INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 5, Issue 6)
Available online at: www.ijariit.com

Securing healthcare system using quantum cryptography mechanism

Shraddha T. Shelar
shelartshraddha@gmail.com
D. Y. Patil College of Engineering,
Akurdi, Pune, Maharashtra

Deepali D. Rane
deepalirane35@gmail.com
D. Y. Patil College of Engineering,
Akurdi, Pune, Maharashtra

ABSTRACT

In today's fastest-growing life, all need to be more secure in terms of advancement in technology. Everything is going to be a part of digitization. In this, almost everyone is using online storage for storing their personal and important and official secret information. To sustain the integrity there should be trustworthy services must be carried out in the back end. Online security has been provided for the cloud with very powerful privacy system. But still, there is a possibility of different interrupts in terms of stacks like DoS, Denial of Service attack can happen any time to break the normal flow of service. Henceforth, this paper will provide the strong security system for data storage with double encryption format and more complex structure, for we will express the algorithm through a quantum cryptographic environment to use under the homomorphism technique of modern cryptography.

Keywords— *Encryption, Quantum Key, Photon, Decryption, Cryptography, Polarization*

1. INTRODUCTION

Transferring data through a secure network is the most important concern of every professional when online data storage or data transfer facility used. To do so we have presented this paper for use and implementing the idea of quantum cryptography under the modern cryptography technique. In previous work encryption and decryption has been carried out using simple encryption algorithms like identity-based encryption. It is done by Adi Shamir [1] is based on the user's personal credentials. With more advancement, attribute-based encryption (ABE) has been expressed by Sahai[2][3]. It is based on the multicast technique. Manner. But this is done using the single encryption technique with attributes which is somewhat breakable mechanism if attributes received by an untrusted third party. When such a data transferring security mechanism is used for online service providing system such as medical health care system, there should be a very trusty environment to be used with the help of the best cryptographic technique. In this paper, we have expressed the newest technique called quantum cryptography in modern cryptography which is based on quantum physics. It is used for encryption and decryption using photons patterns which is a particle-based flow. So, this is a highly secure pattern to store data online. To store data of patients and doctors online we are using quantum cryptography for encryption. Hence only authorised user will understand the particles patterns for decrypting the data.

2. LITERATURE SURVEY

Before the digitization, everyone needs to keep patient's information on a paper format which is very hectic to keep it in a safe way. It's also a very weak system to understand the best doctor. So much more problems need to face to find the best doctor for the best treatment. To give a proper solution with positive direction, there should be a scheme needs to be implemented such that all the patients will get the easy and best treatment from the best doctor with all the medical history known. Online data stored in terms of the patient's medical history and the doctor's personal information like his/her medical experience, specialization. This all information should be stored with very securely using cryptographic techniques. Here there are many security options to make the encrypted system. Such as public-key encryption, digital signature. Homeomorphism. We have used modern cryptographic technique in which quantum cryptography [4][5] is the most secure and trustworthy mechanism.

Basically, cryptography is the technique of communication with different parties who don't keep trust in one another. For this sender must follow the key distribution. We have quantum key distribution (QKD) [6][7] in modern cryptography technique where secret communication between two parties is satisfied in a very secret manner. A key transfer is depending upon the flow of polarization pattern hence third party or who is willing to interrupt so-called as eavesdropper will be easily observed if the pattern breaks in the middle due to disturbance. The polarization concept introduced by the Heisenberg's uncertainty principle, which states that measuring the polarization pattern disturbs the flow and alerts the incomplete behaviour. Therefore, it is used in between the sender and receiver for key distribution to produce the secret key such as one-time data to transfer and communicate with another party in an absolutely secret manner.

Quantum cryptography has great value as its security is completely based on the law of physics. It includes QKD bit commitments with zero, one, left-45 right-45 angles of polarized particles. It uses the series of photons to transfer through fibre optic cable. This cable is not necessarily secure because photons travel through it are of randomized patterns. When it is received at the receiver's end using a comparison method the key is determined and then used as the safest communication.

3. OUR APPROACH

In this paper, we have proposed the quantum cryptography for producing a levelled trustworthy key for storing the data of patient and doctor. This paper gives a secure online scheme for health care database system. Here we are storing the patient's and doctor's information online through the registration process. Doctors have to register for providing the service. This information includes his or her personal information like medical registration number, name, specialization, address etc. Patients also have to register separately for getting the best treatment by storing the information such as name, medical history. We are producing the keys using the QKD and the above data will be stored in an encrypted format. So here decryption will be carried out when patient's and doctor's id get matched.

In this approach, the patient and doctors will store their secret information separately on the cloud.

- When patients need treatment, he or she will first register using his or her special information along with the previous medical history.
- On the portal, separately doctors will also register with their personal information with their registration number, specialization and experience.

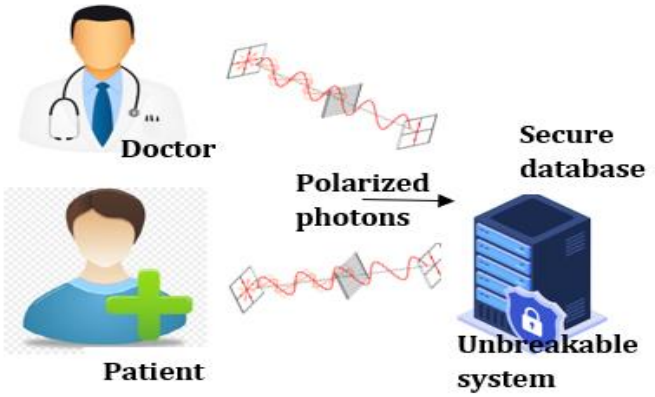

Fig. 1: Cloud deployment using QKD

- When patients wish to choose the doctor for treatment, he or she will search for a doctor by putting the information lie specialization and nearby area.
- When the doctor's information is displayed, it will be displayed with specialisation and ratings given by previous doctors.
- Once the appointment became fixed by the doctor, the patient will visit the hospital in person.
- At this time when a patient enters his registered number on portal doctors also needs to enter the registered number so as to see the original database entries.

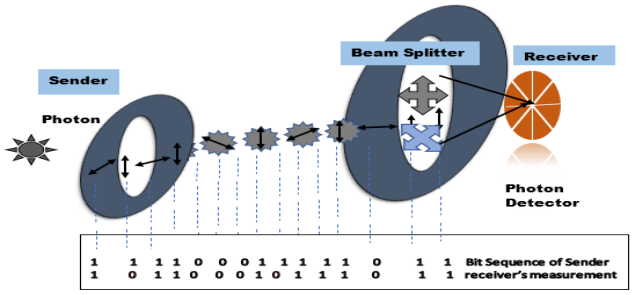

Fig. 2: Quantum key distribution polarization pattern

Here at this point, we are expressing the quantum cryptography [8][9] with QKD. As both the information's need to see from the cloud there should not be any kind of eavesdropper to interrupt the personal information. Data of both patients, as well as doctors, will be stored on encrypted forms on the cloud with the particle pattern hence it will b a truly unbreakable scheme by a single entity.

Firstly, when the patient and doctors register to the scheme, the data will be sent to the cloud in an encrypted format. This is through the QKD with the key exchange without any loss. When a patient goes to the doctor, if the keys in terms of id are not matched then it will not decrypt the text and original data will not be seen. The keys are generated as when the sender sends photons to a receiver, it sent in randomized particle ways through the polarized beam splitter. When it comes to the receiver, it is guessed without knowing the proper beam but, those beams which are not matched are discarded and send back to make the proper communication channel. If the photons states are detected by the eavesdropper then its measurement gets automatically changed and it is automatically detected at the other end.

4. CONCLUSION

Everyone is most concern about his or her health. Keeping and maintaining all the medical information history on paper is a very big task and requires extra efforts. To avoid it, we have expressed and presented a theoretical idea to store all the data online in most secure way using the mechanism of quantum key distribution theory. IT will also help to identify the best treatment facility for patients. This technique will truly help to provide the best service to patients and with leading time. Here. Quantum cryptography will play an essential role for storing the most important data of doctors and patients which will be carried out with no care system. It will help for making the unbreakable and trustworthy cloud

5. REFERENCES

[1] Shraddha Rasal, "Improving revocation scheme to enhance the Performance in Multi-Authority ABE" IJCA 2014, DOI:10.5120/15818-4542.

[2] Chase, M, "Multi-authority attribute-based encryption", Vadhan, S.P. (ed.) TCC 2007.LNCS, vol. 4392, pp. 515–534. Springer, Heidelberg (2007)

[3] Shraddha Rasal, "Enhancing Flexibility for ABE through the Use of Cipher Policy Scheme with Multiple Mediators", Springer's Advances (AISC). November 2014.

[4] Charles H. Bennett, "Experimental Quantum Cryptography", Journal of cryptography, IEEE, 1992.

[5] Jayadip Sen" Theory and Practice of Cryptography and Network Security Protocols and technologies", book by Intech,2013

[6] Stephen Wiesner "Conjugate Coding", ACM SIGACT News, Volume 15 Issue 1, New York, 1983

[7] Mohamed Elboukhari , "Quantum key distribution in practice: the state of art", IEEE symposium 2010

[8] Bennett, C. H. and G. Prasad, "quantum Cryptography: Public key distribution and coin tossing" Processing IRRR International Conference on computers, system and signal processing, Bangalore, India, December 1984. Pp 175-179.

[9] Bennett, C. H. and G. Prasad, "Quantum public key distribution system", IBM, Technical Disclosure Bulletin, Vol 28, 1985, pp 3153-3163.

