptography and blind quantum computing to secure cloud computing. Quantum cryptography will secure the user data transmission and communication through cloud form hackers. And blind computing will secure the instant eavesdropping or accessing of data processing in cloud from any vicious cloud provider or third party. This paper's major target is to show advantages and disadvantages of quantum computing in the viewpoint to integrate it with cloud system. Also review some current improvement of quantum computing and computer.

Keywords: cryptography, entanglement, polarization, qcaas, qubit, quantum cloud.

GJCST-B Classification : C.2.1 C.2.1 H.3.4

Strictly as per the compliance and regulations of:

A Review on Progress and Problems of Quantum Computing as a Service (Qcaas) in the Perspective of Cloud Computing

Mijanur Rahaman [α] & Md. Masudul Islam [σ]

Abstract- Cloud computing is a global established system. Quantum computing is hypothetical model which is still in tentative analysis. Cloud system has some weakness in security, processing, backup and vicinity. Somehow quantum computing illustrates some revolutionary solution to overcome cloud weakness. Most researchers are optimistic in quantum computing that it will improve cloud system. It is not easy to combine these two different systems along. We will show two quantum approaches; quantum cryptography and blind quantum computing to secure cloud computing. Quantum cryptography will secure the user data transmission and communication through cloud form hackers. And blind computing will secure the instant eavesdropping or accessing of data processing in cloud from any vicious cloud provider or third party. This paper's major target is to show advantages and disadvantages of quantum computing in the viewpoint to integrate it with cloud system. Also review some current improvement of quantum computing and computer. Also we will represent some aroused criticism of quantum cloud computation system in practical research field in recent days. This paper will help us to summarize the major issue that we should concern in quantum cloud computing for future works.

Keywords: cryptography, entanglement, polarization, qcaas, qubit, quantum cloud.

I. Introduction

Cloud computing is globalization for computer and internet. When we hear "Cloud Computing" it actually means "X as a Service" such as, SaaS (Software as a Service), IaaS (Infrastructures as a Service), PaaS (Platform as a Service), DaaS (Data as a Service), NaaS (Network as a Service), StaaS (Storage as a Service) etc.[11] Different services provide different benefits but security is a big issue for cloud computing which is still a burning question. Commercial offerings of market-oriented Clouds must be able to define computational risk management tactics to identify, assess, and manage risks involved in the execution of applications with regards to service requirements and customer needs.[9]

Cloud computing is 50 year old business model, which still needs to expand and overcome limitations that prevent the full use of its potential. [10] Classical computing, cryptography and storage processing is not enough to secure the cloud. So there comes a new era of quantum computing, quantum cryptography and quantum processing. If we could just add the upcoming quantum technology as a service for cloud it will be revolutionary. This new service will be called as "QCaaS" or "Quantum Computing as a Service". Our main target is to review on some recent progress and rising problems in "Quantum Computing as a Service (QCaaS)" for cloud computing.

II. Main Problems of Cloud Computing

Cloud computing is not totally free of access and private to customers in every aspects. There are some cloud providers such as Amazon EC2 gives customer free cloud access for a specific period but that's not applicable for all providers. Moreover, different stages of threat are there such as, data loss, user privacy issue, user data theft, user-vendor security, data locality etc. Even if we use most powerful encryption system or secured medium to pass information over cloud despite these an inside attacks such as; where cloud provider itself could overhears client's secrete information and an outside attacks such as; where intruders could eavesdrop or eliminate client's information could happen. We are not safe from cloud provider's immoral actions.

III. Quantum Computing Basic

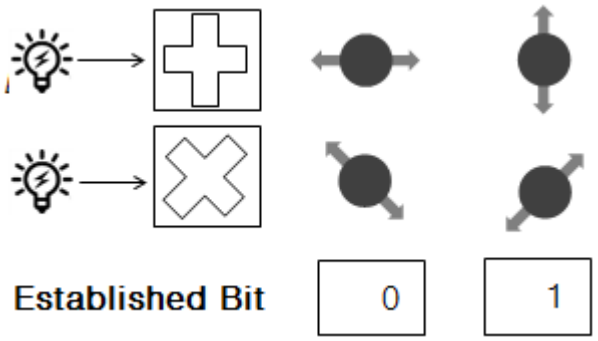
In the case of merging quantum computing with cloud system at first we must ensure about some essential terms on quantum computing.

a) Polarization

Polarization is actually passing a photon through a filter to get a specific spin (vertical/horizontal/diagonal). For example, the output value of photon spins using different polarization is given below:

Author α : Lecturer, Dept. of CSE, Bangladesh University of Business and Technology, Mirpur-2, Dhaka-1216, Bangladesh.
e-mail: riponcse.it@bubt.edu.bd
Author σ : Lecturer, Dept. of CSE, Bangladesh University of Business and Technology, Mirpur-2, Dhaka-1216, Bangladesh.
e-mail: masudulislam11@gmail.com

Fig.1. Photon polarization using 2 different filters with their established bit values



b) Qubit

Classical computer uses 0 or 1 as bit system. But in quantum system the fundamental unit is known as Qubit (|0> or |1>) or superposition of both 0 and 1. By analyzing Bloch sphere, if we measure 0 bit as south pole and 1 bit as north pole then a Qubit means any alternative possible state of a rectilinear combination of |0> and |1>. This often referred to as a superposition: $|\psi\rangle = a|0\rangle + b|1\rangle$. [1]

c) Quantum Entanglement

This is a ghostly particle reaction issue. When two photons are entangled pairs it means, one photon has the opposite spin of another one without having any bodily connection among them.

d) Qubit Measurement

According to Heisenberg's uncertainty principle, we will never be able to measure both speed and position of any particle at a time. If we try to measure a Qubit we'll only get discreet 0 or 1. So there's no way we can tell the real-time measurement of a Qubit.

IV. Two Different Quantum Approaches

Two different quantum approaches could solve these problems. they are, blind computing and quantum cryptography. Blind computing means, where all the data input, output, processing will become unidentified by any quantum computer. In blind computing theoretically the cloud user generates some qubit where only he knows the initial states of those qubit. After sending these qubit to the quantum computer, the computer entangles the qubit using a standard system. the actual computation is measurement-based. The user adapts measurement guidelines to the specific state of each quantum bit. and he sends them to a quantum server. after successful processing the user gets back his result and he can interpret the final result. the whole process is "blind" because even if the quantum computer or an eavesdropper tries to decipher the qubit, they will not get any beneficial information. it's because they don't know the initial states. [2] Another approach is quantum cryptography is given below in details.

a) Quantum computation & cryptography in cloud system

Beyond current two type classical cryptography now a day's physics has discovered new age of quantum mechanics. Using quantum physics law a quantum computer could have incredible power of compute within a shortest possible time. From earlier discussion each time a single Qubit is added to a quantum computer its computational power gets double. We can get 2128 different of I/O at a time only using 128 Qubit. A quantum algorithm called Grover's quantum algorithm $O(\sqrt{n})$ which states that, using superposition of Qubit anyone can search any data by $\sqrt{250000} = 500$ steps from 250000 data. In the case of classical computer, it need at least $n/2 = 125000$ steps. This means a perfect quantum computer can reduce any processing time of years into milliseconds. So once quantum computer is fully developed our present 128-bit cryptography system could easily be beaked by it. Also government agencies, banks, security companies, defense need to secure their information from being hacked, because one day this quantum technology might decipher their system. So we need new strong encryption and secured communication system. And there comes quantum computation for fast processing and quantum cryptography for security issues.

There is a common example where two users (Sara and Musa) in cloud sending-receiving key using quantum cryptography encryption technique and at the same time hacker are trying to eavesdrop it. Sara the sender first creates a simple Qubit and sends it to Musa. Sara is using a diagonal filter (X) and a rectilinear filter (+) to send the key. Here "/", "\" indicates 45° diagonal photon spin and "-", "|" indicates 90° rectilinear spin. Sara uses polarization and evaluates the value of key. Musa is waiting for incoming photons which randomly applies any rectilinear or diagonal polarization filter. He also keeps a note of used polarization, its value and spin. After successful communication, Sara and Musa interconnect over open channel. Musa gives Sara only polarization filter orders that he used. Table (i) shows Sara sends a key [01011001]. Now if Musa received an incorrect order of information shown in Table (ii) [00011001] after that, Sara will tell whether the order is exact or not. After full transmission by fixing the mistaken polarization sequence the ultimate encoded data can be sent. Eavesdropper cannot deduct all the polarization sequence exactly in this system. If Musa unable to decode the sent data he cloud notice easily the interference of communication by hacker's. Other criteria called quantum non-cloning criteria of quantum computation guarantees us not to achieve an identical copy of any quantum polarized state in the middle of calculation. This means spy will never be able to get a duplicate copy of transported quantum cryptography keys. If someone is able to clone any state then he

could make many identical copies of it. At the same time he can measure each dynamic variable with random precision; that will avoid the uncertainty principle. But due to the non-cloning theorem this fear is prevented [3]. The cold true is that, there is still no completed quantum computer yet to establish system.

Table.1. Sara sending key

Sara's polarization	X	X	+	+	X	+	+	+
Sara's spin	\	/	–	|	/	–	–	|
Sara's value	0	1	0	1	1	0	0	1

Table. 2. Musa receiving key with error

Sara's answers	Y	N	Y	Y	N	Y	Y	N
Musa's polarization	X	+	+	+	+	+	+	X
Musa's spin	\	–	–	|	|	–	–	/
Musa's value	0	0	0	1	1	0	0	1

V. Problems and Recent Progress of Quantum Cloud Computing

a) Raising problems of quantum cloud computing

The burning question of Cloud computing is whether it is secured and reliable for users or not. Theoretically quantum computing can solve all the complications of cloud computing. But some key challenges arise to develop a quantum computing system. There are some uncertainties on quantum computation. It said that this quantum computer stuff may not be quantum at all as we are fascinating.[4] The newly developed D-Wave quantum computer system has some major concerns. In quantum computation system question arises that, is the d-wave really a quantum computer? Also we need to build a physical logic gate to control Qubit. Even if we build a gate how we will prevent noise effect on photon? If a little noise disentangles the Qubit then the whole quantum computer will be a classical computer type. Because we still cannot control the subatomic level of any system. Another key paradox is that even we effectively run a calculation or process we will never be able to find every single phase of it. We can only get only single state of all possible superposition of photon. So error checking is tough. This makes the quantum computation ambiguous and the quantum cloud computing too. But we must aware that, we can't fully prevent an inside unethical attack in cloud system. According to Seth Lloyd, an expert in quantum computation at the Massachusetts institutes of technology "treachery is the primary way, "there's nothing quantum mechanics can do about that". [5]

b) Recent improvement of quantum cloud computing

Quantum computer development is still ongoing. There are so many research, methods, architectures and approaches to achieve quantum computer and cloud system integration. Google has already declared their first quantum computer will build on d-wave's approaches. They are going to design Qubit in different way by improving d-wave's hardware. [6] Recently in 2012, s. Barz, e. Kashefi, a. Broadbent, j. F. Fitzsimons, a. Zeilinger and p. Walther demonstrate an experimental blind quantum computing for secured cloud computing. They completed the theoretical framework of measurement-based quantum computation that allows a user to represent a computation to a quantum server. [7] Also a quantum-cloud system in 27 September 2013 has been confirmed by a group of scientist of Bristol University in UK. It is named as Qcloud. The Qcloud quantum computer placed at the center for quantum photonics in the Bristol University. The idea is to establish a practical aspect of quantum computing as a service (QCaaS). This quantum processor would be remotely accessed and controlled by anyone in the world. It would allow people to run an experiment, and test the real experimental data against their simulations. However, they are only using two Qubit. This shows a practical example of application of the quantum computing-cloud computing in recent time. [8]

VI. Conclusion

We are showing summery review of how effectively quantum based computation could improve our classical computations and communication in cloud

our classical computations and communication in cloud computing system. We also try to show all possible area of major problems in quantum computing for further analysis and future works. This new service we called "Quantum Computing as a service or QCaaS" is still under development. Until the quantum computer attains its final state we should try to improve our present classical system and deprive their limitations. We expect in near future quantum cloud computing will bring revolutionary change in cloud system.

References Références Referencias

1. Wikimedia Foundation (2001), Qubit. 17 March, 2015. Retrieve from: https://en.wikipedia.org/wiki /Qubit
2. PhysOrg (2012). Quantum mechanics enables perfectly secure cloud computing, 19 January 2012. Retrieve from: http://phys.org/news/2012-01-quantum- mechanics-enables-perfectly-cloud.html
3. Quantiki (2010), the Non-Cloning Theorem. 9 June, 2010. Retrieve from: http://www. quantiki. org/wiki/ The_nocloning theorem
4. Wired Magazine (2014), The Revolutionary Quantum Computer That May Not Be Quantum at All, 20 May 2014. Retrieve from: http://www.wired.Com/2014 /05/quantum-computing/
5. Stix, Gary (2004). Best-Kept Secrets. Scientific American.
6. Simonite, Tom (2014). Google Launches Effort to Build Its Own Quantum Computer. 17 September, 2014. Retrieve from: http://www.Technologyre view. com/news/530516/google-launches-effort-to-build-its-own-quantum-computer/
7. S. Barz, E. Kashefi, A. Broadbent, J. F. Fitzsimons, A. Zeilinger And P. Walther (2012). Demonstration of Blind Quantum Computing. Science Journal Vol. 335 No. 6066, pp: 303-308
8. Harpreet Singh, Abha Sachdev (2014). The Quantum Way Of Cloud Computing, Optimization, Reliabilty, and Information Technology (ICROIT). pp: 397 – 400.dx.doi.org/10.1109/ICROIT.2014.6798362
9. R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg and I. Brandic, "Cloud Computing and Emerging IT Platforms: Vision, Hype and Reality for Delivering Computing as the 5th Utility", Future Generation Computer Systems, Elsevier, Vol. 25, pp. 599-616, 2009.
10. F. Durao, J. F. S. Carvalho, A. Fonseka and V. C. Garcia, "A Systematic Review on Cloud Computing", The Journal of Supercomputing, Vol. 68, Issue 3, pp. 1321-1346, 2014.
11. B. P. Rimal, E. Choi and I. Lumb, "A Taxonomy and Survey of Cloud Computing Systems", Fifth International Joint Conference on INC, IMS and IDC, pp. 44-51, 2009.

Global Journals Inc. (US) Guidelines Handbook 2015

www.GlobalJournals.org