RSA Algorithm with Quantum and Artificial Neural Network for Securing Big Data

Krishnapriya Raj, Saranya T.R, Rosemary Antu, Roshni Alex
Department of Electronics,
MES College Marampally

***Abstract*: Cryptographic techniques are used for securing our private data from eavesdropping. Now a days data are analyzed and operated as big data. Big data analysis and techniques for managing such data is increasing and receiving more popularity. Big data are voluminous and difficult for processing and security issues arise in such big data managing because of its larger size. To solve this issue of privacy, we propose a cryptographic technique using RSA Algorithm combined with Artificial Neural Network and Quantum cryptography.**

Keywords:Cryptography, big data, rsa

1. INTRODUCTION

RSA is one of the popular encrypting technique, belongs to asymmetric key encryption standard .In order to make it more efficient and unbreakable it is combined with ANN (Artificial Neural Network) and Quantum cryptography.
Quantum cryptography traced from the concepts of quantum mechanics in which qubits of data are encoded, using photons key distribution is provided in quantum cryptography.
ANN (Artificial Neural Network) which works beyond the number theory, the requirements of time consumptions, computation load can be reduced to an extent. This kind of architecture minimizes the time requirement of RSA Algorithm.

Key words: RSA, Quantum cryptography, ANN

I.INTRODUCTION

In secure communication, cryptography is the science to convert a plain text to a cipher text with the use of keys. Cryptographic technique has vital importance in the field of science as confidential data privacy is a big thing.

Science, technology and business sectors are developing on a day-to day basis, data analyzed, stored and managed as big data. They are a kind of large volume of data which are both structured and unstructured such kind of big data are most vulnerable to insecurity. Big data security issue is now a big thing and we have proposed a cryptographic technique using RSA algorithm combined with quantum and neural network.

II.RSA ALGORITHM

RSA is one of relevant and most used encrypting technique using asymmetric encryption standard. Asymmetric encryption standard means it has 2 keys used to encrypt and decrypt the data using a public and a private key, which means, were at the sender the message will be encrypted with the public key of the intended recipient and at the receiver it decrypts the cipher text by using the private key of the recipient.

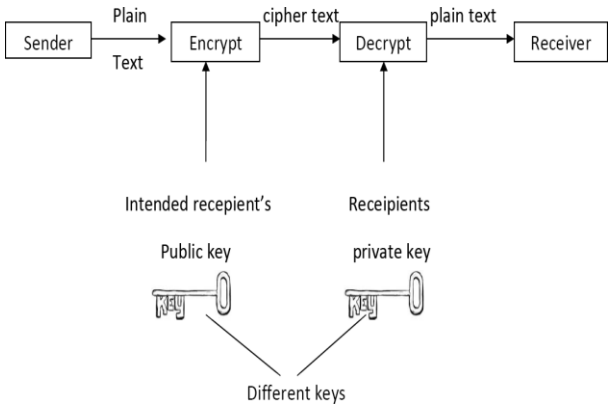

Fig 1:Encryption Process

RSA use large key size, it can be typically 1024 or 2048 bits long, due to larger key size more computational power and time consumption occurs, which is a major drawback to overcome this crisis, we proposed the new design of RSA standard with the combination of quantum cryptography and ANN.

III.QUANTUM CRYPTOGRAPHY

Quantum cryptography is derived from the idea of quantum physics, which is an unbeatable cryptographic technique with high security with an efficient key distribution technique at a faster rate.

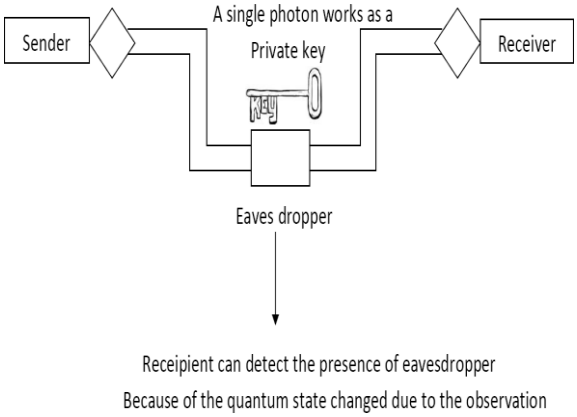

Fig 2:Quantum Cryptography System

From the theories of Heisenberg's uncertainty principle and principle of photon polarization, quantum cryptographic idea extracted.

Heisenberg's uncertainty principle states, that we cannot determine the velocity and position of a particle at the same time.

Principle of photon polarization states that when a plane polarized light is used to eject photo electrons, and then there is a preferred direction of emission of the electrons, clearly about the wave and particle behavior of light.

In quantum cryptographic technique, if someone eaves drop the quantum state of the data should change according to quantum mechanics, that is no one can unknowingly interrupted our data. To perform such tasks we need a quantum computer because the data are in qubits form. We can reduce the time consumption instead of solving one problem at a time we can solve a hundreds of problems at the same time.

IV. ARTIFICIAL NEURAL NETWORK

Neural network is a complex model which is similar to the neural system in a biological creature. The way neural network learns the true function is by building complex representation on the top of simple ones. It is a three layered architecture with an input layer, a hidden layer and an output layer. Its depth increases as the number of hidden layer increases between the input and output layer, its width increases as the number of nodes or neurons increases in the hidden layer. From the input layer the information is transmitted linearly and then via a non linear path it goes to the next layer and this continues until it reaches the output layer, here data are transmitted as weights instead of bits or bytes

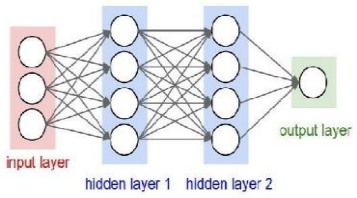

Fig 3: Neural Network Model

V. CONCLUSION

RSA is one of the efficient cryptographic standards, its major drawback is the lengthy key size and this takes more time for encryption and decryption. Combination of quantum cryptography and ANN Architecture ensures more security, with a higher complexity and faster processing than conventional RSA mechanism.

REFERENCES

[1] A.Mahdy, D. Chait, "A Survey on Quantum and Classical Cryptography ", Available:http://www.csc.org/southcentral/EJournal/2008/papers/p-0006.final.pdf[Accessed: September 2013

[2] Amita SharmaDeepshikha Sharma, The IIS University, Jaipur, India, "Big data protection via neural and Quantumcryptography",Available:https://ieeexplore.ieee.org/document/7724953/metrics#metrics

[3] A.K. Lal, Dr. S.Sharma, "The New Approach of Quantum Cryptography in Network Security", International Journal Of Emerging Technology and Advance Engineering, ISSN: 2250-2459(online)

[4] Abhishek Bhardwaj, Research Scholar, Subhranil Som2, Associate Professor, AIIT, Amity University Uttar Pradesh Noida, U.P., India,2016 1st International Conference on Innovation and Challenges in Cyber Security (ICICCS 2016) "Study of Different Cryptographic Technique and Challenges in Future"

[5] Moumita Chakraborty ,Department Of Computer Science & Engineering Chaibasa Engineering College, Techno India Group, Chaibasa, Jharkhand, India, Bappaditya Jana, Department Of Computer Science & Engineering Techno India Banipur West Bengal, India, Tamoghna Mandal , Malay Kule, Department of Computer Science and Technology, Indian Institute of Engineering Science and Technology, Shibpur "An Performance Analysis of RSA Scheme Using Artificial Neural Network" IEEE - 43488

[6] P. Mahajan and A. Sachdeva, "A study of Encryption algorithms AES, DES and RSA for security", Global Journal of Computer Science and Technology, vol. 13, no.15, (2013).

[7] P. Kumar and S. B. Rana, "Development of modified AES algorithm for data security", Optik-International Journal for Light and Electron Optics, vol.127, no. 04,(2016), pp. 2341-2345.