*I.J. Mathematical Sciences and Computing*, **2016, 1, 16-22**
Published Online January 2016 in MECS (http://www.mecs-press.net)
DOI: 10.5815/ijmsc.2016.01.02

***Available online at http://www.mecs-press.net/ijmsc***

# An Overview on Quantum Computing as a Service (QCaaS): Probability or Possibility

Mijanur Rahaman[a], Md. Masudul Islam[b]

[a]*Bangladesh University of Business & Technology, Dhaka, 1216, Bangladesh*
[b]*Bangladesh University of Business & Technology, Dhaka, 1216, Bangladesh*

**Abstract**

Cloud computing is a worldwide classical system. Quantum computing is theoretical concept still in experimental review. Where cloud system is facing vulnerability in security, backup, processing and locality, there quantum computing shows a strong solution to overcome it. Most researchers are optimistic in quantum computing that it will improve cloud system. But to associate physics based subatomic computing system with software based cloud system is not an easy option. Our paper will show all the major advantages and disadvantages of quantum computing in the perspective to integrate it with cloud system. And review some recent progress with some foremost doubtful future aspects of quantum cloud computing. Also we will review the reality of quantum computation and internet system in applied viewpoint until present.

**Index Terms:** Qubit, polarization, entanglement, QCaaS, non-cloning, cryptography and quantum cloud.



## 1. Introduction

Cloud computing is called the globalization for computer and internet. According to NIST, Cloud Computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction.[13] Either directly or indirectly we are using cloud technology almost every day. In a word, cloud computing stands for keeping, accessing and processing data and programs over the internet instead of using local computer. The cloud is a representation for the internet.

Cloud computing means “X as a Service”. For example; IaaS (infrastructures as a service) which provides storage to customers, SaaS (software as a service) which provides web applications as service and PaaS (platform as a service) which provides development environment as service, NaaS (Network as a Service),

* Corresponding author. 01671118854
E-mail address: masudulislam11@gmail.com

StaaS (Storage as a Service) etc. [15] There are so many terms and levels in cloud system. There are some benevolent facts of cloud computing. Although cloud computing system has advantages, but there are major dependencies which make some weakness for cloud system. By integrating the upcoming quantum computing technology as a service for cloud it will be an avant-garde. This new service we called as "QCaaS" or "Quantum Computing as a Service". Our main concern is to show a summarize view on secured encrypted data passing and processing (quantum cryptography) through cloud and some of its drawbacks. At first we must know some fundamental terms and issue on quantum cryptography.

### *1.1. Qubit*

Where classical computer based on bit (0/1) in quantum system the fundamental unit is Qubit (|0> or |1>) or superposition of both 0 and 1. According to Bloch sphere, If we measure bit (0) as south pole and bit (1) as north pole then a Qubit can be in alternative potential state a rectilinear combination of |0> and |1>, often referred to as a superposition: [1]

$$|\psi\rangle = a|0\rangle + b|1\rangle \quad (1)$$

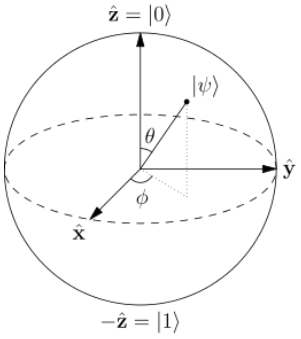


Fig. 1. Bloch Sphere

### *1.2. Photon Polarization*

This is passing a photon through a filter to get a specific spin (vertical/horizontal/diagonal). Example of output photon spins using different polarization:

Table 1. An example of Polarization Values

| Spin | Horizontal spin (–) | Vertical spin (\|) | Left diagonal spin (\) | Right diagonal spin (/) |
|---|---|---|---|---|
| Value | 0 | 1 | 0 | 1 |

### *1.3. Quantum Entanglement*

This is a spooky particle reaction issue states that, two photons are entangled pairs. It means, if one photon has the opposite spin of another one not having any physical connection among them. For example if photon1 is rotating horizontally then another photon2 must have the vertical spin. If we know one photon spin any one

can find out another one's spin. This issue has both advantages and disadvantages on communication and computing.

### *1.4. Quantum Entanglement*

Sending photon as key using polarization filters such a way that only sender and receiver will know the filter sequence to encrypt and decrypt the data. We will discuss it later.

## 2. Major Drawbacks of Cloud Computing

Cloud computing is not in the hands of customer. So there are different levels of threat models such as, data integrity problem, data theft, privacy issue, data loss, data location, user-vendor security etc. Our main concern is inside attacks; where cloud provider itself could cheat or eavesdrops client's secrete information.

On other side, outside attacks; where hackers or intruders could eavesdrop or abolish client's information.

Both are catastrophic threat for any cloud user! Even if we use most powerful encryption system or secured medium to pass information over cloud it could save us from network hackers but we cannot be safe from hands of cloud provider's unethical actions.

## 3. Two Quantum Approaches

Recently experimental view of quantum principle shows us two different ways to secure cloud system. One of them is called blind computing where all the input, output, data processing will remain unknown to the quantum processed computer itself. According to blind computing, the cloud user generates Qubit and he only knows the initial states. Then 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 approaches is quantum cryptography with quantum internet system, where information is encrypted and decrypted using photon polarization filters, we will discuss it below.

## 4. Quantum Computation in Cloud System & Some Major Concerns

Recent two type classical cryptography (symmetric cryptography, asymmetric cryptography) both has disadvantages. For example in asymmetric cryptography if someone's private key get lost or disclosed then he must generate a new pair of public and private keys. These cryptography is using 128-bit key that makes any hacker huge amount of time to crack even if we use supercomputer.

Now a day's physics has revealed new era of quantum mechanics where a quantum computer has unimaginable power to 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. Using only 512 Qubits we can get 2512 combination of input/output at a time. Again according to Grover's quantum algorithm o($\sqrt{}$ n) using superposition of Qubits anyone can search from 250000 data using only $\sqrt{}$ 250000 = 500 steps where classical computer need at least n/2 = 125000 steps. This means quantum computer can shrink any operation 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.

Let's see a familiar example where two users (Xion and Ezekiel) in cloud sending-receiving quantum key using quantum cryptography encryption method and at the same time a hacker is trying to overhear it.

Step 1. Xion (sender) first generate Qubit to send message to Ezekiel over optical fibers.

Step 2. Xion used polarization and estimate the value of key

Step 3. Ezekiel is waiting for incoming photons and randomly applies any rectilinear or diagonal polarization filter and keeps a memo of used polarization, spin and its value.

Step 4. After total transmission, Xion and Ezekiel communicate over unencrypted public channel and Ezekiel gives Xion only polarization filter sequences that he used.

Here in Table 1. Xion sends the key in this format: (01011001). Without giving the key directly Xion and Ezekiel just needs to compare polarization filter sequence.

Table 2. Xion Sending Polarized Key

| Xion polarization | X | X | + | + | X | + | + | + |
|---|---|---|---|---|---|---|---|---|
| Xion spin | \ | / | – | \| | / | – | – | \| |
| Xion value | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 1 |

Table 3. Ezekiel receiving key with some bit error

| Xion's answers | Y | N | Y | Y | N | Y | Y | N |
|---|---|---|---|---|---|---|---|---|
| Ezekiel polarization | X | + | + | + | + | + | + | X |
| Ezekiel spin | \ | – | – | \| | \| | – | – | / |
| Ezekiel value | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 1 |

Step 5. Now if Ezekiel received a wrong sequence of information as per table: 2 (00011001) then Xion will say whether the sequence is correct or not. After complete transmission and fixing the mistaken polarization the final encrypted data can be sent and decrypt.

In this system no eavesdropper in the middle can deduct all the polarization exactly. So when Xion and Ezekiel authenticate the polarizations, and if Ezekiel fails to decrypt the data, then the interference of communication by hacker's will get detected easily.

This same technique applies to Quantum internet system to over secure the cloud communication to the end-users. Quantum internet is based on photon transmission, so when we send any information over cloud if someone eavesdrop it then the data get changed instantly. Finally when the data is gained by end user he will able to find out that someone spy on their communication during transmission. So if we build an internet using quantum physics or photons then the security medium system will improve unimaginably. A team of researchers from the Massachusetts Institute of Technology (MIT) and Northwestern University (NU) developed a system for long-distance, high-fidelity Qubit teleportation. Such a system will be required if future quantum computers are to be linked together into a quantum Internet. [14]

Also no cloning criteria of quantum computation ensures us that, we cannot achieve an identical copy of any quantum state in the middle of computation. This means no eavesdropper can able to get a copy of transferred 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 dynamical variable with random precision; that will avoid the uncertainty principle. But due to the non-cloning theorem this fear is prevented. [3]

So what are the major difficulties of quantum cryptography? Firstly most of the quantum issues are in theories. Some of them are proved and some are in experimental process. Beside this major concern for quantum computations are:

1. Generating a Qubit and synchronize multiple Qubits at a time is extremely difficult.
2. The length of quantum cryptology transmission capability is too short because of interference. Recently a team of Boris Korzh, Charles ci wen Lim and many other demonstrated an acceptable practical and secure quantum key distribution (QKD) over 307 km of optical fiber.[4]
3. Hardest fact for quantum communication is quantum distributed networks, where we must convert multiple Qubits into photons based on which matter we are using. It is essential for long distance communication to convert any quantum states from atomic system to photonic system.
4. We cannot amplify the quantum key carrier signal to transmit long distance because an optical amplifier could corrupt the Qubits. Even a single particle effect can corrupt the polarized photon. It's too sensitive.
5. A photon's spin can be changed when it bounces off other particles, and so when it's received, it may no longer be polarized the way it was originally intended to be.
6. Most of the quantum computation is based on law of physics; there are several complexities on developing quantum code compilation or software controlled system.
7. What if the eavesdropper also has a quantum computer?
8. The whole process is expensive, sensitive and not yet fruitful.

But the unpleasant true is there is still no full featured quantum computation system with proper advanced technologies. Finally we have to remember that, an inside unethical attack in cloud system is irresistible. 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]

## 5. Recent Progress to Overcome These Problems

Whatever the problem arise but the quantum mechanics, computation progress is still ongoing. All we need advanced quantum computer, generate multiple Qubits, quantum protocol and proper medium for communication.

Google has already declared their first quantum computer will build on d-wave's approaches. They are going to design Qubits in different way by improving d-wave's hardware. The recent d-wave's main machine chip contains 512 Qubits. Also Google's quantum researcher believed that they and d-wave will build a new 1000 Qubit processor and make it become available. [6]

As we say about blind computing 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 achieved the theoretical framework of measurement-based quantum computation that enables a user to represent a computation to a quantum server. [7]

Also in 27 September 2013 a quantum-cloud system has already been demonstrated by a group of scientist of Bristol University, United Kingdom. This initiative has been 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 Qubits. This shows a practical example of application of the quantum computing-cloud computing in recent time. [8]

In the case of quantum key's long distance transmission, we need some kinds of quantum repeater. We can take the advantage of photon's "spooky action at distance". Because of link between two pairs of entangled

photons any information could 'teleport' across a huge distance. In this way quantum keys could be teleported anywhere in the world. In august 19, 2004 at the institute of experimental physics in Vienna scientist Anton Zeilinger and his team took an initial pace to demonstrate a repeater. Zeilinger and his team took the advantage of entanglement and "teleport" an information over 600 meters distance carried by a 3rd photon across the Danube. If this system could extend into multiple relays then the Qubits in a key could be transmitted across continents or oceans. [9]

## 6. Certain and Uncertain Future

Cloud computing always will be questionable if there is no secured and reliable adaption for users. We have already seen theoretically quantum computing can remove all the problems of cloud if and only if quantum computer and network system is completely developed. At present 2015, development of quantum system is still doubtful but it is ongoing. IBM claimed that they developed a new superconducting chip to build a quantum computer. [10] But in 2014, wired magazine stated doubt on quantum computation. It claimed that this quantum computer stuff may not be quantum at all as we are fascinating. [11] The major concerns are: Is the big black box: d-wave a quantum computer? Can we control the subatomic level? How to build a new gate to operate Qubits? How we will prevent noise effect on photon? If a little noise disentangles the Qubits then the whole quantum computer will act like a classical computer. Also how to integrate large-scale (1000) Qubits in parallel? How much portability it contains? Another crucial paradox is that even we successfully run a calculation we can't find every single step of it (for further use or error checking) rather than we will find only single state of all possible superposition of photon. [12] There are so many questions to be answered. This makes the quantum computation uncertain and so the quantum cloud computing.

## 7. Conclusions

In this paper we try to review briefly how essentially quantum based computation could change our classical processing and communication in cloud system. Also we are putting up all the major advantages with simple example and major problem with some recent progress in quantum computation. The new approaches "quantum computing as a service or QCaaS" is still ongoing. But until the quantum computer arrives we should improve our present system, deprive limitations. Also beside these we need to develop a flexible quantum computation system for enterprise use. We hope in future our continuous development in quantum computation will bring a revolution and will make a way to improve quantum-cloud system.

## References

[1] "https://en.wikipedia.org/wiki/Qubit" Wikimedia Foundation, 2001.Web. 17 March, 2015.
[2] "http://phys.org/news/2012-01-quantum-mechanics enables-perfectly-cloud.html". Web. 19 January 2012
[3] "http://www.quantiki.org/wiki/The_nocloning theorem" Web. 9 June, 2010.
[4] Boris Korzh, Charles Ci Wen Lim, Raphael Houlmann, Nicolas Gisin, Ming Jun Li, Daniel Nolan, Bruno Sanguinetti, Rob Thew and Hugo Zbinden. "Provably Secure And Practical Quantum Key Distribution Over 307 Km Of Optical Fibre", Nature Photonics 9 (2015): 163–168.
[5] Stix, Gary. "Best-Kept Secrets", Scientific American, 20 December 2004: 83.
[6] "http://www.technologyreview.com/news/530516/google-launches-effort-to-build-its-own-quantum computer/" Web. 3 September 2014.
[7] S. Barz, E. Kashefi, A. Broadbent, J. F. Fitzsimons, A. Zeilinger And P. Walther. "Demonstration Of Blind Quantum Computing", Science Journal Vol. 335 No. 6066 (2012): 303-308.
[8] Harpreet Singh, Abha Sachdev. "The Quantum Way Of Cloud Computing", Ieee (2014): 397 - 400.
[9] Stix, Gary. "Best-Kept Secrets", Scientific American, 20 December 2004: 83.

[10] "http://www.technologyreview.com/news/537041/ibm-shows-off-a-quantum-computing-chip/". Web. 29 April 2015.
[11] "http://www.wired.com/2014/05/quantum computing/". Web. 20 May 2014.
[12] "http://www.wired.com/2014/05/quantum computing/". Web. 20 May 2014.
[13] Peter Mell, Timothy Grance, "The NIST Definition of Cloud Computing" The NIST Definition of Cloud Computing. NIST Special Publication 800-145, U.S Department of Commerce. September, 2011.
[14] Seth Lloyd, Jeffrey H. Shapiro, Prem Kumar and Selim M. Shahriar. "Infrastructure for the Quantum Internet". ACM SIGCOMM Computer Communications Review. Vol. 34, Number 5. October, 2004.
[15] 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.

**Authors' Profiles**

**Mijanur Rahaman,** Lecturer in Dept. of CSE in Bangladesh University of Business & Technology. His main area of working is networking, cryptographic security system and software base automation system. He is the developer and controller "Student Information and Management System" software of current university. He was the main webmaster and master analyzer of ACM-ICPC regional Dhaka site 2014.

**Md. Masudul Islam,** Lecturer in Dept. of CSE in Bangladesh University of Business & Technology. He has developed an entire online student management system for Bangladesh University of Business and Technology. He was the webmaster in ACM-ICPC 2014 regional contest. He has developed a full-featured online automation system for ACM-ICPC regional Dhaka site contest. His main areas of working are Web technologies, quantum physics & computing and cloud computing.

**How to cite this paper:** Mijanur Rahaman, Md. Masudul Islam,"An Overview on Quantum Computing as a Service (QCaaS): Probability or Possibility", International Journal of Mathematical Sciences and Computing(IJMSC), Vol.2, No.1, pp.16-22, 2016.DOI: 10.5815/ijmsc.2016.01.02