Article can be accessed online at http://www.publishingindia.com

An Enhanced Cloud Security using Quantum Teleportation

D. Sowmya*, S. Sivasankaran**

Abstract

In the cloud environment, it is difficult to provide security to the monolithic collection of data as it is easily accessed by breaking the algorithms which are based on mathematical computations and on the other hand, it takes much time for uploading and downloading the data. This paper proposes the concept of implementing quantum teleportation i.e., telecommunication + transportation in the cloud environment for the enhancement of cloud security and also to improve speed of data transfer through the quantum repeaters. This technological idea is extracted from the law of quantum physics where the particles say photons can be entangled and encoded to be teleported over large distances. As the transfer of photons called qubits allowed to travel through the optical fiber, it must be polarised and encoded with QKD (Quantum Key Distribution) for the security purpose. Then, for the enhancement of the data transfer speed, qubits are used in which the state of quantum bits can be encoded as 0 and 1 concurrently using the Shor's algorithm. Then, the Quantum parallelism will help qubits to travel as fast as possible to reach the destination at a single communication channel which cannot be eavesdropped at any point because, it prevents from creating copies of transmitted quantum key due to the implementation of no-cloning theorem so that the communication parties can only receive the intended data other than the intruders.

Keywords: Qubits, Quantum Key Distribution, Quantum Repeaters, No-Cloning Algorithm, Quantum Parallelism

Introduction

Existing System

In existing system, the security of the cloud environment is prone with numerous attacks as the prevention provided is made with only mathematical cryptographic algorithms which can be easily cracked. Unfortunately when data is of massive scale, the uploading and downloading mechanisms will be subjected to extremely time-consuming process and consequently cause serious delay for the urgent tasks.

The consequence of this pitfall will allow the intruder to access the whole network if at least one client node is subjected to the attack. Vast amount of data is being intercepted today and stored for future decryption so that the massive collection of data are encrypted with more computational complexity and prone to be hijacked easily. Though the improved version of RSA (SRNN) has increased the security level by using two primary numbers, it hardly consumes time in generating keys.

Proposed System

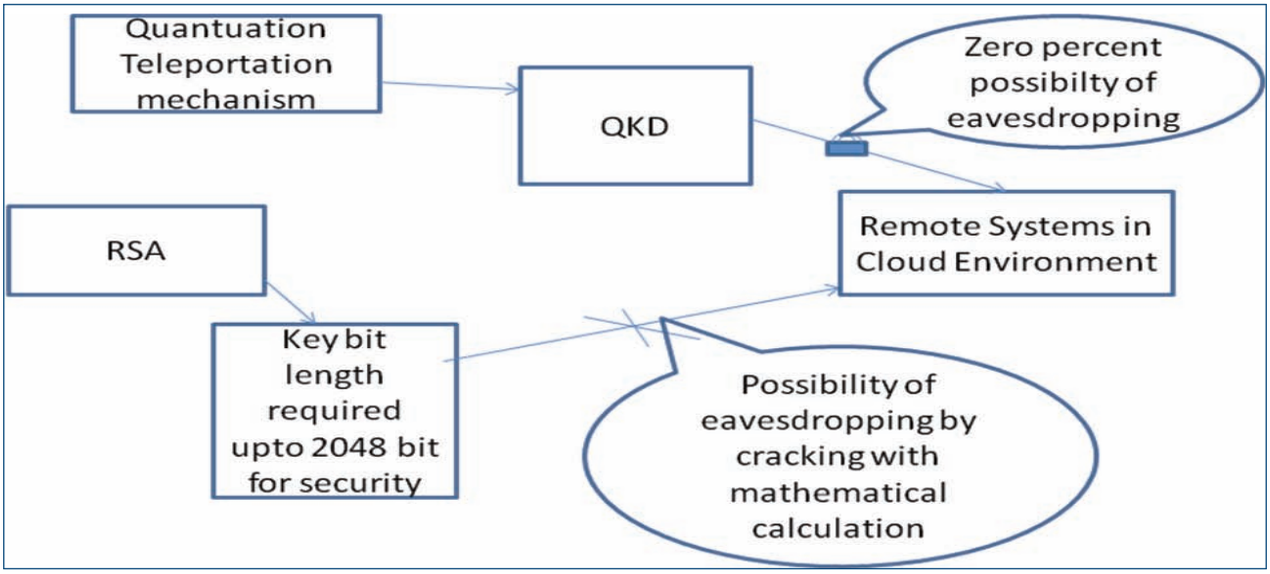
A wide range of industries relies upon the ability to keep sensitive information secure. So, to satisfy the need, quantum teleportation is used.

Quantum teleportation is the concept of law of physics used to encode data using QKD (Quantum Key Distribution) to ensure secure communication. It is mainly used to improve the security of cloud data.

* Final Year PG Student, Department of Computer Applications, IFET College of Engineering, Villupuram, Tamil Nadu, India. E-mail: sowmya.sowmyad@gmail.com

** Senior Assistant Professor, Department of Computer Applications, IFET College of Engineering, Villupuram, Tamil Nadu, India.

Figure 1: Possibility of Eavesdropping in Quantum Teleportation and RSA



When compared to other cryptographic algorithms like RSA, QKD which is completely based on mathematical computations cannot provide any indication of eavesdropping at any point in the communication channel. Moreover, it is better to use the teleportation technique which provides the parallelism, security in an integrated manner rather than implementing those techniques separately.

The QKD can be done using the encryption algorithm called Shor's algorithm in which the factorisation of large integers takes place.

As shown in Figure 1, it is apparent that using Quantum Key Distribution, there is very less assumed to be zero percent possibility of gaining access to the credential data.

Quantum Key Distribution

Quantum Key Distribution is completely used for avoiding the eavesdropper to hack the information at the time of establishment of communication channel or quantum channel. It is clear that the cryptographic algorithm based on some mathematical computation is avoided in this technique as it is prone to high security attack.

Quantum key distribution is a key establishment method which creates key material by using the quantum properties of light to transfer information between two parties along with a specialised quantum channel, such as a fiber optic link. Depending on the detection equipment used to recognise quantum information sent that will either be perfectly correct, or a completely random value. The sending and receiving of quantum information is the only quantum part of QKD and is called classical post-processing. The key which is sent by the source is subjected to various states during polarisation and if the input size increases, the speed can be accelerated by providing the quantum parallelizing technique. The destination system will receive the key which is not affected to any attack by the third party. Then, the measurements will be used to generate the secret key. This potential key material is subjected to standard error-correcting routines.

No-Cloning Algorithm

The no-cloning theorem will help in protecting the security key (Quantum key) distributed over the communication network by preventing the creation of copy while relaying the qubits along the network. This theorem emphasizes that during the entanglement of qubits, there will be different degree of polarisation for example 90 degree, 110 degree, etc which possess different states during the polarisation in the optical fiber. Henceforth, the process of getting the clone of data is not possible as it disrupt the channel.

This concept assures that at any point, the remote system in a cloud environment will have the guaranteed communication with the quantum mechanism. The Cloud Service Provider (CSP) must stand as an intermediate to ensure the successful transportation of data.

This theorem will reduce the transmission of data over long distances as it will not allow to create copy of qubits but the cloud services requires the data to travel over large distances. So it is necessary to take copy at particular client station as a backup. This issue can be solved by placing a repeater to extend the communication range which can be explained clearly in the following paragraphs.

Shor's Algorithm

In this algorithm the representation of qubits can be represented as superposition which possesses 0 and 1 at the same time to factorize the large numbers in rapid manner which is faster than normal mathematical algorithms.

The Shor's algorithm is dependent on three procedures. They are

- Modular Arithmetic
- Quantum Parallelism
- Quantum Fourier Transform

This is particularly used to handle massive data to produce result in a faster manner.

For factoring N bits,

$$O\left(\exp\left(\left(\tfrac{64}{9}\right)^{1/3} N^{1/3} (\ln N)^{2/3}\right)\right)$$

This operation scales exponentially with input size.

Modular Arithmetic Method

There are many classical algorithms to factorize pure prime powers (and of course to recognize a factor of 2), but an efficient probabilistic algorithm for the factorisation of all possible inputs to prime number to produce the fast result is only through modular arithmetic method. Here the transformation x a mod N can be applied with a random number and produce an output with superposition as 0 and 1 concurrently. These states can be entangled to transmit the data in a rapid manner.

Quantum Parallelism

In this mechanism, the immediate result can be generated for every possible input by processing in a simultaneous manner. It will reduce the size of the input there by reduces the computational complexity. It provides scalability to work with the massive data in the macroscopic world.

Quantum Fourier Transform

This is a discrete Fourier transform, not upon the data stored in the system state, but upon the state itself. The fourier transform has the effect of taking a state |a> and transforming it into a state given by

$$\frac{1}{\sqrt{q}} \sum_{c=0}^{q-1} |c> * e^{2\pi i a c / q}$$

Where a is any set of whole numbers and

q is a qubit value and

i is an integer value .

The QFT comes up short and reveals the wrong period. This probability is actually dependant on your choice of *q*. Larger the q, the higher the probability of finding the correct result.

$$\tilde{f}_k \equiv \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{2\pi i j k / N} f_j, \quad f_j \equiv \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{-2\pi i j k / N} \tilde{f}_k.$$

The discrete Fourier transform (DFT) ˜ f of a discrete function f1, . . . , f ,N and its inverse are given by

Here N is an odd integer,

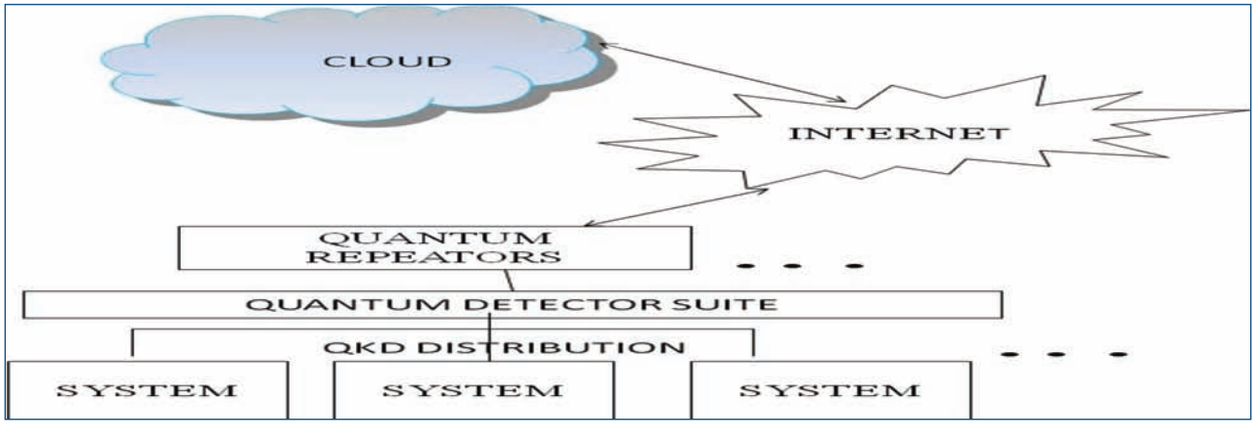
Enhanced Speed of Data Transfer

In the cloud environment, the upstream and downstream speed of data can be highly improved using the improved quantum repeaters.

Quantum Repeaters

A quantum repeater is the one which is able to relay quantum information and extend the communication range of a quantum network. In cloud environment, there are possibilities of occurring attenuation. So by using the repeaters it can be solved and also provide fast transmission. Since there is the restriction in copying data

Figure 2: Architecture of Quantum Repeaters



due to no cloning algorithm, these repeaters will be used for relaying information.

Physical Architecture of Quantum Repeaters

The Quantum repeaters are the core concept of quantum internet. This can be used to increase the distance of the data to be travelled. In the cloud environment, it will be used in the middle of each station (client station) to improve the restriction of quantum memory as it was not longer persisted during entanglement of the photons.

In the classical architecture, the mirroring of data is used for the purpose of backup but this is highly prone to security issue but in quantum teleportation there is no possibility of taking copy of entangled qubit. To solve this, the quantum repeaters are used for the network coverage over larger distances. Moreover, the qubit must be detected through the quantum detector required to recognise the actual data sent by the sender.

Here, the quantum repeaters not only increase the speed of the data flow but also the communication range through optical fiber. There the quantum detectors will be resided in both the source and destination to decode the data after the entanglement.

The physical requirement of this architecture includes quantum processor, quantum detectors, quantum repeaters, and the communication medium called optical fiber. Over the Internet, the qubit can be sent to end-to-end client station to reach the destination in a fraction of second as this follows quantum parallelism concept as noted earlier. For large amount of input size it will take primary factor of the power of two to reduce the delay exponentially.

The quantum key will be distributed across the remote systems which are in connection with the cloud server. Layered quantum communication relies on five key vertical layer functions that are uniquely quantum

First phase: At this stage, the light is allowed to encode quantum state. Many technologies for this layer are under development. Then the entanglement will happen across a link. Because most physical entanglement mechanisms are probabilistic, this includes an acknowledgment to the sender indicating which attempts are succeeded.

Second phase: At this stage, the remote state composition occurs in which the quantum repeaters will extract the data and copying packets from one node to the next. In a cloud environment, the qubits must be allowed to pass through various client stations to improve the communication range. As the study about the cloning theorem reiterated the discomfort of communication over the large distances, at this stage the attenuation of channel may occur. So the repeaters will take care of this issue and guarantees the flawless transmission.

Third phase: This is the final phase, where the error management will occur. In the classical Internet, errors are managed using redundancy (e.g., forward error correction) or error detection and retransmission. As noted earlier, the no-cloning theorem prevents straightforward use of either of these mechanisms. It is obvious to know that due to the polarisation of qubits at various angles, there will be less possibility of errors. Consequently the data will be sent to the cloud in a safe manner.

The CSP must be responsible for the photon entanglement at various levels which may disrupted at any cause such as eavesdropping. So for promising end-to-end connection between the remote system, the required data must be intimated to the sender. The speed of macroscopic data transfer will be finished in seconds than expected.

The services such as Iaas (Infrastructure as a Service), Paas (Platform as a Service), must be dependent on quantum processors to decode and recognize the quantum bits for the computational requirement. For the long period, it was a challenging task to recognise the bit and produce computational result in a fast manner but using the processor to be implemented in every system to accept the request and process the result instantaneously.

Data Upload and Download with Entanglement

In the cloud network, there are various multi hops require a means of selecting a path through the network. A new approach is to build a forwarding table during the connection establishment stage with the implementation of the shortest path first algorithm to repeater networks. It can be said that the data transfer speed is hundred times faster than the normal speed of uploading and downloading to and from the cloud server. The repeater in the cloud network must provide the forwarding table with the algorithm to catalyze the data transfer speed. This approach will definitely embark the transportation in an easier and fast way.

Random Key Distribution for Fault Node Detection

This approach also concerns the fault node detection which actually affects the forwarding table which is dynamically created. For this reason, the random keys must be generated and distributed to every node once the network connection is established with the remote system. Periodically every node will be checked and each node must return true to intimate that it is live node otherwise the node will be localised and new forwarding table will be created. This can be done by matching algorithm which actually checks the key of every node that is distributed initially.

To make the transmission more fast, the resource allocation will also be occurred during the connection establishment for each node so that the more the requirement of resource the more will be the priority. On this basis the data upload and download will be done.

On the other hand, the entanglement swapping of qubits will be directed to a node as mentioned in forwarding table rather than to a specific node in a random manner. By rectifying the fault node, the paths then can be transparently relocated within the sub network. This approach makes the cloud environment to get rid of path constraint and simplifies the rearrangement of the forwarding table. The entangled states built within the network also must be named, to facilitate their management and delivery to the cloud storage. On the Internet, quantum keys are mapped to a connection using a tuple consisting of node (slave node) addresses, a connection identifier (port numbers), and possibly an application-level identifier. In quantum networks, such a tuple may not exist because at distributed state, the uploaded data might be at risk if any noise disruption occurs. So this approach will definitely reduces the delay of data transfer and simulate the power of transmission exponentially using quantum teleportation.

Conclusion

Quantum computing and cloud computing are two giants for futuristic computing. The quantum clouds, therefore, will be necessary for extremely fast data transfer and then it is highly secured enough for protecting the privacy of the data owner. Further in the cloud network, every node which is alive is updated with the current forwarding table such that flawless data upload and download streaming will be enabled. Moreover, this approach is quite promising for the detection of fault node through the distribution of random key. The speed of data transmission through the implementation of the shortest path is again added advantage to provide sophisticated cloud environment .The resources of quantum computation in a cloud environment, is to provide solution to the challenges and problems faced by present model of classical cloud computation. This technology improvement will give the better data security when comparing to other technologies that are dependent on algorithms like RSA possesses mathematical computations.

Future Work

In the near future quantum teleportation will be used with big data framework like Hadoop (IaaS) to improve the cloud technology in a flexible manner. The security will be once again strengthened by combining with OTP (One time Password).

References

Aaronson, S. (2007). *The limits of quantum computers*. In Proceedings of the 2nd International Conference on Computer Science: Theory and Applications.

Butler, B. (2012). *Cloud security: Outages are bigger risk than breaches*. Retrieved from http://www.infoworld.com/article/2613560/cloud-security/cloud-security-9-top-threats-to-cloud-computing-security.html

Buzek, V., & Hillery, M. (2001). Quantum cloning. *Physics World*, 14(11), 25-29. Retrieved from http://www.quantiki.org/wiki/The_no-cloning_theorem

Dieks, D. (1982). Communication by EPR devices. *Physics Letters A*, 92(6), 271-272.

Harrison, D. M. (2001). *Quantum Teleportation, Information and Cryptography*. Retrieved from http://www.upscale.utoronto.ca/PVB/Harrison/QuantTeleport/QuantTeleport.html

Lovgren, S. (April 18, 2004). *Teleportation Takes Quantum Leap*, National Geographic News. Retrieved from http://news.nationalgeographic.com/news/2004/08/0818_040818_teleportation_2.html

Matson, J. (2012). *Quantum Teleportation achieved over Record Distances*. Retrieved from http://www.sott.net/article/249799-Quantum-Teleportation-Achieved-over-Record-Distances

Moore, S. K. (2012). Computing's power limit demonstrated. *Spectrum*, 49(5),14.

Moorhouse, G. E., & Math, U. W. (1998). *Shor's algorithm for factorizing large integers*. Retrieved from http://www.google.co.in/url?sa=t&rct=j&q=&esrc=s&source=web&cd=6&ved=0CEcQFjAF&url=http%3A%2F%2Fwww.uwyo.edu%2Fmoorhouse%2Fslides%2Ftalk2.pdf&ei=j3gdVYnpPMGvsAHa3YGYAw&usg=AFQjCNHZyWj6CTG3nxCHS7p3pZggrCu5Qg&bvm=bv.89744112,d.bGg

Ouellette, J. (2013). *How Quantum Computers and Machine Learning Will Revolutionize Big Data*. Retrieved from http://www.wired.com/2013/10/computers-big-data/all/

Quantum Key Distribution. Retrieved from http://en.wikipedia.org/wiki/Quantum_key_distribution

Russell, J. (2008). *Application of quantum key distribution*. In IEEE Military Communications Conference.

Sharbaf, M. S. (2009). *Quantum cryptography: A new generation of information technology security system*. In 6th International Conference on Information Technology: New Generations.

Singh, H., & Sachdev, A. (2014). *The quantum way of cloud computing*. International Conference on Optimization, Reliability, and Information Technology, (pp. 397-400).

Singhal, S., Jain, A., Gankotiya, A. K., & Aggarwal, K. (2012). *An investigation on quantum teleportation*. 2nd International Conference on Advanced Computing Communication Technologies, (pp. 132-137).

Watrous, J. (2006). *Quantum Key Distribution*. Retrieved from https://cs.uwaterloo.ca/~watrous/CPSC519/LectureNotes/18.pdf

Wootters, W. K., & Zurek, W. H. (1982). A single quantum cannot be cloned. *Nature*, 299(5886), 802-803.