A Study on Quantum Cryptography Based Security Management in Cloud

Priya Raina
Department of Computer Science and Engineering
UIET, Panjab University,
Chandigarh,India
priyaraina1807@gmail.com

Sakshi Kaushal
Department of Computer Science and Engineering
UIET, Panjab University,
Chandigarh,India
sakshi@pu.ac.in

ABSTRACT

Cloud Computing is the latest technology that has come to the center-stage because of its ability to achieve economies of scale, quite like mass-production. However, shifting to Cloud comes with certain strings attached, especially security concerns associated with outsourcing critical data and processing to a third party. One way to tackle the security issues can be approaching it using Quantum Computing, which itself is a highly researched area with huge expectations from the researchers. So far, the two fields (viz. Cloud Computing and Quantum Computing), have been researched independent of each other. The paper explains why they should be integrated. The paper presents quantum cryptographic protocols and studies their application in enhancing Cloud security, particularly Network security and Data security. Further, it outlines the work that can be done and finally, seeks to identify possible research directions.

Categories and Subject Descriptors

C.2.0 [**Computer-Communication Networks**] *Security and protection*

General Terms

Security

Keywords

Cloud Security, Quantum Computing, QC

1. INTRODUCTION

Cloud Computing is a trending technology that has been commercialised very rapidly in a span of few years. All want to go the cloud way- from individual users, who use applications like Dropbox to save their personal data on cloud, to organisations, which outsource their critical data and even processes to cloud providers. Thus, Cloud is a way of economizing and optimizing the resource usage in computing. Outsourcing of data and processes imply that the organisations can focus on their core capabilities, rather than wasting time and resources in maintaining server rooms and data centres. This is promising for both the Cloud user and the Cloud provider. In such a scenario, security becomes a real concern, for both users and providers.

Concerns about the safety of data and processes are hindering a large scale migration to the cloud.

Various solutions are available and are being developed to resolve the security issues associated with the cloud [27]. Classical cryptography is still in use but is threatened by the computation power of Quantum Computing. Post-Quantum Cryptographic techniques are being proposed in order to overcome this potential threat. These techniques include Lattice based and Coding based cryptosystems, Fully Homomorphic Encryption (FHE), to name a few. Work is also being done in the field of Multi Party Computation (MPC). However, not much work has been done to propose solutions based on Quantum techniques, probably because of specialized hardware it requires, and the fact that a "real" Quantum computer still seems a little far-fetched. But, the fact that giants like Google and IBM are showing interest in the technology means that it will be a reality soon and shall have a bright future. Quantum techniques can offer a lot to cloud security and its time that their potential role is acknowledged. They can be useful in enhancing network and data security in cloud, particularly on the server side. Confidentiality, privacy and authentication services can be provided by various mechanisms like protocols for secure key management, bit commitment, MPC, Blind Quantum Computation etc.

This paper introduces Quantum Cryptographic (QC) protocols and explores how they can be used to alleviate the security concerns in cloud. It is organized as follows. Section II introduces Quantum Computing to the readers. Section III gives a birds' eye view of QC and its protocols. Section IV presents a brief survey of work done so far in securing the cloud using QC and goes on to identify the open issues and highlight the proposed work. Section V concludes the paper and identifies some of possible the research directions and is followed by References.

2. QUANTUM COMPUTING

Quantum Computing is an emerging field that has attracted the attention of physicists and computer scientists alike, because it holds the possibility of bringing about a paradigm shift in our way of computing. Quantum Computing promises a radical change - not just a change in hardware or software, but a change in the very definitions of computer and computing. A Quantum Computer obeys the laws of Quantum mechanics, the physics behind subatomic particles.

2.1 Qubits and their properties

The fundamental unit in a Quantum Computer is a Qubit; which, unlike a "classical" bit, can exist in a state of "superposition" of 0 and 1, but on measurement(in standard basis) collapses to either 0

ICCCT '15, September 25-27, 2015, Allahabad, India

DOI: http://dx.doi.org/10.1145/2818567.2818672

or 1. Thus, a qubit in state $|\psi\rangle$ is represented in Dirac's Bra-Ket notation as follows:

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

Which simply depicts that the qubit in question collapses to state $|0\rangle$ with probability $|\alpha|2$ and to state $|1\rangle$ with probability $|\beta|2$, when measured in the standard basis.

2.2 Entanglement

Apart from superposition, which is a property exhibited by individual qubits, they demonstrate another interesting phenomenon: Entanglement. Entanglement is a tight correlation between two qubits such that the system formed by them can't be expressed as product of its components' state. The EPR or Bell states are the most well-known examples demonstrating this phenomenon:

$$|\beta 00\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \qquad |\beta 01\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}$$

$$|\beta 10\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}} \qquad \beta 11\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

Knowing the state of one of the qubits in the entangled pair leads to determination of the other. This holds good even if the qubits are separated by some distance, provided they continue to remain in the state of entanglement.

These phenomena along with the No-Cloning Theorem [28] form the basic premises of various applications of quantum computing, one of them being QC.

3. QUANTUM CRYPTOGRAPHY (QC)

3.1 Classical Cryptography

Cryptography is the study of techniques used for encryption and decryption of a secret message. There are classical techniques like Caeser cipher, block based symmetric ciphers like AES and DES where the encryption and decryption require same algorithm and asymmetric ciphers like RSA where encryption and decryption have different operations. Key distribution schemes are also studied under cryptography. The aim is to devise new techniques or modify the existing ones so that they are secure against malicious third party attacks. So far, the only cipher that has proved to be unbreakable is the one time pad or vernam cipher. However, the reason it is scarcely used is that it requires frequent exchange of keys, so frequent that it becomes impractical, as the keys once used are discarded. Asymmetric ciphers are rather popular these days and are used in several protocols used over the internet e.g. SSL and digital signatures. These techniques rely on the computational difficulty of calculating GCD (RSA) or finding discrete logarithms (Deffie Hellman). However, Shor's factorization algorithm [25] designed for quantum computers, even if only a simulation showed that these ciphers can no longer be relied upon. But it also proved to be an impetus to discover ways to overcome this problem and thus, research in fields like post-QC and QC gained momentum.

3.2 Quantum Key Distribution

First proposed by Weisner, QC is still in its infancy and is presently synonymous with Quantum Key Distribution (QKD). QKD seeks to resolve the practical issues facing one time pad by providing a way for generation of a truly random key between two principles wishing to communicate securely rather than key exchange. Apart from being used for key generation for one time pad, it can be combined with any scheme requiring use of a Key Distribution Centre. The advantages of using QC include the fact that it offers unconditionally security and thus capable of offering various levels of secrecy depending on the security of the encryption scheme it is used with [2]. It also is capable of detecting eavesdropping. Additionally it can be used to enforce Bit commitment, albeit only computationally secure [20][22][28], for communication between parties that don't trust each other. The disadvantages include susceptibility to masquerading attacks due to authentication issues for which solutions like quantum tagging have been proposed; denial of service attacks which happens in case eavesdropper listens so frequently that it is impossible for the principles to establish the key; and the infeasibility of incorporating it into existing networks due to requirement of specialized hardware [2][7]..

3.3 Popular Protocols

BB84: Proposed by Bennett and Brassard [6], the protocol uses any two pairs of conjugate states for key generation. The sender and receiver (Alice and Bob) are connected by a quantum channel and a classical channel. Alice sends random bits encoded in random non orthogonal axes ("+" and "x") to Bob over the quantum channel. Bob measures the states in randomly chosen bases. Then they reconcile the key over classical channel. The bits measured using same basis as used by Alice while encoding are retained and others are discarded. Alice then discloses some bits in the key, if the mismatch exceeds threshold, eavesdropping is detected and the key is dropped. Otherwise, after dropping the disclosed bits, the remaining ones serve as the shared key. This is shown in Figure 1(a) (taken from Benett Charles' slides).

B92: Proposed by Bennett[5], it is similar to BB84 but for the fact that it uses only two states. It too involves one quantum and one classical channel between Alice and Bob. Alice chooses a random vector of bits, A. She transmits $|0\rangle$ if Ai=0 and $|+\rangle$ if Ai=1. Bob measures the states in chosen basis, "+" or "x" (selected using a random vector B; Bi=0 leads to choosing "+"), and builds test vector with Ti=0 if he measures $|0\rangle$ or $|+\rangle$ and Ti=1 otherwise. Bob then sends the vector T over classical channel and the bits in A and B corresponding to Ti=1, are preserved as the raw key. Then Alice reveals some sample bits and if Ai≠1-Bi, Eve is detected and the key is discarded. Otherwise key is generated after elimination the sample bits. This is illustrated in Figure 1(b)[11].

EPR: Proposed by Ekert [13], it is a 3-state protocol based on entanglement, which is used to detect the presence of Eve. EPR pairs are generated and each bit in the pairs is sent to Bob and Alice. They select a measurement operator to measure it. Alice stores the measured value; Bob stores the complement of the measured value. During classical communication, they identify the bits where they used the same measurement operators and establish the raw key. The remaining bits form the rejected key and are tested for Bell's inequality. If they satisfy the inequality, presence of Eve is assumed and the raw key is discarded [11].

4. APPLICATIONS OF QC IN CLOUD SECURITY.

4.1 Work Done

Two ways have been suggested for applying QC in the cloud context:

Direct application where QKD is used for securing the communication between the client and the server over a quantum network like BBN or SECOQC [17] [18][19]

Indirect application where blind quantum computation is used, which is a technique based on QC designed to secure the client's data against an untrusted server [3] [4] [8] [23] [26].

Table 1 lists the progress so far.

Bits chosen by Alice	$A_i = 0$				$A_i = 1$			
States sent by Alice	$\|0\rangle$				$\|+\rangle$			
Bits chosen by Bob	$B_i = 0$		$B_i = 1$		$B_i = 0$		$B_i = 1$	
Basis chosen by Bob	$\oplus$		$\otimes$		$\oplus$		$\otimes$	
Results of the measures of Bob	$\|0\rangle$	$\|1\rangle$	$\|+\rangle$	$\|-\rangle$	$\|0\rangle$	$\|1\rangle$	$\|+\rangle$	$\|-\rangle$
Probability to measure the state	1	0	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	1	0
The value of the test	**0**	-	**0**	**1**	**0**	**1**	**0**	-

Figure 1(a):BB84 (left) and Figure 1(b): B92 (right) – some popular protocols in QKD

Table 1: Survey of applications of QC in Cloud Security

	Paper	Description
DIRECT	[14]	Integration of Quantum Key Distribution (QKD) with PPP i.e. at the data link layer rather than network layer because it would make the encryption transparent to the whole network and would not require much change in equipment and infrastructure. Their protocol Q3P (a modification of PPP) was implemented over the SECOQC network.
	[21]	Securing WLAN using QKD by integrating it with 802.11i [RFC 4018], using quantum handshake.
	[12]	QKD for key distribution in IPSec, by integrating it with standard IKE.
	[24]	Proposed IKE like new protocol based on the ISAKMP mechanism i.e., SeQKEIP.
	[10]	Quantum handshake for TLS/SSL
	[18] [19]	Authentication scheme with unconditional security of QKD and flexibility of PKI for grid architecture with the communities connected via a quantum network like SECOQC
	[17]	Tight Finite Key in addition to MQKD i.e., multi QKD for distributing same secret key within a group in order to make multi-party authentication possible in cloud.
INDIRECT	[23]	Suggested Measurement Based Blind Quantum Computing(BQC). BQC is the quantum analog of homomorphic encrytion.
	[8]	Improved upon BQC protocol suggested by Raussendorf and Briegel.
	[4]	Demonstrated measurement based BQC
	[3][26].	Ancilla-Driven BQC, i.e., based on quantum circuits rather than measurement.

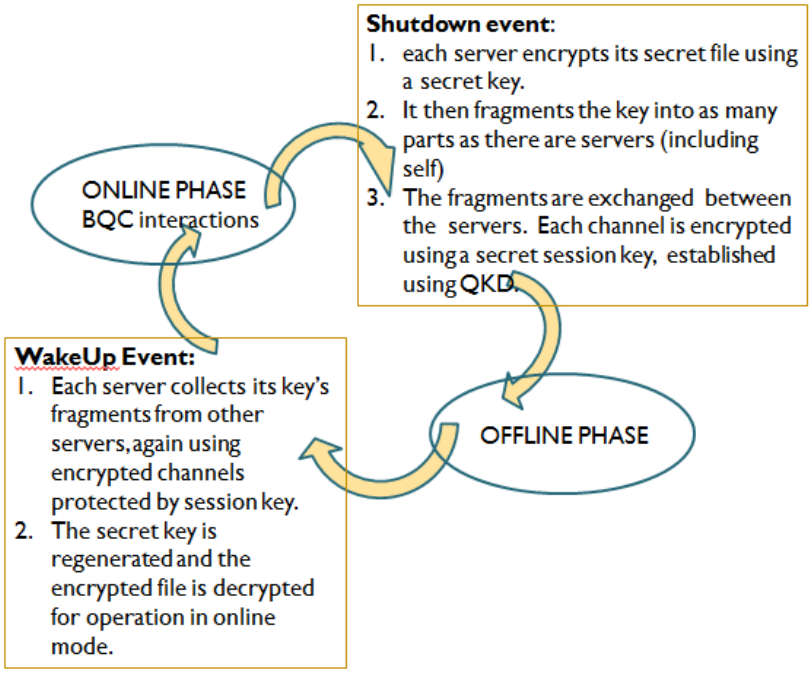

Figure 2: Using QC in cloud - A model

In Table 1, Some protocols [14][21][12][24][10] are modifications of existing ones so as to make them compatible with quantum networks. Some protocols [18][19][17] have been designed to offer authentication services. And the rest [23][8][4][3][26] seek to achieve blind computation i.e. computation without divulging the inputs.

4.2 Issues and Proposed Work

The issues with applying QC in Cloud Security in particular and Security in general, ultimately boil down to implementation. On Paper, Quantum Cryptographic protocols for key exchange offer unconditional security. But current implementations are susceptible various attacks like Siphoning attack etc. With time, the technology will become more sophisticated and hopefully offer the unconditional security that it promises. Besides this, protocols that have been modified to include QKD, need to be checked for composibility. And finally, it would be more fruitful to come up with Quantum Cryptographic protocols for the server side in particular e.g. the Blind Quantum Computation.

One possible application may be using QC for Key Exchange between servers where they are involved in Multi Party Computation (MPC). MPC is a secure way of computation, wherein the parties compute a function of the inputs without actually knowing the inputs. Such a protocol finds use in many applications like e-bidding etc. MPC involves use of secret keys. Storage of such keys becomes an issue, especially when the servers have the ability to switch modes, from online to offline and vice versa. Damgard et al.[9] suggested a protocol for securing the keys when the servers are in offline mode. The servers are autonomous or semi-autonomous i.e., switch from online to offline mode with no or little intervention from outside. Further, this work can be extended for providing secure key distribution mechanism between cloud servers by using QC.

Suppose there are n servers that want to compute a function of their "inputs", without revealing them, a scenario typical of MPC (For example, in awarding e-tenders the secret input would be the bid while the output will be finding the minimum bid). The input file is thus the server's "secret file". This paper proposes a model in Figure 2 for maintaining privacy in a situation where the servers are "QC-capable". (QC capability means compatiblity with existing Quantum cryptographic techniques).

In the model, it is assumed that the servers are not engaged in continuous computation, thus going into "offline" mode. Moreover, the switch from "online" state to "offline" state is either autonomous or semi-autonomous, i.e., requiring no or little intervention from outside to effect such change of state. The secret file needs to be secured in both the online as well as the offline state.

5. CONCLUSION AND FUTURE WORK

Cloud computing is a fast paced technology and tagging quantum techniques with it may serve two purposes. One, when we finally have quantum computers (which is not too far), cloud computing will be ready to be integrated with them. Also if the existing protocols are proved to be unconditionally secure i.e., even against a quantum adversary, it would mean that the cloud is prepared to handle attacks by such an adversary. If not, then it would fuel research along these lines. Either ways, we would have to combine the two fields. Secondly, tagging quantum research with cloud computing may spell revolution for the former. Thus, one will reinforce the other.

There is a lot of scope as far as the future work is concerned. One research direction may be modification of the quantum counterpart of MPC, to make it more efficient. Yet another possibility is to prove the security of classical MPC in a quantum setting and so on.

6. REFERENCES

[1] R. Alleaume, N. Lutkenhaus, R. Renner, P. Grangier, T. Debuisschert, G. Ribordy, P. Painchault, T. Pornin, L. Salvail, M. Riguidel, a Shields, M. Peev, a Leverrier, a

Poppe, J. Bouda, C. Branciard, M. Godfrey, J. Rarity, a Zeilinger, and C. Monyk, “Using Quantum key distribution for cryptographic purposes : a survey,” Security, vol. 560, pp. 62–81, 2009.

[2] R. Alleaume, J. Bouda, C. Branciard, T. Debuisschert, M. Dianati, N. Gisin, M. Godfrey, P. Grangier, T. Langer, A. Leverrier, N. Lutkenhaus, P. Painchault, M. Peev, A. Poppe, T. Pornin, J. Rarity, R. Renner, G. Ribordy, M. Riguidel, L. Salvail, A. Shields, H. Weinfurter, and A. Zeilinger, “SECOQC White Paper on Quantum Key Distribution and Cryptography,” p. 28, 2007.

[3] J. Anders, D.K. Oi, E. Kashefi, D.E. Browne & E. Andersson “Ancilla-driven universal quantum computation,” Physical Review A, vol 82, no.2, 020301,2010

[4] S. Barz, E. Kashefi, a. Broadbent, J. F. Fitzsimons, a. Zeilinger, and P. Walther, “Demonstration of Blind Quantum Computing,” Science (80-.)., vol. 335, pp. 303–308, 2012.

[5] C.H. Bennett, “QC using any two nonorthogonal states,” Physical Review Letters, 68(21), 3121,1992.

[6] C. H. Bennett, G. Brassard, A. K. Ekert, R. C. Merkle, and S. Uni, “QC,” pp. 57–61, 1992

[7] G. Brassard, N. Lutkenhaus, T. M. T. Mor, and B. C. Sanders, “Security aspects of practical Quantum Cryptography,” Conf. Dig. 2000 Int. Quantum Electron. Conf. (Cat. No.00TH8504), 2000.

[8] A. Broadbent, J. Fitzsimons, and E. Kashefi, “Measurement-based and universal blind quantum computation,” Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 6154 LNCS, pp. 43–86, 2010.

[9]] I. Damgård, T. P. Jakobsen, J. B. Nielsen, and J. I. Pagter, “Secure key management in the cloud,” Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 8308 LNCS, pp. 270–289, 2013.

[10] M. Elboukhari and A. Azizi, “Implementation of Secure Key Distribution Based On QC,” 2009 Int. Conf. Multimed. Comput. Syst. (Icmcs 2009), pp. 361–365, 2009.

[11] M. Elboukhari, M. Azizi, and A. Azizi, “Quantum Key Distribution Protocols : A,”Intl.Journal of Universal Computer Science vol. 1, pp. 59–67, 2010.

[12] C. Elliott “ Building the quantum network,” New Journal of Physics, vol 4, 46.1-46.12, 2002

[13] A.K. Ekert, “Quantum Cryptography based on Bell’s theorem,” Physical review letters, 67(6), 661,1991.

[14] S. Ghernaouti-H´elie & M.A.Sfaxi “Upgrading PPP security by quantum key distribution,” In Proc NetCon 2005 conference, 2005

[15] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, “QC,” arXiv Prepr. quant-ph/0101098, vol. 74, pp. 145–195, 2001.

[16] J. Gruska and C. Republik, “Quantum computing,” 2004.

[17] R. Khalid and Z. Zulkarnain, “Enhanced Tight Finite Key Scheme for Quantum Key Distribution (QKD) Protocol to Authenticate Multi-Party System in Cloud Infrastructure,” Appl. Mech. Mater., no. November, pp. 25–26, 2014.

[18] M. Khan and J. Xu, “Enhancing Grid Security using Quantum Key Distribution,” Sersc.Org, vol. 6, no. 4, pp. 67–76, 2012.

[19] M. M. Khan and J. Xu, “Applications of QKD Network for High Performance Distributed Computing,” pp. 2–4.

[20] H. K. Lo. & H.F. Chau “Is quantum bit commitment really possible?,”.Physical Review Letters, 78(17), 3410, 1997.

[21] T. Mai, T. Nguyen, M. A. Sfaxi, and S. Ghernaouti-hélie, “802 . 11i Encryption Key Distribution Using QC,” 1st Int. Conf. Availability, Reliab. Secur., vol. 1, no. 5, pp. 116–123, 2006.

[22] D. Mayers, “Unconditional security in Quantum Cryptography,” vol. 48, no. 3, p. 18, 1998.

[23] R. Raussendorf & H.J. Briegel “ A one-way quantum computer,” Physical Review Letters, vol 86, no.22, 5188, 2001.

[24] M. A. Sfaxi, S. Ghernaouti-Hélie, G. Ribordy, and O. Gay, “Using Quantum Key Distribution within IPSEC to secure MAN communications,” IFIP Open Conf. Metrop. Area Networks Archit. Protoc. Control. Manag. MAN, 2005.

[25] P.W. Shor “Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer,” SIAM journal on computing, vol 26, no.5, pp.1484-1509, 1997.

[26] T. Sueki, T. Koshiba & T. Morimae,: Ancilla-driven universal blind quantum computation, Physical Review A, 2013, vol 87, no.6, 060301, 2013.

[27] A. Verma and S. Kaushal, “Cloud computing security issues and challenges: a survey,” Adv. Comput. Commun., vol. 193, pp. 445–454, 2011.

[28] W.K. Wooters & W.K. Zurek, “Quantum no-cloning theorem,” Nature, 299, 802, 1982.