QUANTUM CRYPTOGRAPHY AND CLOUD COMPUTING SECURITY WITH RE-ENCRYPTION SCHEME

A. ARSHAD AAQIB **S. CHANDRA MOHAN**
Bannari Amman Institute of Technology

ABSTRACT

The question, "How to build a securesystem?"baffled everyone who are currently enjoying the services provided by recent trends and technological developments achieved in the field of computers, especially the "Internet".No doubt, gaining access to Internet and its services is quite simple, by just using gateways, dial-up connections,and ISP. But beneath this, the problems of security come as the information may be lost, stolen or corrupted. So, if the question"Why should one hack my PC?" is always backing at your mind, then there is a definite scope to challenge the "Bad guys" who want to break down the layers of security defenses. But there is no single foolproof solution for building such a secured system. Our security has to be a layered structure and that should start all the way from the selection of the Operating System even.

In this paper we mainly concentrated on Cryptography Science. We briefly discussed various Cryptographic Systems i.e., Symmetric and Asymmetric key Cryptography and their limitations. Owing to the drawbacks of basic Cryptographic Systems, our focus turned towards Quantum Cryptography whose strength, secrecy and privacy lies in the Laws of Physics than current state of unproven mathematical assumptions in Classical Cryptography. The core of the paper contains the detailed description of the fundamentals of Quantum Cryptography and how this concept overcomes the loopholes in Conventional Cryptographic System, especially "The KeyDistribution Problem". Finally we moved over to Commercial Implementations of Quantum Cryptography paving the path to Research Scope in this arena. Also this paper contains the technique of keeping information in secured way in cloud storage system with secured Data Forwarding using Re-encryption Scheme using server key and cipher key

KEYWORD: Quantum Cryptography, Key Distribution Problem, Data Forwarding, cloud storage, Re-encryption

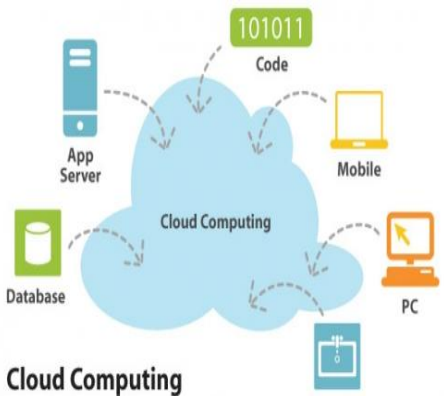
INTRODUCTION

In the early years of development of Internet protocols, stress was given more towardsubiquitous connectivity and guaranteed delivery of data. Once the Internet usage started increasing, the focus turned towards adding quality of service. People started participating in interactive environment, irrespective of geographical boundaries, within no time. As the Internet usage exploded,it became a medium even for financial transactions such as online banking. No doubt, the conveniences and the services provided by Internet are awesome but the inconveniences are ominous, really threatening. This is better understood by the practical example which happened earlier this year, "Slammer" infected the first few PCs, 8.5 sec after it was discovered; in 11 min it had corrupted 75,000 systems worldwide. Thus the worldstarted feeling the heat of exploitation of security holes in the Internet. Even as late as earlynineties, Internet security was not of concern but soon it became an issue of paramountimportance. If Internet has to survive and grow, Internet security is a must.

Cloud computing is basically an Internet-based network made up of large numbers of servers - mostly based on open standards, modular and inexpensive. Clouds contain vast amounts of information and provide a variety of services to large numbers of people. The benefits of cloud computing are Reduced Data Leakage, Decrease evidence acquisition time, they eliminate or reduce service downtime, they Forensic readiness, they Decrease evidence transfer time. The main factor to be discussed is security of cloud computing, which is a risk factor involved in major computing fields.

Cloud computing also describes applications that are extended to be accessible through the Internet.

These cloud applications use large data centers and powerful servers that host Web applications and Web services. Anyone with a suitableInternet connection and a standard browser can access a cloud application.



User of the cloud only care about the service or information they are accessing - be it from their PCs, mobile devices, or anything else connected to the Internet - not about the underlying details of how the cloud works."

SEVEN TECHNICAL SECURITY BENEFITS OF THE CLOUD

- **CENTRALIZED DATA**
- **PASSWORD ASSURANCE TESTING**
- **LOGGING**
- **INCIDENT RESPONSE FORENSICS**
- **IMPROVE THE STATE OF SECURITY SOFTWARE**
- **SECURE BUILDS**
- **SECURITY TESTING**

SECURITY METHODS:

Types of Cryptographic Algorithms

The two types of cryptographic algorithms that will be briefly discussed in this sectionare: symmetric key encryption and asymmetric key encryption. Both schemesutilize trapdoor one-way functions to encipher and decipher messages.One-way functions are mathematical functions that are easy to compute in onedirection but are (believed) to be very difficult to inverse. Here, the inverse of afunction is considered difficult (easy) to calculate if the time it takes to accomplish this task grows exponentially (polynomially) with the size (often expressed as the number of bits) of the input.

In symmetric and asymmetric key encryption the concept of trapdoor one-wayfunctions is applied as follows:

A key and a cleartext message are used as theinput to a trapdoor one-way function to generate ciphertext. A key (not necessarilythe same key as before) and the ciphertext are then used as input to the inverse ofthe trapdoor one-way function to recover the cleartext message.

The major difference between symmetric and asymmetric key encryption lies in theway the necessary keys are generated and distributed.

Symmetric Key Encryption:

Symmetric key encryption uses the same cryptographic algorithm and the samekey to encipher and decipher messages. The key is chosen pseudo-randomlyfrom a subset of all possible key values.As opposed to the one-time pad, symmetric key encryption uses the same keyrepeatedly to encipher and decipher messages. This makes it inherently lesssecure than the one-time pad since in its most straightforward implementation thesame plaintext will result in the same ciphertext. Special care has to be taken to circumvent this problem. Other problems with symmetric key encryption include the secure generationof keys and, since the same key is used to encipher and decipher messages, thesecure distribution of keys to both Alice and Bob.

Examples of commonly used symmetric key encryption algorithms are DataEncryption Standard (DES), 3DES, RivestCipher (RC-4), and International DataEncryption Algorithm (IDEA).

Asymmetric Key Encryption:

Asymmetric key encryption is also known as public key encryption. As the nameimplies, it requires two different but mathematically related keys, one to encipher amessage and the other corresponding key to decipher the message. Since one of the keys is known publicly, it is called the public key. The other key has to be keptprivate with one or the other party to the secure communication. It is therefore referred to as the private key.This system works analogous to a drop mailbox with two locks. The owner of the mailbox provides everybody

with a key for dropping mail into his box, but only he has the key to open it and read the messages inside.

A very popular asymmetric key encryption algorithm is RSA. A most basic secure exchange of messages between Alice and Bob usingasymmetric key encryption will proceed as follows:

1) Alice and Bob agree on a particular asymmetric key encryption method.
2) Both Alice and Bob generate their own, separate public/private key pairs.
3) Alice and Bob exchange their public keys.
4) Alice uses Bob's public key to encipher a message and sends it to Bob.
5) Bob uses his private key to decipher the message.
6) Bob enciphers a reply using Alice's public key.
7) Alice deciphers the reply using her private key.

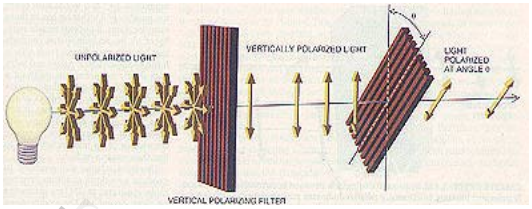
The advantage of asymmetric key encryption is that it solves the key distribution problem that plagues symmetric key algorithms. No secret keys are everexchanged - only public keys. However, the private keys are still vulnerable to compromise. Also asymmetric key encryption is too slow for many high bandwidthcommunications.

The most popular public key cryptosystem, RSA (Rivest-Shamin-Adleman), gets its security from the difficulty of factoring large numbers.This means that if ever mathematicians or computer scientists come up with fast and clever procedures for factoring large numbers, then the whole privacy and discretion of widespread cryptosystems could vanish overnight. Indeed, recent work in quantum computation suggests that in principle *quantum computers* might factorize huge integers in practical times, which could jeopardize the secrecy of many modern cryptography techniques.

QUANTUMCRYPTOGRAPHY

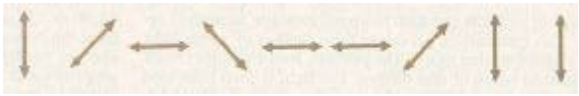
Fundamentals:

The foundation of quantum cryptography lies in the Heisenberg uncertainty principle, which states that certain pairs of physical properties are related in such a way that measuring one property prevents the observer from simultaneously knowing the value of the other. In particular, when measuring the polarization of a photon, the choice of what direction to measure affects all subsequent measurements. For instance, if one measures the polarization of a photon by noting that it passes through a vertically oriented filter, the photon emerges as vertically polarized regardless of its initial direction of polarization. If one places a second filter oriented at some angle q to the vertical, there is a certain probability that the photon will pass through the second filter as well, and this probability depends on the angle q. As q increases, the probability of the photon passing through the second filter decreases until it reaches 0 at q = 90 deg (i.e., the second filter is horizontal). When q = 45 deg, the chance of the photon passing through the second filter is precisely 1/2. This is the same result as a stream of randomly polarized photons impinging on the second filter, so the first filter is said to randomize the measurements of the second.



Polarization by a filter:

Un-polarized light enters a vertically aligned filter, which absorbs some of the light and polarizes the remainder in the vertical direction. A second filter tilted at some angle q absorbs some of the polarized light and transmits the rest, giving it a new polarization. A pair of orthogonal (perpendicular) polarization states used to describe the polarization of photons, such as horizontal/vertical, is referred to as a basis. A pair of bases are said to be conjugate bases if the measurement of the polarization in the first basis completely randomizes the measurement in the second basis, as in the above example with q = 45 deg. It is a fundamental consequence of the Heisenberg uncertainty principle that such conjugate pairs of states must exist for a quantum system.



If a sender, typically designated Alice in the literature, uses a filter in the 0-deg/90-deg basis to give the photon an initial polarization (either horizontal or vertical, but she doesn't reveal which), a receiver Bob can determine this by using a filter aligned to the same basis. However

if Bob uses a filter in the 45-deg/135-deg basis to measure the photon, he cannot determine any information about the initial polarization of the photon.

These characteristics provide the principles behind quantum cryptography. If an eavesdropper Eve uses a filter aligned with Alice's filter, she can recover the original polarization of the photon. But if she uses a misaligned filter she will not only receive no information, but will have influenced the original photon so that she will be unable to reliably retransmit one with the original polarization. Bob will either receive no message or a garbled one, and in either case will be able to deduce Eve's presence.

The BB84 Quantum Key Distribution Protocol

In this section we will use the following notation:

"|" denotes a photon in a vertically polarized state.

"." denotes a photon in a horizontally polarized state.

"/" denotes a photon in a 45 degree polarized state.

"\" denotes a photon in a 135 degree polarized state.

"+" denotes the pair of states {|,.}, also called the +-basis.

"X" denotes the pair of states {\, /}, also called the x-basis.

Let us further assume that Alice and Bob have agreed to associate the binary digit1 with the states | and \, respectively, and the binary digit 0 with the states • and /,respectively.

Here quantum key distribution protocol requires twocommunication channels: a quantum communication channel which transmits thephotons, such as a standard fiber-optic cable, and a classical communicationchannel, such as a phone line, e-mail, etc. Here, the classical communicationchannel is used to ascertain whether confidentiality on the quantum channel hasbeen breached and to facilitate error correction and privacyamplification It is assumed that Eve has unlimited computing power and complete access to both communication links, except that she cannot impersonate either Alice or Bob on the classical communication channel .

With this setup , the BB84 quantum key distribution protocol proceedsthrough the following steps:

1) Alice sends a stream of individual photons in one of the four polarizationstates |, •, /, or \ to Bob. Alice picks each photon's polarization staterandomly and independently.

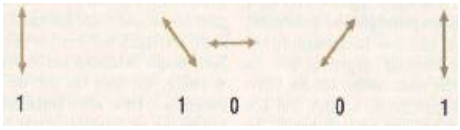
2) For each photon, Bob randomly chooses either the +-basis or the x-basisand measures the polarization of the photon in that basis.

3) For each photon, Bob records the basis he used and the result of thepolarization measurement.

4) Through the classical communication channel, Bob communicates to Alicefor each photon his choice of basis, but not the result of his polarizationmeasurement.

5) Still through the classical communication channel, Alice tells Bob whichphoton was measured in the correct basis.

6) Both, Alice and Bob, discard the polarization data that correspond to thosephotons that were not measured in the correct basis.



Since Bob's chance of picking the correct basis is about 50%, the length ofthe sifted key is about ½ of the total number of photons that Alice sent to Bob.

Limitations of Quantum Cryptography

A number of technical challenges still remain in quantum cryptography.

1) Single Photon generating systems

2) Deterministic Random number generation by computers

3) Quantum repeaters to strengthen the photons

4) Low transmission rate

Commercial Implementations of QuantumCryptography

During the past year two commercial products implementing the BB84 quantumkey distribution protocol have been launched.

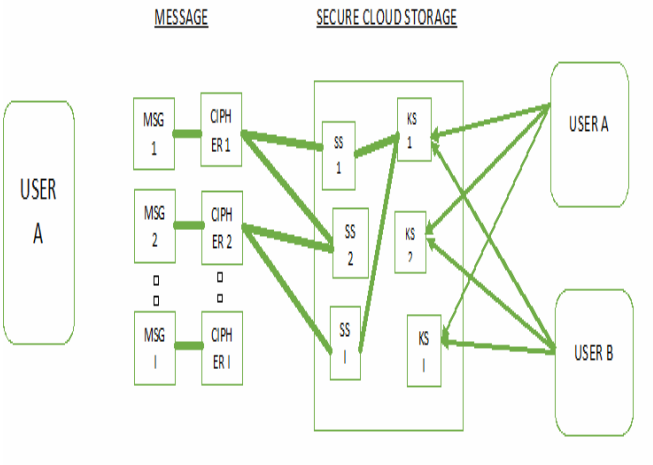
One of the products is providing a VPN gateway claiming a 70mile transmissiondistance through standard fiber-optic cable with a key refresh rate of up to 100 new keys per second.

The other product is providing a point-to-point quantum key distribution hardwaresystem. It claims a 40mile key distribution distance over standard optical fiber witha key distribution rate of up to 1Mbit/s. However, the key distributionperformance degrades over long distances, being only 100bits/s for distances of50km. This device also offers a random number generator that is based on arandom physical process.

PROPOSED SYSTEM ON CLOUD COMPUTING FOR SECURITY

In the proxy Re-Encryption key, the messages are encrypted by the owner and stored in the storage server. When a user wants to share his messages, he sends a re-encryption key to the storage server. The Storage sever re-encrypts the encrypted messages for the authorized user. Thus their system has data confidentiality and supports the data forwarding function. An encryption scheme is multiplicative homographic if it supports a group on encrypted plain texts without decryption. The multiplicative homographic encryption scheme supports the encoding operation over encrypted messages. We convert into proxy re-encryption scheme with multiplicative homographic property into threshold version. A secret key is shared to key servers with threshold value. To decrypt the messages, the key can be taken from the storage server system. Here a message is forwarded to different storage servers SS1, SS2,….SSi where i=∞. The data is forwarded and re-encrypted using the private key and the cipher key so as to maintain security and the other user can receive the information by decrypting from different storage servers. The encryption scheme supports encoding operations over encrypted messages and forwarding operations over encrypted and encoded messages.

Fig. General system model of our work



ADVANTAGES OF PROPOSED SYSTEM

- Tight integration of encoding, encryption and forwarding makes storage system efficiently meet the requirements of data robustness, data confidentiality and data forwarding
- The Storage serves independently perform coding and re-encryption process and the key servers independently perform partial decryption process
- More flexible adjustment between the number of storage servers and robustness.

CONCLUSION

Even though Quantum cryptography promises to revolutionize secure communication by providing security based on the fundamental laws of physics, instead of the current state of mathematical algorithms or computing technology. There is no doubt that there are still quite difficult technical problems to overcome, such as its limited range and low transmission rate, before it will findwidespread use in today's network infrastructure.The devices for implementing such methods exist and the performance of demonstration systems is being continuously improved. Within the next few years, if not months, such systems could start encrypting some of the most valuable secrets of government and industry in cloud.

As a final word, we know that future is going to be networked everywhere .Hence "Network Security" and "Cloud Computing" is gaining importance globally. So with everyone's operation and with consistent

practices, will it be achievable. No doubt, Science and Technology develops day by day. We need to utilize the advancements in emerging fields of Science and Technology to come up with highly secured and consistent practices so that we can challenges at the Bad guys, who want to break down our layers of security defense in cloud storage system.

REFERENCES

- "Quantum Cryptography" –by Charles H. Bennett, Gilles Brassard, and Artur K. Ekert.
- "Securing any time any where information"-- by Gaurav Vaidya
- " Network security white papers" --by interhack /pubs
- "Quantum cryptography: public key distribution and coin tossing"-- by Bennett, C. H. and G. Brassard.
- "Quantum Cryptography and Privacy Amplification"-- by Goldwater, S.
- "Hackers beware: quantum encryption is coming"-- by Johnson, R. Colin.
- "Quantum Is Key to New Security Alliance"-- Johnson, R. Colin.
- "Code based erasure using re-encryption in Cloud Storage system"- G.ChimaPullaiah