Indian Journal of Signal Processing (IJSP)
ISSN: 2582-8320(Online), Volume-1 Issue-1, February 2021

Quantum Cryptography for Security of Data in Smart Grid System

B.Kedar Nath,B.Ramanuja Charya, Y.V.Avinash, Siva Priya

Abstract: ***Smart grid is a highly reliable power system equipped with cyber-physical framework with sustainability of energy production, distribution and usage. It is a planned network that uses information technology to supply power efficiently and securely. The flow of energy in smart grid is bidirectional i.e. two way communication with control. It used for power monitoring, distribution of automation and protection. It offers ascend to significant measures of heterogeneous power information and plausibility of numerous assaults on the shrewd framework which bargains the privacy and trust-worthiness of the power information. The Aim is to avert digital assaults on the Smart Grid framework utilizing Quantum Cryptography guideline.***

Keywords Quantum cryptography, QKD, RSA, Power Data, Smart grid.

I. INTRODUCTION

Keen networks have been producing from decades as a significant role of the vitality environment. From savvy meters, keen machines to sustainable power source assets. Vitality has been given through imaginative innovations prompting a superior control of utilization, utilization of information progressively and alterations of vitality streams for the fundamental target of a productive administration of the electrical system. This speedy advancement of savvy networks combined with IOT gadgets has brought the issue of digital assaults.

Electrical power stations and atomic offices have demonstrated ruptures that need to be controlled manually. Shrewd matrices have been a significant piece of power systems including various devices. It has improved creation, appropriation, utilization and capacity of vitality. The digital technology that allows for twoway communication by sensing along the transmission lines between utility and its customers is called a smart grid. Smart grid has the potential to help you save money, manage your electricity. The smart grid conceptually works taking care of electrical energy flow interface as well as communication interface

Manuscript received on 19 January 2021 | Revised Manuscript received on 29 January 2021 | Manuscript Accepted on 15 February 2021 | Manuscript published on 28 February 2021.

***** Correspondence Author

B.Kedar Nath, Department of Computer ScienceEngineering, SRM Institute of Science & Technology, Chennai, India

B.RamanujaCharya, Department of Computer ScienceEngineering, SRM Institute of Science & Technology, Chennai, India

Y.V.Avinash, Department of Computer ScienceEngineering, SRM Institute of Science & Technology, Chennai, India

Siva Priya, Asst. Professor, Department of Computer ScienceEngineering, SRM Institute of Science & Technology, Chennai, India

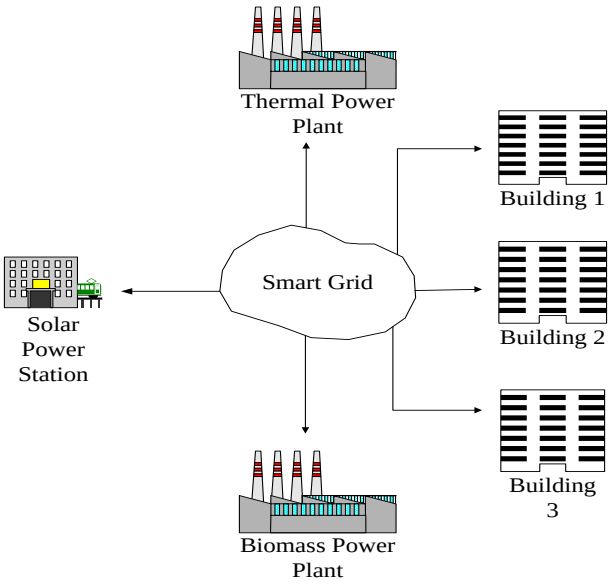

Figure 1: Smart Grid

The presentation of PCs and complex gadgets to modernize the electric lattices has opened breaks of security prompting digital assaults that utilization PCs vulnerabilities to infiltrate systems. For such cases Quantum cryptography provides a method for recognizing and vanquishing an enemy who may attempt to catch or assault the correspondences. Single photons are utilized to deliver secure arbitrary numbers among clients, and the irregular numbers are then used to validate and scramble the network control information and directions.Since the irregular numbers are created safely, they identified as cryptographic key material for information confirmation and encryption calculations.

II.LITERATURE SURVEY

Progressions in data and correspondence innovation have built up a universe of quicker and productive method for trading the data. Information that is essential for business activities ought to be available to all offices and transferable to other working organizations that work inside a system. These incorporate different client reports financials, restorative records, and corporate information. The present information assurance strategies will never again be compelling. The innovation known as Quantum Key Distribution or QKD is the main exchange strategy that is provably verified by the laws of material science to help secure .the touchy information we convey. There are different vulnerabilities in frameworks we use today Consider an individual sending an exceptionally characterized record utilizing the web. So outrageous consideration must be taken to verify the data the data sent is carefully bolted and sent to the beneficiary.

The current standard for scrambling information is called Public Key Cryptography. Sender makes an advanced key to verify the archives. Since the data is sent over the web, which is vulnerable to undetected block attempt. This would make it simple for a system programmer to catch and make a duplicate of the grouped reports. By replicating the information, the programmer can misuse vulnerabilities in open key cryptography in the end including quantum PCs to reproduce an ace key and after that access many ordered archives. This case of a traded off information transmission is really conceivable in true circumstances. QKD depends on creating a totally irregular key and safely transmitting it separate from the encoded information key.

Key information is made by a quantum motor and transmitted as a flood of photons through a fiber-optic quantum connect. The key is totally arbitrary and contains quantum data that must be effectively perused by the proposed beneficiary. For instance, the profoundly ordered report is over the web and their quantum motor creates an irregular key. Information on the best way to recreate the key is then transmitted through the quantum connect to the sender. While it is conceivable that a programmer can catch the report however he can't reproduce the key. At the point when the programmer attempts to block the photons stream in the quantum connect, any interference or adjustment to the photons will alarm the arrangement of the unapproved get to.

The advantages of utilizing secure fiber line bode well in every single ensured correspondence. In any case, the photon transmission is restricted to some specific range. This physical restriction is tackled by making a chain of QKD believed hubs spread over the areas. These enable keys to be shared over long separations and between various clients Proprietary data that is sent over the web can be taken and replicated. Current encryption strategies can ensure the information; anyway enhancements in processing innovation will in the long run outcome in the decoding of these standard codes. Quantum Key Distribution is an answer that is provably verified and can be utilized in verifying all the heterogeneous power information that is being transmitted in the savvy matrix where all the data is shared through lattice lines and all the data is in fact in danger of being duplicated by the system programmer.

III.PROPOSED SYSTEM

Quantum cryptography gives methods for distinguishing and crushing an enemy who may attempt to capture or assault the correspondences. Quantum cryptography is perfect with electric network control interchanges, giving solid security affirmations established in the laws of material science, without presenting over the top deferrals in information conveyance. The proposed framework comprises of utilizing RSA cryptographic calculations

IV.CRYPTOGRAPHY

Cryptography is the system which is utilized to verify correspondence between two gatherings in the open condition where unapproved clients and malevolent assailants are available. In cryptography there are two procedures i.e. encryption and decoding performed at sender and collector end individually. Encryption is where basic interactive media information is joined with some extra information (known as key) and changed over into unintelligible encoded arrangement known as Cipher. Unscrambling is the invert strategy as that of encryption where the equivalent or distinctive extra information (key) is utilized to translate the figure and it is changed over in to the genuine media information.

Classical Cryptography Method is old style cryptography depends on the science and it depends on the computational trouble of factorizing huge number. The security of old style cryptography depends on the high multifaceted nature of the scientific issue for the occurrence factorization of enormous number. In the old style cryptography the first information i.e. the plain content is changed into the encoded organization. The key known as information string which is utilized to control the change of the information from plain content to figure content and without the key none can peruse the information.

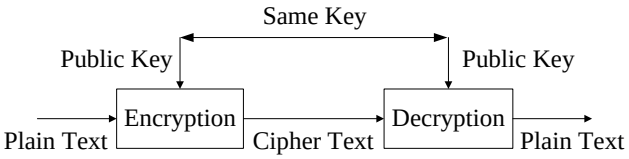

Figure2: Classical Cryptography Method

Quantum Cryptography Method depends on material science and depends on the law of quantum mechanics. It is an emerging innovation which stresses the wonders of quantum material science wherein two gatherings can have secure correspondence dependent on the invariabilities of the law of the quantum mechanics. Quantum mechanics is the scientific system or set of standards for the development of physical speculations.

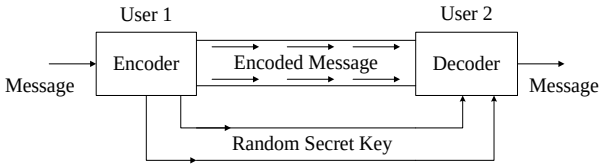

Figure 3: Quantum Cryptography Method

Quantum Key distribution (QKD) enables to produce a safe key that sent mystery data safely starting with one area then onto the next. It ensures security where old style cryptography frameworks just can't. This is conceivable by utilizing entrapped photons and two recipient structures in shrewd network.

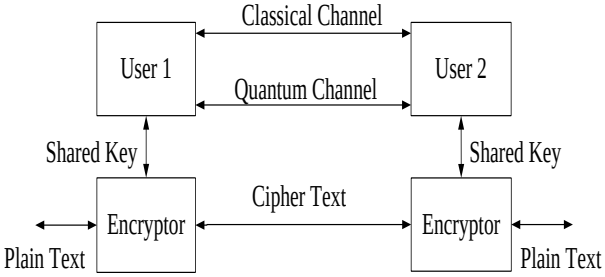

Figure 4: Quantum Key Distribution

V.METHODOLOGY

Let's assume two users would like to exchange the information, but they are in different buildings with the source position between them.

Both users will have a crystal to convert the laser light into pairs of entangled photons. These photons are in a state; such that their directions will be measured when the polarization of two photons is opposite i.e. +45 degrees and -45 degrees.

After measuring, a shared key is obtained at two users. From the crystal the created photon pairs are directed separately into optical fibers. These fibers are connected to roof of the CIT building where two telescopes are located; one pointed towards User1 and the other towards User2. The photons travel through free space from the source telescopes to identical telescopes located at the IQC headquarters and the PI building.

Now focus on User1 photons that are transmitted from one end to other by a telescope, these photons are channeled into a receiver box. Once in the receiver, the photos are directed through a system that measures the polarization of each. The photons polarized horizontally or +45 degrees are recorded as zero, the photons polarized vertically or -45 degrees are recorded as 1.

With the string of 0 and 1 a key will be generated at the User1 end. User2 also have the similar measurement on his photons to obtain the same sequence of bits and they share an identical key. However, the keys only agree if the photos are left undisturbed. If an eavesdropper disturbed the system then inconsistencies get created between User1 and User2 keys. Both users are able to see the errors and can come to conclusion that the key has been compromised.

If no eavesdropper has been detected, the information or messages get exchanged between both the users. The received message will be converted into binary and then the string of zeros and ones are added that forms the key to the binary message, thus encrypting the transmission.

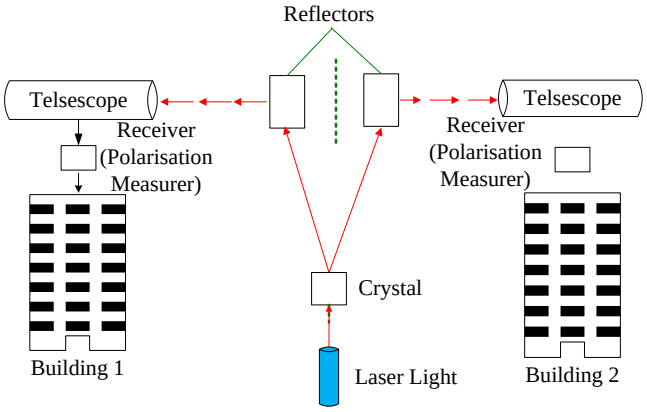

Figure 5: Random Key Generator

The encrypted message will be sent to Other User and gets decrypted with same copy of key.

VI.CONCLUSION

Quantum cryptography gives methods for recognizing and overcoming a foe who may attempt to capture or assault the correspondences. Single photons are utilized to deliver secure arbitrary numbers among clients, and these irregular numbers are then used to confirm and encode the framework control information and directions. Since the arbitrary numbers are created safely, they go about as cryptographic key material for information confirmation and encryption calculations. A ton of privacy-enhancing advancements have been acquainted with shrewd networks.

In this paper, we presented another route dependent on quantum Cryptography. Ventures that discharge quantum gadgets have another market, and analysts that work on this new region will have a few fascinating difficulties both in programming and in equipment for example, managing codification of the messages and sign transmission. Quantum calculation can break some significant codes dependent on old style advances. Subsequently, electrical power matrices are helpless against aggressors with a quantum PC, and individual data of clients can be spilled. Quantum mechanics can give a more grounded degree of cryptographic crude, in light of the fact that their calculations depend on RSA.

REFERENCES

1. President's Council of Advisers on Science and Technology. (2007, Aug.). Leadership Under Challenge: Information Technology R&D in a Competitive World. An Assessment of the Federal Networking and Information Technology R&D Program, Washington, DC, USA. [Online]. Available: http://www.nsf. gov/geo/geo-data-policies/pcast-nit-final.pdf.
2. Cyber-Physical Systems Executive Summary: Cyber-Physical Systems Summit, St. Louis, MO, USA, Apr. 24-25, 2008, Accessed 25-09-2012. [Online]. Available: http://varma.ece.cmu.edu/ Summit/CPS-Executive-Summary.pdf.
3. E.A. Lee, ''Cyber Physical Systems: Design Challenges,'' in Proc. 11th IEEE ISORC, 2008, pp. 363-369.
4. ''Workshop Overview Workshop on Foundations of Dependable and Secure Cyber-Physical Systems,'' in CPS Week 2011, Chicago, IL, USA, Apr. 11, 2011. [Online]. Available: https://www.truststc.org/conferences/11/CPSWeek/index.htm.
5. Y. Mo, T.-J. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, and B. Sinopoli, ''Cyber-Physical Security of a Smart Grid Infrastructure,'' Proc. IEEE, vol. 100, no. 1, pp. 195-209, Jan. 2012.
6. S. Sridhar, A. Hahn, and M. Govindarasu, ''Cyber-Physical System Security for the Electric Power Grid,'' Proc. IEEE, vol. 100, no. 1, pp. 210-224, Jan. 2012.
7. R.H. Lassetter, ''Smart Distribution: Coupled Microgrids,'' Proc. IEEE, vol. 99, no. 6, pp. 1074-1082, June 2011.
8. M.G. Simpson, ''Chapter 1 Plant Systematics: An Overview,'' in Plant Systematics, 2nd ed. New York, NY, USA: Academic, 2010.
9. S. Hansman and R. Hunt, ''A Taxonomy of Network and Computer Attacks,'' Comput. Security, vol. 24, no. 1, pp. 31-43, Feb. 2005.
10. G. Creech and J. Hu, ''A Semantic Approach to Host-Based Intrusion Detection Systems Using Contiguous and Discontiguous System Call Patterns,'' IEEE Trans. Comput., vol. 63, no. 4, pp. 807-819, Apr. 2014.