Indian Journal of Science and Technology, *Vol 10(7), DOI: 10.17485/ijst/2017/v10i7/110897, February 2017*

ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Cryptography as a Service (CaaS): Quantum Cryptography for Secure Cloud Computing

Rashidah Funke Olanrewaju[1], Thouhedul Islam[1], Othman O. Khalifa[1], Farhat Anwar[1] and Bisma Rasool Pampori[2]

[1]Department of Electrical and Computer Engineering, Kulliyyah of Engineering, International Islamic University Malaysia, Kuala Lumpur, Malaysia; frashidah@iium.edu.my, tisuchi@gmail.com, khalifa@iium.edu.my, farhat@iium.edu.my

[2]Department of Information Teachnology, Central Univerity of Kashmir, Nowgam Campus-II, (Near Puhroo Chowk, Nowgam Bye Pass), Srinagar – 190015, Jammu and Kashmir, India; bismarasoolhr@gmail.com

Abstract

Cloud Computing is an emerging technology nowadays. Due to the accessibility, availability, and cost effectiveness, cloud computing has became essential computing system in both, private and public sectors. However, secure data transfer is still a big question where transferring link between user and server are not stabilized yet. As a result, many cloud users lost their valuable data. However, this paper proposes as integrated service of Advanced Quantum Cryptography with Cloud Computing. To ensure the secure Cloud Environment between sender and receiver, Quantum Cryptography proposes the use of photons and physics to generate cryptographic keys.

Keywords: Cloud Computing, Cryptography, Cloud, Quantum Cryptography

1. Introduction

The word, Cloud, itself is a metaphor of Cloud. The concept of using the word Cloud in computing world is t make it more sensible to users in order to integrate the availability, accessibility, reliability, security and cost[1]. Due to the improvement of cloud concept over other computing systems, within a short period of time, cloud reduction has easily reached everywhere and became trustworthy[2].

Cloud Computing provide 3 types of service oriented computing3, i) Software As A Service (SaaS), ii) Infrastructure As A Service (IaaS), and iii) Platform As A Service (PaaS) provide huge flexibility to clients. Client can choose the suitable service for business. In terms of development mood in cloud environment, it provide 3 flexibility; public, private and hybrid; that enhance developer's workflow.

Due to 65% uses of cloud by giant business company[2] in the world, it has a huge demand now and will be in future. Google, Twitter, Amazon are totally cloud oriented. In 2014, many account security passwords to Drop box records have been leaked out in the newest security violation, with online hackers harmful to launch large numbers more consideration information in exchange for Bit coin. Hackers, who were obviously able to access weak logins and security passwords through a third-party service, leaked out 400 consideration security passwords and usernames on to site Paste bin. The publish confronted that 6.9 thousand further Drop box consideration information had been acquired, such as images, video clips and other files. In another report, Fear aware as Islamic Region's 'cyber caliphate' hacks more than 54,000 Twitter accounts. Both of the services, twitter and drop box are hosted in cloud computing where they are still struggling to stabilized the security issue in cloud. [4,5] is NOT a new requirements to protected and decrypt details. Rather it is an approach of Quantum Cryptography using photons to generate a cryptographic key and transfer it to a recipient using a appropriate interaction route. A cryptographic key works the most aspect in cryptography; it is used to protected / decrypt details.

**Author for correspondence*

To help make secure cloud environment, Quantum Cryptography and cloud could be the best choose while Quantum Mechanic is depends on photons and physics to generate cryptographic keys.

In the first part of this paper, the basic mechanism of cloud computing will be discussed. In second portion, mechanism of quantum cryptography has been described. In following part, cloud and quantum cryptography has been integrated. Evaluation, Discussion and future work are described in the last part in this paper.

2. Mechanism of Cloud Computing

2.1 Service as a Cloud

One of the main flexibility of cloud computing is service[6] i.e. i) Software As A Service (SaaS), ii) Infrastructure As A Service (IaaS),as a cloud. Cloud offers 3 types of services and iii) Platform As A Service (PaaS). These 3 services particularly working for environmental issue of cloud computing[17]. It ensures working environment of cloud based on users demand.

2.1.1 Software as a Service (SaaS)

Software operates on computer systems possessed and handled by the SaaS provider, compared to set up and handled on user computer systems. The application programs are utilized over the public Internet and generally offered on a monthly or annually subscription system. It allows user to use software only.

- Web access to professional software
- Program is handled from a central location
- Program provided in a “one too many” model
- Customers not required dealing with software improvements and patches
- Program Development Connections (APIs) allow for incorporation between different items of software

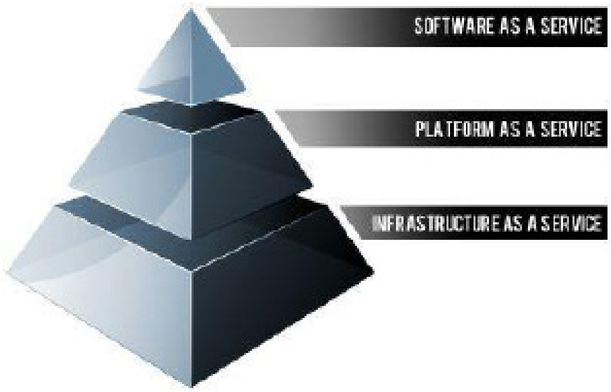

Figure 1. Classification of services of cloud.

2.1.2 Infrastructure as a Service (IaaS)

Computing, storage, social media, and other components (security, tools) are provided by the IaaS company via public Internet, VPN, or devoted system relationship. Customers have independence to own and handle operating-system, programs, and information running on the facilities and pay by utilization.

2.1.3 Platform as a Service (IaaS)

All application and elements needed to create and performance cloud-based applications are provided by the PaaS company via group Internet, VPN, or dedicated program connection. Clients pay by use of the program and control how applications can be used throughout their lifecycle.

2.2 Development as a Cloud

In terms of development environment, cloud provides 3 types of development facilities. i) Private Cloud ii) Public Cloud and iii) Hybrid Cloud. Such kind of facilities brings huge elasticity for instant development for up and running application without interruption.

2.2.1 Private Cloud

Private reasoning is reasoning facilities devoted to a particular company. It allows companies to variety programs in the reasoning, while dealing with issues regarding information protection and control, which is often missing in a public reasoning atmosphere. It is not distributed to other companies, whether handled internal or by a third-party, and it can be organized internal or on the outside.

There are two types of private clouds:

1. On-Premise Private Cloud: This type of reasoning is organized within an companies own service. A companies IT division would have the main city and functional expenses for the actual physical sources with this design. On-Premise Personal Atmosphere is best used for programs that require finish control and configurability of the facilities and protection.

2. Externally Hosted Private Cloud: On the outside organized private atmosphere are also specifically used by one company, but are organized by a third party dedicated to reasoning infrastructure.

2.2.2 Public Cloud

Community atmosphere are made available to people by a service agency who serves the reasoning facilities. Community reasoning suppliers like Amazon.com AWS, Microsoft company and Google own and function the facilities and offer access over the Internet. Clients have no exposure or control over where the facilities is located. All customers on public atmosphere share the same facilities present to restricted settings, security rights and accessibility variances.

2.2.3 Hybrid Cloud

Several Atmosphere are a structure of two or more clouds (private, group or public) that remain unique organizations but is limited together providing the advantages of multiple implementation designs. In a hybrid reasoning, user can make use of third party reasoning suppliers in either a full or limited manner; increasing the freedom of processing. Boosting a traditional personal reasoning with the time of a group reasoning can be used to handle any surprising rises in workload.

3. Existing Encryption Technology in Cloud

Existing Cloud Technology are using traditional cryptography algorithm to make secure data encryption. Different types of algorithm are used depends on different could service providers. The most common used algorithm are[7,8]

3.1 RSA

A cryptographic criteria whose security key is community and is different the decryption key which is kept secret ii) Information Encryption Conventional (DES) and Makes easier Information Encryption Conventional (S-DES), where DES used symmetrical key for security and decryption

3.2 Secure Outlet Layer (SSL) 128 Bit Security

It is commonly-used method for managing the security of a message transmitting on the Internet and it uses community and private key security system.

However, the traditional encryption system has some vulnerability while hackers are able to replicate public and private keys.

4. Quantum Cryptography

Quantum cryptography is not a new specifications to secured and decrypt information. Rather than using statistical strategy, it is an approach of using photons to produce a cryptographic key and return it to a recipient using a appropriate relationships path[9,10]. A cryptographic key works the greater degree in cryptography; it is used to secured/ decrypt information. There are two types of cryptography. i) Symmetric Cryptography and ii) Asymmetric Cryptography.

4.1 Symmetric Cryptography

[11]are means of cryptography that use the same cryptographic key elements for both Symmetric-key algorithms protection of plaintext and decryption of cipher text. The key elements may be identical or there may be a simple adjustment to go between the two key elements. The key elements, in work out, represent a allocated key between two or more activities that can be used to have a individual information weblink[12]. This need that all parties get availability to the key is the most significant drawbacks of shaped key protection, in comparison to public-key protection.

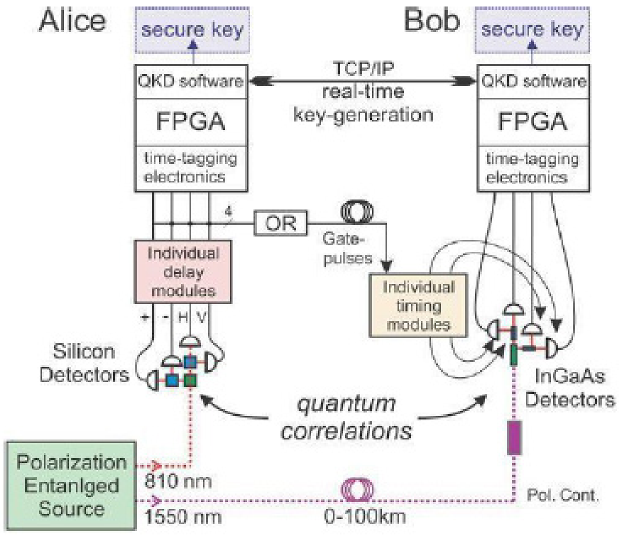

Figure 2. Communication cryptography with quantum mechanism.

Symmetric-key protection can use either circulation ciphers or avoid ciphers i) Flow ciphers protected the figures (typically bytes) of an idea one at a short time. And ii) Prevent ciphers take a wide range of items and protected them as a individual system, support the plaintext so that it is a several of the avoid sizing. Stops of 64 items have been usually used. The Impressive Security Traditional (AES) requirements approved by NIST in Dec 2001 uses 128-bit prevents.

4.2 Asymmetric Cryptography

Asymmetric cryptography or public-key cryptography is Cryptography[10,11] in which a number of key elements is used to protected and decrypt an e-mail so that it comes securely. Initially, a system client gets a group along with key several from accreditations power. Any other client who wants to provide an properly secured idea can get the developed recipient's group key from a group record. They use this key to protect the idea, and they provide it to the receiver. When the receiver gets the idea, they decrypt it with their individual key, which no one else should get connected to.

4.3 Quantum Cryptography's Mechanism

In quantum cryptography, the source provides a key to the receiver, and this key can be used to decrypt any future details that are to be sent. When the key has been effectively sent and acquired, the next step is to provide properly secured details to the receiver and let it decrypt and process those details. The key is the main section of cryptography and should be sent in a much secured way. Huge cryptography[1,2,3] has a different way of providing the key to the receiver. It uses photons to provide a key.

4.3.1 *How Proton it is used?*

A photon is the smallest particle of light. It has three types of spins, i) Horizontal, ii) Vertical and iii) Diagonal (Right and Left).

A photon has the ability to rotate in all three declares at once. Polarization can be used to polarize (pass through a filter) a photon so that it has a particular move, directly or side to side or tilted. Polarization of a photon is carried out using polarization purification.

Heisenberg's Doubt Concept[13], which states that it does not seem possible to assess together the velocity and position of a substance with highest possible perfection, and its situation will be different when measured. Simply, if an eaves dropper intercepts the passed down photons and goes it through its polarizer, if it is wrong way of life the receiver get a different photon. Hence the interception of connections will get identified.

It ensures that if a photon is polarized using say X filter (Diagonal Polarization), then to get the initial move of the photon only X filter can be used. If a + filter (Rectilinear Polarization) is used on the photon, then it will either be absorbed by the filter or the polarized photon, will be of different move than the initial photon. For example, a side to side spinning photon when gone through a bad filter will outcome in tilted move, which is wrong.

4.3.2 *How to deliver information using photons*

One of the important problems before using large cryptography is how to online details with photons. This matter can be easily set by offering the move of every photon as 0 or 13. Following desk will explain how to deliver details using photons-

Spin	Horizontal Spin (–)	Vertical Spin (|)	Left Diagonal Spin (\)	Right Diagonal Spin(/)

polarization, properly secured details can be sent and decrypted when acquired.

Value	0	1	0	1

Think about Alice is applicable polarizations on photons and gets the rotate and keeps a observe of it. Every rotate has a value associated with it.

Polarization	x	x	+	+	x	+	+	+	+	+	x	+	+	x	x	x
Spin	\	/	- -	|	/	- -	- -	|	|	- -	/	- -	|	\	/	/
Value	0	1	0	1	1	0	0	1	1	0	1	0	1	0	1	1

Alice is able to get the move of photon after polarization using four sensors (horizontal, directly, right tilted, staying diagonal).

Now the key in binary structure is: 0101100110101011

This binary information can become other types like sequence and integer, based upon selection of the customers engaged in the interaction. Believe Alice wants the key to be in integer structure, so the key will be:

Binary Data	0101100110101011
Integer Data	22955

5. Key Verification

Centered on above example, Alice used polarization and measured the value of the key, which will be passed on to Bob. The transmitting of these photons occurs in visual fibers wires[13,14].

Alice provides the polarized photons to Bob using the right connections path. Bob is listening to for incoming photons and randomly is appropriate any polarization (rectilinear or diagonal) and keeps a notice of used polarization, move and its value. When the transferring has completed, Alice and Bob link on a group path which needs not be properly secured. Bob shows Alice only the polarizations (not the move or value) he used for the exactly same sequence, and Alice only says YES/NO. This connections will be like appendix Table 1. In this connections, Bob gets to know a different polarizations. But exclusive clients have problem here which is defined in orange colour. Alice said polarization used is wrong but the move Bob acquired had the same bit value (1) as Alice's. But Bob has no strategy to locating what value Alice has so he has no other way but to remove his results for wrong polarization. After efficient key transferring and fixing of wrong polarization, properly secured details can be sent and decrypted when acquired.

6. Connections Interception

While client is intercepting the connections between emailer and receiver, then he will have to randomly apply polarization on the photons sent[15]. After polarization, client will forward it to the very first emailer. However it's hard the eaves dropper to think all polarizations effectively. So when Bob and Alice validate the polarizations, and Bob is not able to decrypt the details, then the interception of connections will get identified.

7. Integrating Cloud and Quantum Cryptography

Cloud computing is well accepted from users while it's provide flexibility of development, availability, cost effectiveness. Due to the accessible from everywhere, security is a big question where most of the existing way are failed to ensure protections. In this circumstance, this paper has proposed to use Quantum Cryptography in cloud computing to protecting data.

Quantum Cryptography use Protons to build encryption key that is almost impossible to break down for hackers while it[13]. This would help in believe in among the customers towards the reasoning will takes millions of years to break technological innovation. Also, the quantum thinking duo security would provide remarkable managing power with you of a lot. This means that clients will access the super-fast and guarded technology of thinking managing from anywhere using the internet. Such a technology would cause way for next development of managing which would make managing easier, secured and may cause a an blast in the area of mobile phones.

Table 1. Output spin for used polarization

Polarization	Output Spin	
Rectilinear Polarization (+)	Horizontal Spin (–)	Vertical Spin (|)
Diagonal	Left Diagonal Spin (\)	Right Diagonal Spin (/)

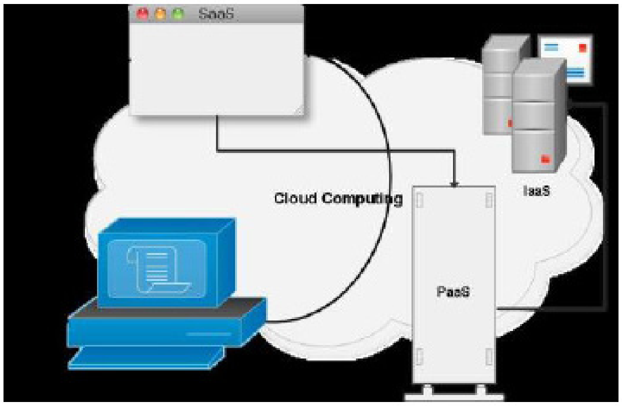

Figure 3. Cryptography as a Service (CaaS) in cloud computing.

8. Conclusion

Through this document, a new strategy to reasoning handling protection incorporated with huge cryptography has been suggested. This strategy provides grounds for yet another performance of reliable reasoning handling. The suggested procedure would offer many advantages in protection issue in reasoning handling in the foreseeable upcoming. Also, it would offer tremendous handling power in the hands of individuals. Moreover, such a technological innovation would lead way for next creation of protected handling which would make handling more convenient, reliable and may lead to a an explosion in the field of smart phones. In the foreseeable upcoming, individuals will use amazing technological innovation which would extremely impact our way of living. People can expect outstanding devices which could have never been thought of. Moreover, there would many new ways by which we will communicate with technological innovation and all these will be based on the ideas which today we term as stories.

9. Acknowledgement

This work was supported by Ministry of Higher Education Malaysia (Kementerian Pendidkan Tinggi) under Researcher Initiative Grant Scheme number (RIGS16-084-0248)

10. References

1. Grodzinsky FS, Wolf MJ, Miller KW. Quantum computing and cloud computing: humans trusting humans via machines. In Institute of Electrical and Electronics Engineers (IEEE) International Symposium on Technology and Society (ISTAS); 2011 May 23–25. p. 1–5. Crossref
2. A Microsoft Research Report. Achieving data privacy in cloud: study of information technology privacy and compliance of small to medium-sized organizations in the united state. In Independently Conducted by Ponemon Institute LLC; 2012 Jun. p. 2–14.
3. Chen CY, Zeng GJ, Lin F, Chou YH, Chao HC. Quantum cryptography and its applications over the internet. Institute of Electrical and Electronics Engineers (IEEE) Network. 2015 Sep; 29(5):64–9. Crossref
4. Li J, Chen S, Song D. Security structure of cloud storage based on homomorphic encryption scheme. In Institute of Electrical and Electronics Engineers (IEEE) 2nd International Conference on Cloud Computing and Intelligent Systems (CCIS). 2012 Oct 30 – Nov 1; 1:224–7. Crossref
5. Ghernaouti-Helie S, Sfaxi MA. Sharing information using quantum cryptography to reach the unconditional security. In Institute of Electrical and Electronics Engineers (IEEE) International Conference on Research, Innovation and Vision for the Future; 2007 Mar 5–9. p. 175–80. Crossref
6. Saroj SK, Chauhan SK, Sharma AK, Vats S. Threshold cryptography based data security in cloud computing. In Institute of Electrical and Electronics Engineers (IEEE) International Conference on Computational Intelligence Communication Technology (CICT); 2015 Feb 13–14. p. 202–7. Crossref
7. Singh H, Sachdev A. The quantum way of cloud computing. In International Conference on Optimization, Reliabilty, and Information Technology (ICROIT); 2014 Feb 6–8. p. 397–400. Crossref
8. Jaber AN, Zolkipli MFB. Use of cryptography in cloud computing. In Institute of Electrical and Electronics Engineers (IEEE) International Conference on Control System, Computing and Engineering (ICCSCE); 2013 Nov 29 – Dec 1. p. 179–84. Crossref
9. Sharma RD, De A. A new secure model for quantum key distribution protocol. In 6th Institute of Electrical and Electronics Engineers (IEEE) International Conference on Industrial and Information Systems (ICIIS); 2011 Aug 16–19. p. 462–6. Crossref
10. Ghonaimy MA. An overview of quantum information systems. In 8th International Conference on Computer Engineering Systems (ICCES); 2013 Nov 26–28. p. xx–xxxii. Crossref
11. Kaaniche N, Boudguiga A, Laurent M. ID based cryptography for cloud data storage. In Institute of Electrical and Electronics Engineers (IEEE) Sixth International Conference on Cloud Computing (CLOUD); 2013 Jun 28 – Jul 3. p. 375–82. Crossref
12. Grodzinsky FS, Wolf MJ, Miller KW. Quantum computing and cloud computing: humans trusting humans via machines. In Institute of Electrical and Electronics Engineers (IEEE) International Symposium on Technology and Society (ISTAS); 2011 May 23–25. p. 1–5. Crossref
13. Kollmitzer, Christian, Pivk, Mario. Applied quantum cryptography. Lecture notes in Physics, Springer. 2010; 797:23–47. Crossref
14. Liu F, Li H. Social network-based quantum trust management. In 2nd International Conference on Computer Science and Network Technology (ICCSNT); 2012 Dec 29–31. p. 487–90. Crossref
15. Niemiec M, Pach AR. Management of security in quantum cryptography. Institute of Electrical and Electronics Engineers (IEEE) Communications Magazine. 2013 Aug; 51(8):36–41. Crossref
16. Kaaniche N, Boudguiga A, Laurent M. ID based cryptography for cloud data storage. In Institute of Electrical and Electronics Engineers (IEEE) Sixth International Conference on Cloud Computing (CLOUD); 2013 Jun 28 – Jul 3. p. 375–82. Crossref
17. Olanrewaju RF, Islam T, Adeniyi AB. r-TOLA: An architecture for real time open learning application for universities. In International Conference on Computer and Communication Engineering (ICCCE); 2014 Sep 23–25. p. 292–5. Crossref

Appendix

Table 2.

Alice Polarization	x	X	+	+	X	+	+	+	+	+	X	+	+	X	X	X
Alice Spin	\	/	–	|	/	–	–	|	|	–	/	–	|	\	/	/
Alice Value	0	1	0	1	1	0	0	1	1	0	1	0	1	0	1	1
Alice Answer	Yes	No	Yes	Yes	No	Yes	Yes	No	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes
Bob Polarization	X	+	+	+	+	+	+	X	+	+	X	+	X	X	X	X
Bob Spin	\	–	–	|	|	–	–	/	|	–	/	–	\	\	/	/
Bob Value	0	0	0	1	1	0	0	1	1	0	1	0	0	0	1	1