Securing Cloud Computing Environment using Quantum Key Distribution

Akhilesh Yadav
Computer Science & Engineering
Galgotias college of Engg & Tech.
Greater Noida, UP

Manish
Computer Science & Engineering
Galgotias college of Engg & Tech.
Greater Noida, UP

Rani Tiwari
Computer Science & Engineering
Galgotias college of Engg & Tech.
Greater Noida, UP

Rishabh Jain
Assistant Professor
Computer Science & Engineering
Galgotias college of Engg & Tech.
Greater Noida, UP

ABSTRACT
Nowadays, Information Technology group is undergone significant shift in computing and protecting business value by using well-built, workable and authentic replacement of Cloud Computing. Cloud Computing is a contemporary computational architecture that provides another type of model. Cloud Computing provides substantial measure of computing, storage services, Data classification, IT assets and data management and cyber security. An unauthorized user may be accessed this data through virtual machines. This uncertainty creates a big problem. Cloud Computing is used in both public and private sector due to its accessibility, availability, and cost effectiveness. However, security of data transfer between client and server is still a big problem. Many scientists and researchers have brought up another cryptographic subject in Quantum Computing which is called Quantum Key Distribution (QKD). The first QKD protocol is BB84 that was presented by Charles Bennett and Gilles Brassard in 1984 [4]. This paper proposes as a service of Advanced Quantum Cryptography in Cloud Computing. This paper discusses the security issues of cloud computing and the role of cryptography technique in Cloud computing to enrich the Information Security [13].

Keywords
Cloud Computing, Quantum Key Distribution, Information Security, Cryptography, BB84.

1. INTRODUCTION
Cloud Computing is a latest service model which has a great development with the benefit of flexible configuration. Cloud Computing provides a new way of services by arrange systematically different resources and providing them to the clients according to their needs [11]. Similarly, capability to serve on demand and share causes it to be strong and supportable. Cryptography has been founded for many years as algorithms. They are established on complex functions. Now, the quantum key distribution is used in an information security that based upon public and private keys, which are totally based on complicated algorithms such as RSA, El-Gamal, or SHA [2]. All these algorithms are secure but if the scientists find the solution to establish quantum key distribution protocol for providing the secret key for exchanging information between different organizations and users that will replace all conventional algorithms immediately. The first QKD protocol is the BB84 published by Bennett and Brassard in 1984. After that, the security of BB84 has not been approved until many years of its introduction. some of which are protocol schemes that are very interesting and hold sparkling ideas in this field such as B92, SARG04, COW, KMB09 and EPR. In this paper, we will discuss the most common quantum key distribution protocols and focus on the mechanism that is used in each protocol to extract the power and the weaknesses of each protocol.

2. LITERATURE SURVEY
2.1 Quantum Cryptography
QKD is a key formation protocol which creates a regular key by using quantum characteristics of light to exchange information from sender to receiver and receiver to sender [11]. Cryptography is a process of study of techniques to provide a secure communication. In traditional cryptography protocols follows the principle of computer science, mathematics and electronics. Cryptography refers encryption of plaintext to cipher text and decryption of cipher text to plaintext. Two widely used key distribution techniques are public key cryptography and secret key cryptography. The secret key and the public key having unique flaws. The problem in the public key cryptography is that it is based on staggering size of numbers that are used by the algorithm to encode the message. To understand every bit of output data, understanding of every bit also very necessary. That means to crack 128 bits key we need number up to 10^{38} numbers [15]. Quantum computer will replace the current computers in near future, since they work on quantum level, these can achieve a speed, which could not possible till now. So that codes which would take billions of years to resolve could possibly cracked in very few time. It means secret key cryptography is also not going to be secured in near future due to quantum computers [13]. A threat to the security of cryptography by the quantum computer, may available in near future, gave rise to a new technology called quantum cryptography, which uses quantum mechanical effects and Heisenberg's principle.

2.2 Heisenberg Uncertainty Principle
According this principle, it is not possible to measure the quantum state of any system without disturbing system itself [13].

Heisenberg Uncertainty principle state that the product of uncertainty in related physical quantities.

$$\Delta x.\Delta p \geq \hbar/2$$

$$\Delta x.\Delta p \geq h/4\pi$$

ħ →Planck's reduced constant

h → Planck's constant

but here is the derivation for uncertainty principle in quantum

mechanism for two operators, x and y are the operators that do not commute, let iC is the commutator of x and y.

$$[x, y] = iC$$

For further evaluation

$$\langle\langle\Delta x\rangle^2\rangle\langle\langle\Delta y\rangle^2\rangle \geq ¼ \|\langle [x, y]\rangle\|^2$$

$$(\Delta x) = \langle(X - \langle X\rangle)^2$$

$$(\Delta y) = \langle(Y - \langle Y\rangle)^2$$

According to HUP, two interrelated properties cannot be measured individually without affecting others [6].

Thus, the polarization of photon can only be known at the point when it is measured.

In Quantum Cryptography, the secret key is sent to the receiver in a very secured way that keep secured and secret shared key, when the key has been adequate sent and obtain and further step to provide effective and secured information to the receiver. The sender provides a secret key to the receiver which is used to decrypt any message or details that are to be send in future.

3. EXISTING STUDY

Quantum cryptography is based on quantum mechanics, qubit used in quantum key distribution cannot be reversed without the possibility of making changes in the original state. In order to share a sequence of bits between two parties such as John and Richard make use of quantum channel to finalize security. The BB84 protocol supports quantum cryptography where quantum channel is used by both the participants to send qubits.

Table 4 State Table

States	Bases	Values
|0>	A	0
|1>	A	1
|+>	B	0
|->	B	1

Let's suppose John wants to send message to Richard, John prepares

16 bits

0101100010101100

In the following bases,

BAABAABAAAABBBBA

Thus, the following states are sent to Richard: +10-10+0101+--+0.

4. IMPLEMENTATION

4.1 Exchanging Message using photon

The essential information required to represent information using photon and which representation is used for describing the nature of photon in different situation. Photon is the smallest particle of the light and it has mainly three types of spin [8].

They are given below.

1) Horizontal

2) Vertical

3) Diagonal

The photon has the ability to rotate in all three spins and at a time in one direction. Polarization can be used to polarize a photon so that it has a particular move, directly or side to side. The following tables explain, how to information exchanging using photons.

Table 1 Following table explain how to transfer details using photons

Spin	Horizontal (-)	Vertical (|)	Left Diagonal (\)	Right Diagonal (/)
Value	0	1	0	1

Let take an example, how to deliver information using photon polarization

Table 2 Example of Photon Polarization

Sender Polarization	X	X	+	+	X	+	+	+
Sender Spin	\	/	_	|	/	_	_	|
Sender Value	0	1	0	1	1	0	0	1

Now the key in binary form is 01011001(Sender value). This binary information can be sent in other form like integer and sequence form also. The key selection method totally based upon the sender and receiver interaction. In this example sender also want to send the information in Integer form.

Table 3 Binary Structure and integer structure of Key

Binary Structure	01011001
Integer Structure	89

Sender can send secret value in Integer form (89).

5. ACKNOWLEDGEMENT

It is with tremendous respect that I acknowledge the priceless guidance and support of my "Guru", Rishabh Jain (Galgotias College of engineering & technology, Greater Noida). I would like to dedicate this paper to him. My sincere thanks go to my respected sir for his valuable, timely guidance who provided awareness and experience that greatly assisted the research.

6. CONCLUSION AND FUTURE WORK

The techniques comes from the classical computer science are applicable to quantum key distribution. It is a sign that quantum cryptography is a latest and new field of research. This paper introduced the quantum cryptography and quantum

key distribution protocols with the help of quantum states, qubits and photon rotations. This survey explains the working of BB84 quantum key distribution protocol. Quantum key distribution can be using quantum gates in a secure manner. The quantum gates operate on number of qubits which are building block of quantum gates.

As we know quantum cryptography is secure enough on paper but it can no longer on paper when implemented on physical device. There are numbers of scientists who build a physical device to implement quantum cryptography but the results of their lab experiments are different from paper work. BB84 protocol used to implement quantum key distribution that uses the photons polarization states to transmit information with high security. To increase security of physical quantum key distribution devices we can implement fibre optics with the combination of photonic simulator.

7. REFERENCES

[1] Prof. Suraj R. Pardeshi, Prof. Kailash D. Kharat, Prof. Vikul J. Pawar, Department of Computer Science and Engineering Government College of Engineering Aurangabad, Maharashtra, India, "Enhancing Information Security in Cloud Computing Environment Using Cryptographic Techniques" IEEE International Conference on cloud computing, 2016.

[2] Jashanpreet Pal Kaur, Rajbhupinder kaur, Yadavindra College of Engineering, Talwandi Sabo, Bathinda Punjab, "Security Issues and Use of Cryptography in Cloud Computing" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 7, July 2014, ISSN: 2277 128X.

[3] Wang, L., Tao, J., & Kunze, M. (2008). "Scientific cloud computing: Early definition and experience". Proceedings of the 10th IEEE International Conference on High Performance Computing and Communications, Austin, TX, 825–830.

[4] Nelson Gonzalez, Charles Miers, Fernando Redígolo, Tereza Carvalho, Marcos Simplicio, "An quantitative analysis of current security concerns and solutions for cloud computing" Springer 2012.

[5] Er. Sharanjit Singh, Er. Rasneer kaur (IJETCAS) ISSN (Print): 2279-0047 , ISSN (Online): 2279- 0055.

[6] Reservoir Project [URL]. http://www-03.ibm.com/ press/ us/ en/ pressrelease/23448.wss/, access on June 2008.

[7] Amazon Elastic Compute Cloud [URL]. http://aws.amazon.com/ ec2, access on Nov. 2007.

[8] IBM Blue Cloud project [URL]. http://www-3.ibm.com/pressrelease/us/en/ pressrelease/22613.wss/, access on June 2008.

[9] Wang, H., Sheng, B. and Li, Q. (2006) 'Elliptic curve cryptography based access control in sensor networks', Int. J. Security and Networks,Vol. 1, Nos. 3/4, pp.127–137.

[10] Ms Bhavana Sharma, B.P.I.T., Rohini, Delhi-"Security Architecture Of Cloud Computing Based On Elliptic Curve Cryptography (Ecc)"- Special Issue: Proceedings of 2nd International Conference on Emerging Trends in Engineering and Management, ICETEM 2013.

[11] Wikipedia, the free encyclopedia of Cloud Computing.

[12] Veerraju Gampala, Srilakshmi Inuganti, Satish Muppidi, "Data Security in Cloud Computing with Elliptic Curve Cryptography""- International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-3, July 2012.

[13] http://www.inforisktoday.in/5-essential-characteristics-cloudcomputinga-4189

[14] Akashdeep Bhardwaja, GVB Subrahmanyamb, Vinay Avasthic, Hanumat Sastry, "Security Algorithms for Cloud Computing" - International Conference on Computational Modeling and Security (CMS 2016), Procedia Computer Science 85 (2016) 535 – 542.

[15] Shweta Sharma, Bharat Bhushan, Shalini Sharma - "Improvising Information Security in Cloud Computing Environment"- International Journal of Computer Applications (0975 – 8887) Volume 86 – No 16, January 2014.

[16] Neha Roy, Rishabh Jain, "Virtual Machine Scheduling on Clouds Using DVFS" - International Journal of Advanced Research in Computer Science and Software Engineering ISSN: 2277 128X, Volume 5, Issue 5, May 2015.

[17] Pooja Ahlawat, Poonam, Rishabh Jain, "An Improvement to Life of Wireless Sensor Network Using Leach Design a Cluster Head"- IJCSMS (International Journal of Computer Science & Management Studies) ISSN(Online) : 2231-5268,Volume 15, Issue 06, June 2015.

[18]