International Journal of Latest Trends in Engineering and Technology
Vol.(7)Issue(4), pp.378-382
DOI: http://dx.doi.org/10.21172/1.74.051
e-ISSN:2278-621X

THE QUANTUM KEY DISTRIBUTION(QKD) BASED SECURITY ENHANCED CLOUD DATA CENTER CONNECTIVITY

Sureshkumar P.H[1], Ambily Pramitha[2] and Dr. R. Rajesh[3]

Abstract- The quantum encryption capable of creating encryption codes that unbreakable with key distribution schemes that can't be intercepted .The power of quantum entanglement can provide a way of instantaneous communication that non-interceptable. The quantum encryption method can be implemented together with scenarios of conventional encryption methods safely. The quantum cryptography will replace conventional key exchange mechanism by using the polarized photons using channels like optic fiber cables that can provide far secure communication. The present day data centers ,which using for storing large amount of data, are connected with conventional cryptography and so it can be replaced with theoretically non-interceptable quantum cryptography mechanism as described in this paper. Obviously QKD will have uses in many areas of communication between remote data centers in cloud computing , defense networks etc.

Keywords – **Network security, Quantum cryptography, Quantum key distribution, Cloud data center**

I. INTRODUCTION

The research on quantum cryptography is very important in future scenarios of computing. The aim of quantum encryption is to create encryption codes that are absolutely unbreakable and key distribution schemes that are non-interceptable [1]. So quantum encryption systems is virtually fail safe against hackers because QKD(Quantum Key Distribution) is considering as far safer[2]. The enormous computing power of quantum computers cause large increase in key length of conventional cryptography but same time it can be used for breaking short key distribution scenarios[3]. The various malicious activities like stealth attack and crimes are increasing day by day over the communication networks[4]. Various attacks over the critical computer networks causes the losses of billions of dollars and can challenge the security of nation. The implementation of quantum key encryption can increase the security of crypto system significantly. So this work can help to the prevention of the malicious activities over the communication networks and increase security of the communication systems.

The research on quantum cryptography is very important in future scenarios of computing. The aim of quantum encryption is to create encryption codes that are absolutely unbreakable and key distribution schemes that are non-interceptable [1]. So quantum encryption systems is virtually fail safe against hackers because QKD(Quantum Key Distribution) is considering as far safer[2]. The enormous computing power of quantum computers cause large increase in key length of conventional cryptography but same time it can be used for

[1] *Bharathiar University, Coimbatore*
[2] *Depaul Institute of Science &technology, Angamaly , Kerala*
[3] *Sree Narayana Gurukulam College of Engineering, Kolencherry, Kerala*

breaking short key distribution scenarios[3]. The various malicious activities like stealth attack and crimes are increasing day by day over the communication networks[4]. Various attacks over the critical computer networks causes the losses of billions of dollars and can challenge the security of nation. The implementation of quantum key encryption can increase the security of crypto system significantly. So this work can help to the prevention of the malicious activities over the communication networks and increase security of the communication systems.

II. QUANTUM CRYPTOGRAPHY PAST AND PRESENT

In the 1980s, C. Bennet, P. Benioff, R. Feynman observed that a new powerful way of information processing can possible with quantum systems . Richard Feynman was the first proposed in 1981 that quantum-mechanical systems could be more powerful than classical computing methods [5] , so eventually concept of quantum computing was born. David deutsch further studied it and published a paper in 1985 [6]. However the origin of quantum cryptography was considering as started from 1983 from the work of weisner[7] .He proposed that single quantum states could be used for information transmission. David deutsch suggests an alternate for the present day turing machine with the quantum computing system , Which is more powerful including generate genuinely random numbers, perform some parallel calculations with the single register using and so it could be performed the simulations very efficiently

Later ,In 1989, Deutch published another paper “Quantum computational networks"[9] and proposed a new quantum circuits that quantum gates can combine for quantum computation as the boolean gates to achieve classical computation so quantum circuits can do well. A further advance in theoretical quantum cryptography happened in 1991 when Ekert suggested that Einstein-Podolsky-Rosen (EPR)[10] entangled two-particle states could be used to implement a quantum cryptography.

III. BB84 ALGORITHM

After the origin of quantum cryptography in 1983 by weisner , a new coding scheme, that was the first proposed and to be known as the BB84 algorithm[11]. This algorithm is based on the uncertainty principle and formulate that any eavesdropper intercepting and measuring the quantum states of particles will also be altering those states. Photons used here is polarizing either horizontally and vertically or diagonally for each representing to a 0 or 1 respectively.

The algorithm for BB84protocol as follows:

1. The sender(alice) chooses a random bit string and a random sequence of polarizations
2. She then sends the other user (Bob) continues of photons each representing one bit of the string.
3. Bob randomly chooses to measure each arriving photon rectilinearly or diagonally.
4. Bob tells Alice the polarizations he used for measurement via public channel.
5. Alice tells Bob about measurements which only correct.
6. Bob and Alice selects a certain number of bits to check for tampering by comparison. At this point Alice and Bob have successfully exchanged a key without fear of eavesdropping by the third party Eve.
7. Because of the uncertainty principle, attempting to measure in one polarization will effectively randomize the other.
8. The quantum key distribution based communication link(QKD Link) between the alice and bob can represented as the figure-1 below. The quantum channel is using for the secure quantum cryptography based key transfer. The classical channel is using for the conventional

data transfer between devices by the medium like optic fibre cables or wireless channels. The figure-2 represents the polarization of photons and corresponding bit values zero or one.

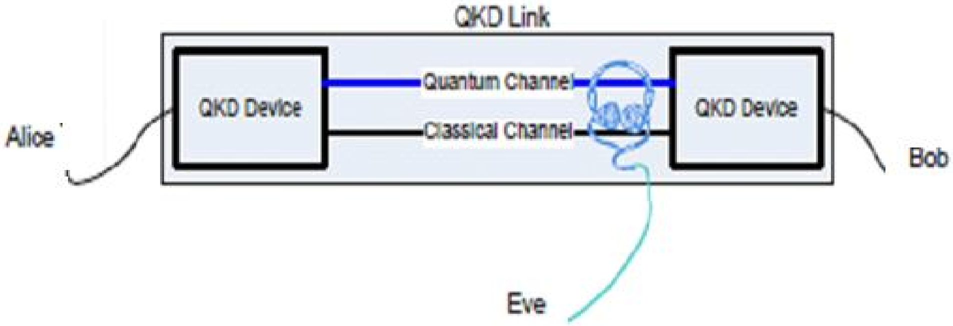

Figure -1 Quantum communication

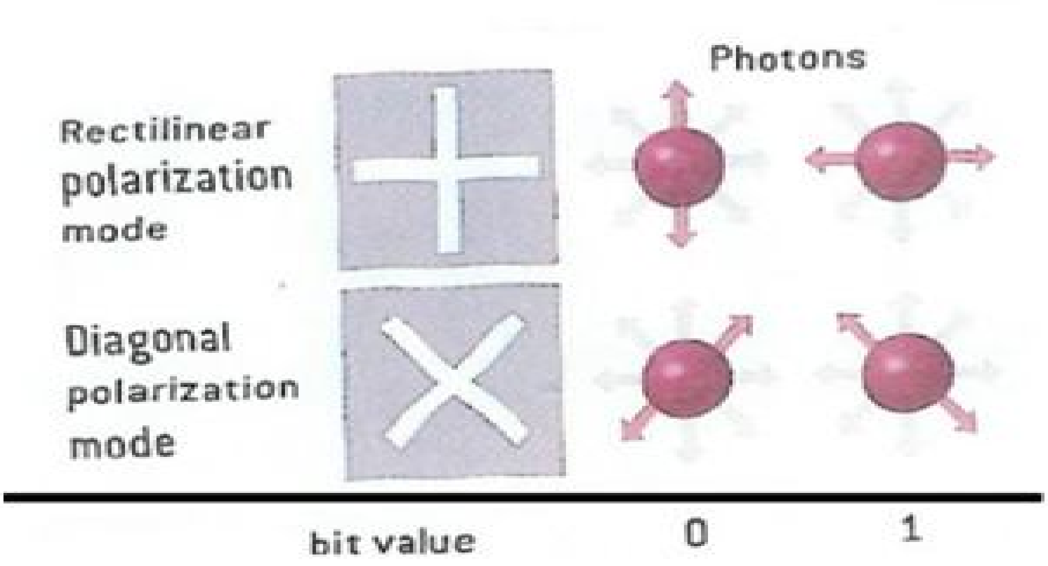

Figure-2 Polarized photons and corresponding bit values

IV. QUANTUM KEY DISTRIBUTION BASED DATA TRANSFER

Alice and bob performs the quantum key distribution as following steps

1)Alice communicates with Bob via a quantum channel sending him photons.

2)Then they discuss results using a public channel

3) After getting an encryption key Bob can encrypt his messages and send them through any public channel. But data being sent out are random, and any incorrect reading effectively destroys the information, any attempt at eavesdropping will not only be unsuccessful, with half the key being correctly found, but Bob and

Alice would no longer have the same key due to the lost information, making the eavesdropper's presence known to both parties .

4)The disadvantage to the BB84 method being that it while is secure when only one photon is sent for each bit, current lasers can often send multiple photons, allowing Eve to intercept one without the other parties knowing it.

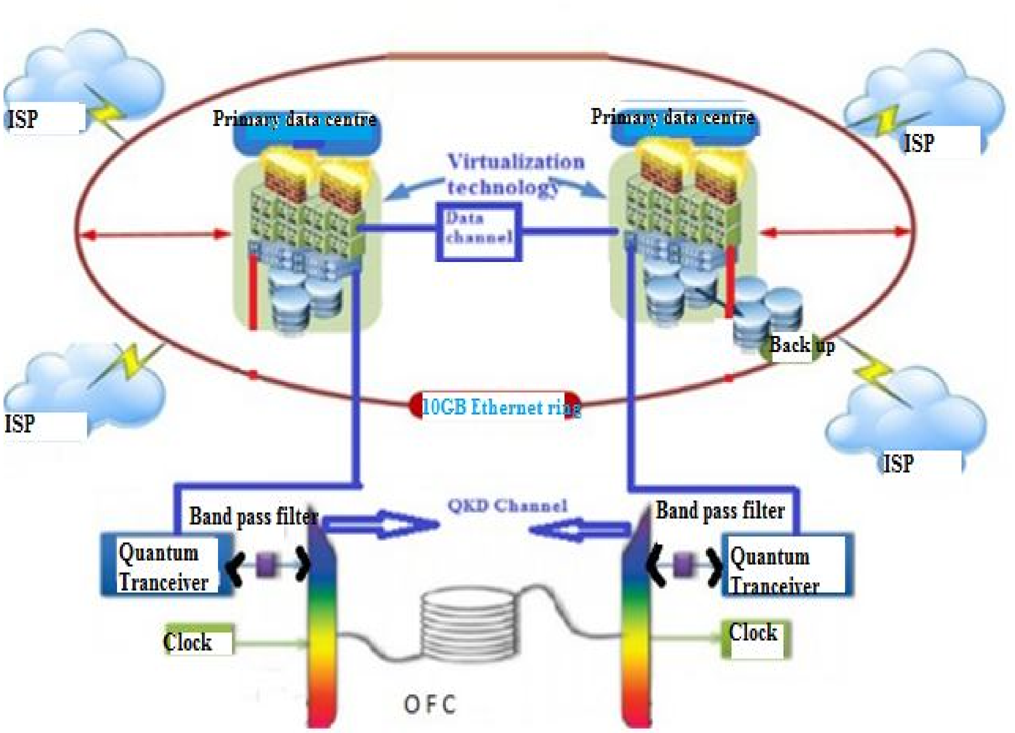

Figure-3 Proposing cloud data center connectivity with quantum key distribution

V. FUTURE POSSIBLE HIGH SECURITY DATA CENTER CONNECTIVITY WITH QUANTUM KEY DISTRIBUTION(QKD)

Quantum key distribution can protects individual’s connections with the outside world. It can protect the personal privacy without any delay of information exchange ,Which guarantees the information exchange with theoretically hundred percentage protection

A. Cloud Infrastructure

Cloud infrastructure has been constructed using high class technology providing a suitable platform for the business critical requirements clients[12].

B. *Virtualization technology* from the industry leader that to meet stringent Business Continuity requirements as well as the ultimate in flexibility

C. *Sophisticated network devices* Providing high speed, reliable networking infrastructure to satisfy high speed data communication with high speed switching capacity ,Performance, including two factor -SSL remote connectivity and WAN .

D. *QKD channel* The quantum Key Distribution(QKD) channel is using for sending keys of encryption throuh quantum channel .The software and hardware presently using in data centres shall be adapted to the quantum communication forsending keys or newly developed in near future .

E. *Point-to-point links:* A point-to-point connection refers to a communications connection between two nodes or endpoints . The QKD devices are directly connected over a short distance (D. Deutsch:1992) . Now QKD technology is progressing and so the structure of the QKD systems are evolving So this technology may be used in future quantum networks in cloud computing.

F. *Optical switching network:* Multiple QKD devices connected in a network with optical s witches to allow connections. Optical communication distance increasing by this method . The switches need not be trusted. One example of such a network is the DARPA quantum network . Multiple QKD devices connected in a network with optical s witches to allow connections. Optical communication distance increasing by this method . The switches need not be trusted. One example of such a network is the DARPA quantum network .

G. *Networks of trusted relays:* Multiple QKD devices are connected in and acts as classical relays that relay information from distant nodes. This type of QKD network is needs to be further evolved for the use of cloud infrastructure.

H. *Fully quantum repeater network*: Multiple QKD devices are arranged in a network with quantum repeaters. So the quantum repeater nodes allow entanglement to be connected across longer distances and QKD can operated between distances. a network.

REFERENCES

[1]. Gui Hua Zeng , " Quantum Private Communication" , Spring series ,pp 23-30, 2010.

[2]. Richard J. Hughes D. M. Alde, P. Dyer, G. G. Luther, G. L. Morgan and M. Schauer, "Quantum cryptography" ,arxiv.org, 1999.

[3]. Diffie,W and HellmanL, "New Directions in Cryptography" , IEEE Transactions on Information Theory, No. 6 ,1976.

[4]. F.Cohen, "simulating cyber-attacks, defense and consequence" , IEEE symposium on security and privacy,Berkeley,CA,1999.

[5]. Richard P Feynman , "Simulating physics with computers , International journal of theoretical physics" . Volume 21 , Nos 6/7 , 1999

[6]. David Deutsch 'Quantum theory, the Church-Turing principle and the universal quantum computer' , Proceedings of the Royal Society of London A 400, pp 97-117 , 1985.

[7]. S J Weisner:1983, 'Conjugate coding' , SIGACT News 15:1 , pp 78-88 , 1983

[8]. I.L.Chuang, L.M.K. Vandersypen, X. Zhou, D.W. Leung, and S. Lloyd, "Experimental realization of a quantum algorithm. Nature", pp 143-146, 1998.

[9]. D. Deutsch. "Quantum computational networks". Proceedings of the Royal Society of London, Series A, 1992 AK. Ekert, Phys. Rev. Lett . pp 67, 661 ,1991.

[10]. C.H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing", Proceedings of IEEE International Conference on Computers, Systems, and signal Processing, Bangalore, India, 1984

[11]. Raghu Yeluri, and Enrique castro-leon, "Building the infrastructure for cloud security", Apress Media , pp 123-159, 2014