Quantum Cryptography For Cloud Computing

Shekhar S. Kausalye[1], Miss. Rina S. Patil[2], Miss. Pranoti V. Hadke[3]
[1, 2] Dept of Information Technology
[3]Dept of Science
[1] Sanjivani College of Engineering
[2]Sanjivani K.B.P. Polytechnic , [3]Sanjivani Academy

Abstract- *Quantum mechanics is the study of the small particles that make up the universe for instance, atoms. At such a microscopic level, the laws of classical mechanics fail to explain most of the observed phenomenon. At such a state quantum properties exhibited by particles is noticeable. Confidentiality, Integrity, and Availability are basic goals of security architecture. Currently deployment of Public Key Infrastructure (PKI) is a most significant solution of this security architecture. But there are certain issues of PKI authentication where the public key cryptography only provide computational security because PKI is based on Asymmetric Key Cryptography & hence it is exposed to widespread security threats such as eavesdropping, man in the middle attack, masquerade, etc. This paper aims to look into basic security architecture in place currently and further it tries to introduce a new proposed security architecture, which makes use of the knowledge of Quantum Mechanics and current advances in research in Quantum Computing, to provide a more secure architecture.*

Keywords- Cloud Computing Security, PKI, Asymmetric Key Cryptography, Threats, Quantum Mechanics, Quantum Computing.

I. INTRODUCTION

Quantum mechanics is the study of the small particles thatmake up the universe – for instance, atoms et al. At such a microscopic level, the laws of classical mechanics fail to explain most of the observed phenomenon. At such a state quantum properties exhibited by particles is quite noticeable rom beginning of computer history various techniques like time sharing, network computing, and grid computing, virtual.

If we look at the basis of quantum mechanics – The Heisenberg's Uncertainty Principle [01] which states that “the more precisely the position is determined, the less precisely the momentum is known in this instant, and vice versa.” For instance, if you measure the position of an electron revolving around the nucleus an atom, you cannot accurately measure its velocity. If you measure the electron's velocity, you cannot accurately determine its position. In a practical scenario, this principle is applied to photons the smallest measure of light. Photons can exist in all of their possible states at once and also they don’t have any mass. For example if you constantly moved east, west, north, south, and up-and-down at the same time.

II. QUANTUM CRYPTOGRAPHY

Confidentiality, Integrity, and Availability are basic goals of security architecture. Many authentication scheme has been introduced in several years. Public Key Infrastructure (PKI) is a most significant solution now a days. It involves exchanging a key using certificates via a public channel to a authenticate users in the cloud infrastructure. However, there is a certain issue relating to the PKI authentication where the public key cryptography only provide computational security because PKI is based on Asymmetric Key Cryptography. It is exposed to widespread security threats such as eavesdropping, man in the middle attack, masquerade [02]. This paper aims to look into basic security architecture in place currently and further it tries to introduce a new proposed security architecture, which makes use of the knowledge of Quantum Mechanics and current advances in research in Quantum Computing, to provide a more secure architecture.

A. Qbits

In a computing system, a bit would have to be in one state or the other. However in a quantum computing system, quantum mechanics allows the qubit to be in a superposition of both states at the same time. In quantum computing, a qubit or quantum bit or qbit is a unit of quantum information the quantum analogue of the classical bit. A qubit is a two-state quantum-mechanical system, such as the polarization of a single photon: here the two states are vertical polarization and horizontal polarization.

Table 1. Example of Physical Qbit

System	Qubit State
Electron	Spin
Photon	Polarization

A qubit has a few similarities to a classical bit but is overall very different. There are two possible outcomes for the measurement of a qubit usually 0 and 1, like a bit. The difference is that whereas the state of a bit is either 0 or 1, the state of a qubit can also be a superposition of both.[03] It is possible to fully encode one bit in one qubit. Hence, a qubit can hold even more information, e.g. up to two bits using super dense coding.

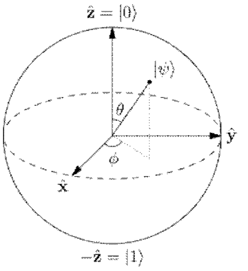

Fig. 1. Bloch sphere representation of a qubit.

The possible states for a single qubit can be visualized using a Bloch sphere (see diagram). Represented on such a sphere, a classical bit could only be at the "North Pole" or the "South Pole", in the locations where |0> and |1> are respectively. The rest of the surface of the sphere is inaccessible to a classical bit, but a pure qubit state can be represented by any point on the surface.

The surface of the sphere is a two-dimensional space, which represents the state space of the pure qubit states. This state space has two local degrees of freedom.

It is possible to put the qubit in a mixed state, a statistical combination of different pure states. Mixed states can be represented by points inside the Bloch sphere. A mixed qubit state has three degrees of freedom: the angles $\emptyset$ *and* θ as well as the length *r* of the vector that represents the mixed state

B. Shor's Algorithm

In 1994, Shor proposed an algorithm for period finding and then subsequently integer factorization problem. Later, Shor also proposed an efficient quantum algorithm for the discrete logarithm problem. Shor's algorithm consists of Classical Part and Quantum Part. Quantum part of the algorithm, uses quantum Fourier transform to find the period of a certain function, which is infeasible with classical computers, but in 2001 a group at IBM, who factored 15 into 3 × 5, using an NMR implementation of a quantum computer with 7 qbits.

Shor mathematically showed that the quantum part runs in time O ((log n)^2 (log log n)(log log log n)) on a quantum computer. Next, it must perform O (log n) steps of post processing on a classical computer to execute the continued fraction algorithm.

Factorizations and discrete logarithm problem are two of the most difficult problems arising in the breaking of current cryptographic algorithms. If the Shor's algorithm is implemented on Quantum Computers, no application using this algorithm will be able to withstand the attackers.

C. Quantum Cryptography

The uncertainty principle, possible of indivisible quanta and the quantum entanglement forms the basis of the quantum cryptography. The no-cloning theorem, presented by Wootters and Zurek in 1982, forms another basis of Quantum Cryptography. As a direct application of no cloning theorem Eavesdropper cannot interpret the unknown qubits i.e. the unknown quantum states, which makes the use of qubits in key transmission for asymmetric cryptography resistant to man in the middle attack. Hence, it is attracting considerable attention as a replacement for other contemporary cryptographic methods, which are based on computational security.

Quantum Cryptography works just like a traditional asymmetric cryptographic system. But like RSA, which use computational difficulty in breaking the key, Quantum Cryptographic system uses quantum physics for key transmission. Quantum cryptographic transmission encrypts the 0s and 1s of a digital signal on individual particles of light i.e. photons. Each type of a photon's spin represents one piece of information - usually a 1 or a 0, for binary code. This code uses strings of 1s and 0s to create a coherent message. For example, 01101000 01101001 could correspond with "hi".

Now, a binary code can be assigned to each photon - for example, a photon that has a vertical spin (|) can be assigned a 1 and a photon with a horizontal spin, can be assigned 0. Alice can send her photons through randomly chosen filters and record the polarization of each photon. She will then know what photon polarizations Bob should receive. Now, even if eve detects (eavesdrops on) the signal, the information on the photons is suddenly transformed, meaning both that it is immediately noticeable that eavesdropping has appeared and that the third party is not able to decrypt the information.

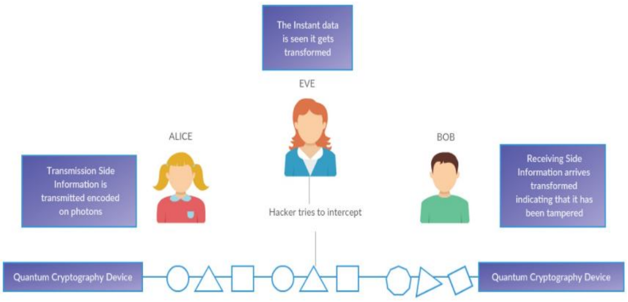
The Instant data is seen it gets transformed
EVE
ALICE
BOB
Transmission Side Information is transmitted encoded on photons
Hacker tries to intercept
Receiving Side Information arrives transformed indicating that it has been tampered
Quantum Cryptography Device
Quantum Cryptography Device

Fig. 2. Working of Quantum Cryptography

D. Quantum Key Distribution

In public key cryptography, before transferring data, both Alice and Bob agrees upon a shared secret key. Alice uses the public key of Bob to transfer the shared secret key to Bob and that encrypted key can be decrypted only by Bob's private key. Now, Bob uses his private key to decrypt the shared key and then using that shared secret key, Bob can decrypt all the encrypted messages that Alice sends.[04] This type of system is susceptible to Man in the Middle attack since the assumption used for transmission of shared key is that decrypting it without the key is, computationally infeasible. But with Shor's algorithm, even this isn't computationally infeasible anymore.

Here concept of QKD comes. It is a method used in quantum cryptography to produce a perfectly random key which is shared by a sender and a receiver while making sure that nobody else has a chance to learn about the key, e.g. by capturing the communication channel used during the process. The best known and popular scheme of quantum key distribution is based on the Bennet Brassard protocol (i.e. BB84). It depends on the no-cloning theorem for non-orthogonal quantum states. [05]

The basic principle of the Quantum Key Distribution (QKD) using the BB84 protocol, involves sending decryption keys as quantum particles. To detect the intruders, the photons can be randomly sampled for different properties. Now, since the measurement in one property results in uncertainty in the measurement of other property, Alice and Bob independently chooses to measure each proton for different properties, say polarization or spin. They then exchange which property they measured on each photon, and examine whether the values are the same on photons that they measured are same or not. If there is a large difference, it is likely the signal was intercepted, and the communication should be dropped. If results are similar, then the values can be stored as binary data; for instance, left spin = 0, right spin = 1. This is the shared key. Once both Alice and Bob have agreed upon the shared secret key, they use the normal channel to transfer the data encrypted with the shared key.

III. QKD USING RSA ALGORITHM

Factoring is widely believed to be a hard problem and the best algorithm for solving with a sub-exponential running time. The principal threat comes from a quantum computer on which factoring can be solved efficiently using Shor's algorithm. The most popular cryptosystem based on factorization is RSA. RSA was invented by Rivest, Shamir and Adelman in 1978. RSA algorithm is as follows:

1. Key generation:

- Choose two large primes p and q & compute $N = pq$.
- Choose an integer e that is co-prime to $(p − 1) (q − 1)$.
- Compute d using $ed \equiv 1 \pmod{(p − 1) (q − 1)}$.
- Publish the public key (N, e) & keep the private key (N, d).

2. Encryption:

- Represent msg to be transmitted as positive integer $m < N$.
- Encrypt m with public key (N, e) using $c \equiv me \pmod{N}$.

3. Decryption:

- The receiver decrypts the message using $m \equiv c\ d \pmod{N}$.
- Transform the positive integer m into the original message.

A. Implementing RSA Algorithm With QKD

Factorization is the underlying hard part in RSA algorithm. Using the Shor's algorithm, it is easy to break the message that has been encrypted using RSA. So, here QKD can be introduced for key generation and distribution and use underlying principles of RSA to transmit the message. [06]
So improved RSA with QKD is:

1. Alice sends a request to QKD to initiate a conversation with Bob.
Alice → QKD: $E_{PR\text{-}ALICE}$ (ID_{ALICE} || ID_{BOB}).
2. QKD logs the Alice's Request and notifies Bob about the possible connection
QKD → BOB: $E_{PU\text{-}BOB}$ (ID_{ALICE} || ID_{BOB})
3. Bob replies by accepting the connection.
Bob → QKD: $E_{PR\text{-}BOB}$ (ID_{ALICE} || ID_{BOB})
4. QKD creates a session key using quantum bases (+, X) in some order and starts distributing those to Alice and Bob, Alice and Bob will use those bases to communicate.

QKD → Alice: $E_{PU\text{-}ALICE}$ (ID_{ALICE} || ID_{BOB} || SK)

QKD → Alice: $E_{PU\text{-}BOB}$ (ID_{ALICE} || ID_{BOB} || SK)
5. Alice encrypts the message using the session key and sends it to Bob over a Quantum Channel. Next, Alice also sends random bits to QKD.
Alice → BOB: $E_{PR\text{-}ALICE}$ (E_{SK} (Message) || ID_{BOB})
6. Bob decrypts the message using the Session Key and sends the random bits to QKD.
7. QKD checks the random bits to know if there’s any intruder. If there’s an intruder QKD notifies Alice and Bob and discards the Session Key to create a new Session Key.

IV. CURRENT WORK

Advancements in storage techniques alongside SaaS techniques have enabled a different computing model – Cloud Computing. Examples of such service providers include Google, Microsoft, Apple, Amazon any others. Since the data transfer for such an application occurs through the classical network, storage on the same server for many users. Here resource allocation and scheduling is provided by the cloud service provider and with the breakthrough in malicious programs, cloud security becomes an important issue.

Every day hackers are trying to hack into some cloud or the other and recently with the security of giants like Apple and Dropbox being compromised10 cloud security has become a hot topic. Here, I’m trying to propose a new hybrid security architecture for the cloud which uses benefits of current protocols like Kerberos and security benefits of Quantum Cryptography. [06].

Now a day’s deploying public key infrastructure (PKI) is one of the most elegant solutions for securing clouds. Another method for secure authentication on Cloud is using Kerberos. Many researchers have proposed a Kerberos-based model for secure data storage and secure authentication on the cloud. There are many benefits for using Kerberos in cloud computing, with the major one being the property of Kerberos that allows the nodes to connection points of the various cloud networks, and to communicate with each other. Apart from this compared to PKI, Kerberos is easy to deploy and it uses a session key which enables the possibility of Single Sign On.

Summary of Kerberos Message Exchange in Cloud Service: [07]

A. AS Exchange: to obtain TGT

1. AS_REQ – {cloud customer name, expiration time, ...}
2. AS_REP – {$S_{A,\ KDC}$, expiration time, tgs cloud service name …} . K_A + {$S_{A,\ KDC}$, expiration time, cloud customer name} . K_{KDC}

B. Ticket Granting Server Exchange: to obtain server granting tickets

3. TGS_REQ – {timestamp, checksum …}.$S_{A,KDC}$ + { SA, KDC, expiration time, cloud customer name…}.K_{KDC}. + cloud service name + expiration time
4. TGS_REP – {$S_{A.B}$, cloud service name, expiration time, …}.$S_{A,KDC}$ + { $S_{A.B}$, cloud customer name, expiration time, …}

C. Customer/Server Authentication Exchange: to obtain cloud service

5. CS_REQ – {timestamp, checksum …}.$S_{A,B}$ + {$S_{A,B}$, cloud customer name, expiration time, …}.K_B
6. CS_REP – {timestamp}.$S_{A,B}$

V. PROPOSED MODEL

As seen above, implementation of Kerberos model to cloud computing, is a very advantageous. But Kerberos also uses algorithms like DES and AES to generate the key. With the help of Groover’s Algorithm, searching an unsorted database with N entries in O(√N) time rather than the usual O(N) time. For AES-256, it currently takes an average of n/2 guesses to break, i.e. 2255. However with quantum computers this can be done in 2128 time, which is very much faster. Now that's only the brute force for AES-256, with the cleverer attacks like using rainbow tables, it can be broken even faster. Hence, for the Post Quantum world, using QKD for Key Generation and Key Distribution within KDC alongside classical Kerberos implementation, would result in better security. Also with the world moving towards the Internet of Things (IoT) Revolution, Single Sign On solution provided by the Kerberos Model could be the ideal security solution. Also, at the brink of this IoT revolution, security issues are of great concern and the possibility of Quantum Computers in near future would mean, when they arrive nothing will be secure. Hence, using QKD inside of the KDC could be the ideal solution. [01]

For the basic approach for cloud computing with Kerberos authentication, the given architecture is almost similar to the Architecture mentioned in the previous section. The only difference is that the Data Transmission between the Cloud and the Client happens through Quantum Channel and there is a QKD inside the KDC.

Now, to use the services of the cloud, a cloud customer should supply a ticket. A ticket for a cloud service is a series of bits with the attribute that it has been enciphered using the private key for that cloud service. That Session key is stored in the global database shared between the cloud service itself and the Kerberos.

Once a cloud customer gets a ticket and wants to use the cloud service, it generates a random quantum bases and sends it to a KDC along with the ticket. Now, anyone can intercept this message but it is of no use to them since they don't have the password to decrypt and even after the brute force attack, to generate the session key they require server's Quantum Bases. In return, KDC generates the Session key and stores it in the database and sends back the Server's Quantum Bases to the Client via a quantum channel. If someone intercepts, the bases change and the session key that client will generate will not match to the session key in the database, which will not let the communication go through.

The client computes the session key using it's Quantum Bases and Server's Quantum Bases and then uses the quantum channel to transmit data. Cloud service can identify the client in the database using client ID and then get the session key to decrypt the message. If the session key cannot decrypt the message Cloud service provider can conclude that somewhere along the line, there is an intruder and entire will have to be repeated again.

Steps:

1. First the Cloud Service Provider generates random Quantum base and shares it with KDC.
2. When a Client logs in, it first sends the request containing Client Name & other information to the KDC encrypted with its own password using the classical channel.

Client → KDC: $E_{PASSWORD\text{-}CLIENT}$ (Client Address) || ID_{CLIENT}.

3. Authentication Server inside the KDC authenticates the client and sends it the ticket-granting ticket (TGT).

KDC → Client: $E_{PASSWORD\text{-}CLIENT}$ (TGT).

4. When a client wants to access the cloud, it generates the random quantum base and sends it to the KDC along with TGT encrypted with its own password via the classical channel.

Client → KDC: $E_{PASSWORD\text{-}CLIENT}$ (QB_{CLIENT} || TGT) || ID_{CLIENT}.

5. KDC generates a session key by comparing the quantum bases of the cloud service provider and client and stores the session key in the global database.
6. After KDC generates the session key, it communicates the base to the client via quantum channel, due to which client can compute the session key itself using the it's base.

KDC → Client: $E_{PASSWORD\text{-}CLIENT}$ ($QB_{CLOUD\text{-}SERVICE\text{-}PROVIDER}$).

7. Once, the client computes the session key, it uses that session key to encrypt and send data to the server via a quantum channel. The client doesn't encrypt its Client ID since server uses the client ID to find the session key to decrypt the data.

Client → Service Provider: $E_{SESSION\text{-}KEY}$ (FILE) || ID_{CLIENT}

The major advantage of using this model is that it uses ease of deployment of a Kerberos Model along with the security benefits of Quantum Cryptography. [08] Kerberos allows the nodes to connection points of the various cloud networks to communicate with each other which in turns helps in providing Single Sign-On solution for using various cloud networks by signing on only once. Any Encryption Algorithm AES, DES et al. can be used for encrypting data.

VI. CONCLUSION & FUTURE WORK

This paper has introduced a new security architecture for Cloud Computing. This new method builds on top of the pre-existing architecture of using Kerberos for Single Sign-On authentication for flexibility and scalability but gives a workaround for the limitation of classical cryptographic algorithms by using QKD inside the KDC for key distribution and using Quantum Channel for transmission.

This paper introduced a new cloud computing environment, which suggested integrates and uses ease and simplicity of Classical Cryptography models and secure benefits of QKD as a new hybrid technique.

Since, there is always another side of coin, in future potential attacks on this like Large Pulse attack, Time Shift Attack, Fake State Attacks and others can be addressed. Apart from this in future, although tremendously complex, proper deployment architecture and the statistical evidence of the benefits could be studied.

REFERENCES

[1] "Heisenberg – Quantum Mechanics, 1925-1927: The Uncertainty Principle".

[2] SECURING CLOUDS – THE QUANTUM WAY Marmik Pandya Department of Information Assurance Northeastern University Boston, USA.

[3] Web Link: https://en.wikipedia.org/wiki/Qubit

[4] R.L. Rivest, A. Shamir and L. Adleman, "A Method of

obtaining Digital Signatures and Public Key Cryptosystems", Communication of the ACM, 21, 2(1978), pp 120-126.

[5] Zukarnain, Zuriati Ahmad, and Roszelinda Khalid. "Quantum Key Distribution Approach for Cloud Authentication: Enhance Tight Finite Key." International Conference on Computer Science and Information Systems (ICSIS’2014)

[6] Odeh, Ammar, Khaled Elleithy, Muneer Alshowkan, and Eman Abdelfattah. "Quantum Key Distribution by Using Public Key Algorithm (RSA)." ResearchGate

[7] Yaser Fuad Al-Dubai and Dr. Khamitkar. “A Proposed Model For Data Storage Security In Cloud Computing Using Kerberos Authentication Service” International Journal of Computer Engineering and Technology (IJCET), 4, 6, 11(2013).

[8] Kilor, Payal P., and Pravin D. Soni. "Quantum Cryptography: Realizing next Generation Information Security." International Journal of Application or Innovation in Engineering & Management (IJAIEM) 3.2 (2014).