International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering (IJAREEIE)

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 6.392|

||Volume 9, Issue 4, April 2020||

Securing the Communication Network of Internet of Things in Smart Cities through Quantum Deployment

Kowsalya T[1], Sukirtha S[2], Krithika S[3]

UG student, Department of Electronics and Communication Engineering, Kumaraguru College of Technology, Coimbatore, India[1]

UG student, Department of Electronics and Communication Engineering, Kumaraguru College of Technology, Coimbatore, India[2]

Asst. Professor, Department of Electronics and Communication Engineering, Kumaraguru College of Technology, Coimbatore, India[3]

ABSTRACT: A smart city is a designation given to a city that integrates ICT (Information Communication and Technologies) and physical devices connected to the IoT (Internet of Things) network. The concept of smart city highlights the need to enhance quality interconnection and performance of technologies. They promote cloud-based and IoT based services in which real world user interfaces using smart phones, sensors and RFIDs. IoT inputs the required intelligence into basic building block of the city and helps in making it smart. As we can see, the base of any'thing' smart is IoT, which involves cloud computing. There are many privacy issues and security threats to be addressed in cloud computing. Without addressing these issues, a smart citywould be baseless with the evolving technology that puts a stake on the CIA (Confidentiality, Integrity and Authentication) of cloud computing. This paper focuses on addressing such threats and replacement of the conventional technologies with QKD (Quantum Key Distribution). Based on it, a system for secure communication is being suggested using aRandom Number Generator.

KEYWORDS: Internet of Things; cloud computing; Quantum key Distribution; Random number generator.

I. INTRODUCTION

In today's scenario, smart city is a product of advanced development of the new era of information technology and smart economy using IoT (Internet of Things) as its heart. Cloud computing and IoT are presently the two most important ICT (Information and Communication Technologies) models that are shaping the next generation of computing. Smart cities are nothing but the convergent domain of IoT and cloud computing[12]. IoT inputs the required intelligence into basic building blocks of the city and helps make it smart. Smart cities possess massive potential in completely turning around the operation efficiency of a city and IoT is the technical foundation behind this[10][11]. This explosive growth of ICT's manifested in smart cities and IoT creates more myriad benefits. However having the advantages on one side there are various threats prevailing in IoT and cloud computing such as data breaches, DDoS attacks, account hijacking, malicious insiders etc. With the emerging era of quantum computers, the existing security algorithms can easily be cracked and the citizen's data becomes more vulnerable to the above mentioned threats as the security of a system lies in the hardness of breaking its encryption. Therefore in this paper we explain how quantum key distribution can serve as a best alternate in such a way that the data is completely secured. We also suggest a system for secure data transmission using the basic principles of QKD (Quantum Key Distribution) implemented by using random number generators.

II. CLOUD COMPUTING AND ITS SECURITY ISSUES

The Internet of Things is increasingly becoming a ubiquitous computing service[1]. In any IoT device, communication with servers play a major role. As the servers are not cost effective, a remote network of server can be accessed online to manage and store huge volumes of data which is termed as Cloud computing. Owing to these unique characteristics of resource constraints, self-organization, and short range communication in IoT, it always resorts to the cloud for outsourced storage and computation. The three main cloud deployment models are Public, Private and Hybrid

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 6.392|

||Volume 9, Issue 4, April 2020||

clouds for personal, industrial and professional usage etc. The major cloud services include Platform (PaaS), Infrastructure (IaaS) and Software (SaaS) services respectively.

Cloud has many best practices such as regular assessment of cloud security, establishing solid access management policies, encryption of data in a secure way, implementation of cloud security monitoring etc. Despite of all these best practices due to weak authentication and encryption techniques there are series of new challenging security and privacy threats[3]. These include

A. Weak authentication and identity management

A lack of proper authentication and identity management is responsible for data breaches within organizations. Businesses often struggle with identity management as they try to allocate permissions appropriate to every user's job role. Poor identity management can leave gaping holes in enterprise cyber security[9]. Two-factor/ Multi -factor authentication systems, like one-time passwords and phone-based authentication, protect cloud services by making it harder for attackers to log in using stolen passwords. But making it harder to crack doesn't seem that harder in the upcoming years. Hence appropriate measures should be taken to overcome these threats

.

B. Hacked interface and insecure API

API (Application Program Interface) are used by cloud service providers and software developers to allow customers to interact manage and extract information from cloud services. Most cloud services and applications use APIs to communicate with other cloud services[6]. As a result, the security of the APIs themselves has a direct effect on the security of the cloud services. The chance of getting hacked increases when companies grant third parties access to the APIs. In a worst-case scenario, this could cause the business to lose confidential information related to their customers and other parties.

C. Data breaches

A data breach is an incident that involves the unauthorized or illegal viewing, access or retrieval of data by an individual, application or service[5]. It is the result of a malicious or probably intrusive action. The threats that impact traditional storage networks also threaten the cloud world. A data breach can expose sensitive customer information, intellectual property, and trade secrets, all of which can lead to serious consequences.

D. Distributed denial of service attacks (DDoS)

A distributed denial of service attack is a malicious attempt to disrupt the normal traffic of a targeted server, service, or a network by overwhelming the target or its surrounding infrastructure with a flood of internet traffic.[2] When cloud computing first became popular Distributed Denial-of-Service (DDoS) attacks against cloud platforms were largely unthinkable; the sheer amount of resources cloud computing services had made DDoS attacks extremely difficult to initiate. But with as many Internet of Things devices, smart phones, and other computing systems as there are available now, DDoS attacks have greatly increased in viability. If enough traffic is initiated to a cloud computing system, it can either go down entirely or experience difficulties.

III. SECURITY OF QKD

Data stored in cloud is usually subjected to various, modern techniques of cryptography in order to ensure the Confidentiality, Integrity and Authentication (CIA) of the information. These techniques include the public key algorithms like RSA, ECC etc which are used for secure net banking, emails, phone conversations and more. Most of the modern techniques follow the Public Key Encryption[8]. By the advent of Quantum Computers, the Public Key Infrastructure is put at stake. Quantum Key Distribution (QKD) makes use of qubits and is based on the laws of quantum physics, utilizing the polarization of photons for the construction of private key, transmitted via the optical channel/free space which gets disturbed upon measuring, thereby making it impossible to copy the key. Upon eavesdropping, any illegal act can easily be detected as the probability falls below a certain threshold and the mission can be aborted according to the BB84 protocol. In QKD, only the sharing of private key takes place in optical channel and with this key, the data is encrypted and transmitted through classical channel[7]. This demands that the classical channel be secured well through proper authentication. A real time example would be Micius, the quantum satellite launched by China in 2016. Further, there is a constrain of distance in key distribution through optical fibre cables which can be overcome by using satellites to transmit the key through free space as a medium.

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 6.392|

||Volume 9, Issue 4, April 2020||

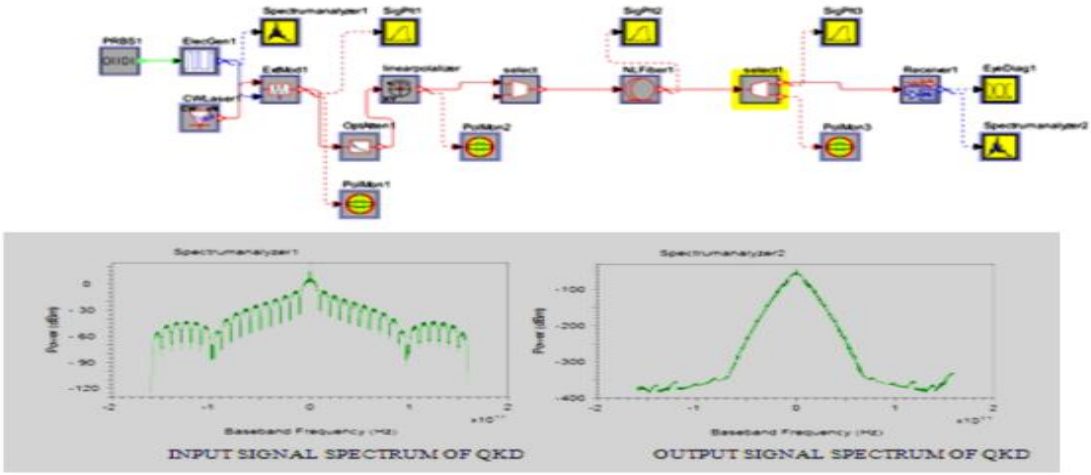

Fig 1. Simulation result of BB84 protocol using optsim

IV. SECURE COMMUNICATION SYSTEM

The system involves a conventional network where in a client to server data communication takes place while a large amount of data storage occurs in the cloud.

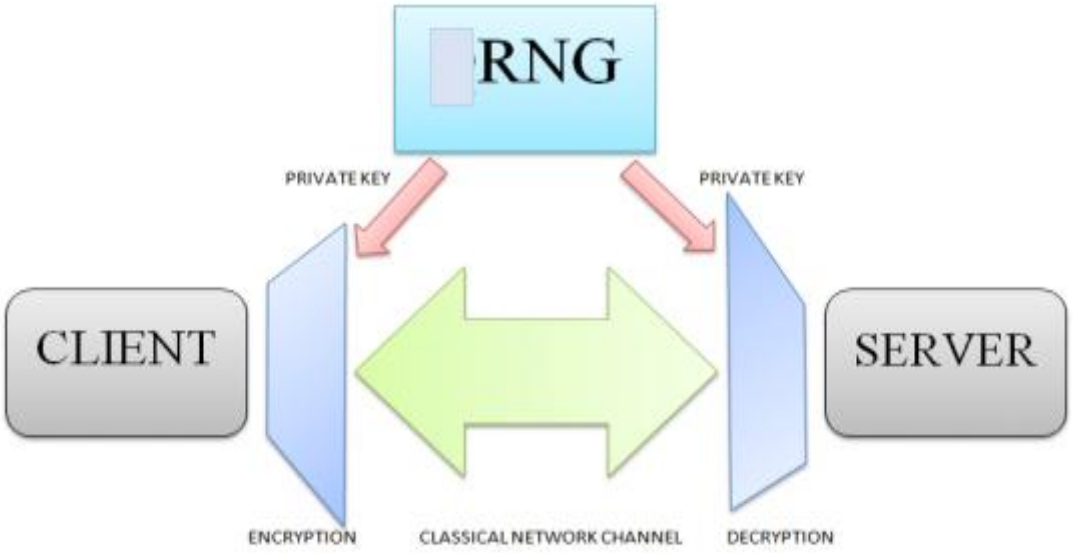

Fig 2. Block diagram of secure communication system

A communication network usually comprises of many intermediate nodes, in addition to the client and server. Data is encrypted with the private key at the transmitting interface before it makes its way to the server via these nodes facilitating end to end decryption. The functionality of the system is based on the existing protocols of quantum key distribution like BB84 protocol and E91 protocol.

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 6.392|

||Volume 9, Issue 4, April 2020||

Fig 3. Visualization of the System

The quantum key is shared between the client and server through free space via a satellite consisting of a Random Number Generator (RNG) thereby making use of the power of randomness in encryption. An RNG generates a random number of bits which will transmitted as entangled pair of photons (E91)and they willbe measured using rectilinear or orthogonal basis at the sending and receiving end (BB84). The key generated and basis chosen for measuring that key is random, increasing the complexity of hacking andsecures the information stored in cloud.

V. PROPOSED SOLUTION

Though QKD provides a provably secure encryption, the encrypted data makes its way through the classical channel for which authentication plays a key role in the information security. Multi-factor authentication is now in implementation. This reduces Man in the Middle and DDoS attacks.Still, attacks like shoulder surfing, phishing etc. are prevailing. To reduce these attacks, different passwords should be used at the time of log while improving its conventionality. In this regard, anybody signing up will be asked three personal questions (private). A master password will be generated as a result of the hash function of these answers. In addition, ten multiple choice questions will be asked and the answers should be chosen at random. A set of different combination of these answers could be then used as passwords, each being unique at the time of log in. Once all combinations are utilized, the process is repeated and another set of different password combination will be used for authentication.There will be a maximum of 30,000 password combinations that can be used for logging in at the end of this process. Conventional methods of verification like OTP (One Time Password)/Two step verification using mail id and session time limitsare added as additional factors for authentication. Questions from the repository will demand various combination of answers asked in a random manner in order to lower the risk of the mentioned security threats. Minimum time constrains for a user also reduces the risk of DDoS attacks.

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 6.392|

||Volume 9, Issue 4, April 2020||

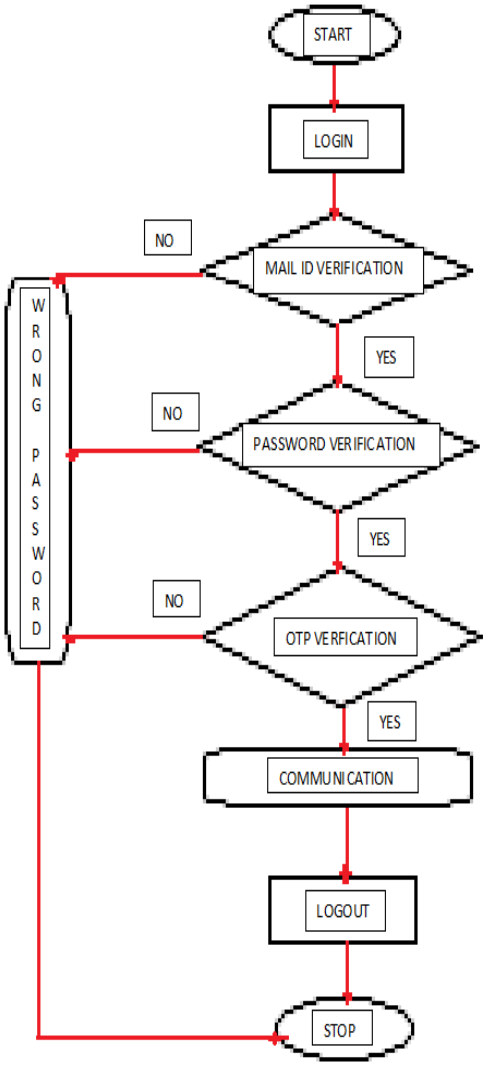

Fig 4. Flowchart describing the process

VI. CONCLUSION

In this paper we have analyzed the security of issues of cloud computing which has a major part in IoT. IoT plays a predominant role in developing a smart city, as smart city is all about data storage and linking information[4]. With this in mind we must also think about securing the citizen's data in all possible ways. So we have suggested a data transmission using QKD as it is proven to be the most secured way of communication, which provides better encryption. Our system overcomes most of the security breaches in cloud computing. Further working and research in this area is being carried out, leading us to a new and even safe cum secure protocol.

REFERENCES

1. S. Krithika and T.Kesavmurthy , "Securing IOT network through quantum key distribution" , International journal of innovative technology and exploring engineering(IJITEE), volume – 8, issue-6s4,April 2019.3
2. Ravi kumar choubey and Ahtisham Hashmi , "Cryptographic techniques in information security ", school of computing science and engineering , greater noida , India.
3. Kowsalya.T, Sukirtha.S and Krithika.S," Quantum key distribution for internet of things – a review", National conference on research advances in engineering and technology (NCRAET) , CSI college of engineering, Ooty, 15 march 2019.
4. Marmik Pandya " Securing clouds – the quantum way" , Department of information assurance, northeastern university, Boston , USA.
5. Zuriati ahmad zukarnain and Rosezelinda khalid "Quantum key distribution approach for cloud authentication enhance tight finite key", International conference on computer science and information systems (ICSIS'2014) , oct 17-18, Dubai UAE.

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 6.392|

||Volume 9, Issue 4, April 2020||

6. Suresh kumar P.H , Ambily pramitha , DR Rajesh R, " The quantum key distribution (QKD) based security enhanced cloud data center connectivity" International journal of latest trends in engineering and technology, vol(7),issue(4), pp.378-382.
7. V.Padmavathi , B.Vishnu Vardhan , A.V.N. Krishna , " quantum cryptography and quantum key distribution" , IEEE 6 th national conference on advanced computing (IACC), 2016.
8. Vishnu teja , Payel banerjee , N.N. Sharma and R.K. mittal , " quantum cryptography: state of art , challenges and future perspectives" , proceedings of the 7th IEEE international conference on nanotechnology , august 2-5 , 2007 , Hong kong.
9. Ajith. B , deepa . R , " end to end encryption using QKD algorithm" , international conference on innovative science and research technology , October 2017, Graz , Austria.
10. Dr Madhvi A Pradhan , Supriya Patnakar , Akshay shinde , Virendra shivarkar , Prashant phadatare "IOT for smart city : improvising smart environment " International conference on energy , communication , data analytics and soft computing (ICEDES).
11. Husam rajab , Tibor cinkelr , "IOT based smart cities" , IEEE international conference ,2018.
12. Salvisa aleksic , Dominic winkler , Forian hipp , Andreas poppe , Greald franzi and Bernhard schrenk " Towards a smooth integeration of quantum key distribution in metro networks" , International conference on transparent optical networks (ICTON) , July 20.