International Journal of Enhanced Research in Management & Computer Applications
ISSN: 2319-7471, Vol. 7 Issue 12, December-2018, Impact Factor: 3.578

A Study on 'Cyber-Physical Systems in the Cloud via Design and Development'

P. Bharathi Devi[1], Shamim[2], M.V.T. Ram Pavan Kumar[3]

[1,2,3]K.B.N. College (Autonomous), Vijayawada-520001, Andhra Pradesh, India

ABSTRACT

The design and development of Cyber physical systems has emerged as a major focus of study in recent years because to their promising potential in resolving difficult challenges. As the number of cyber physical systems (CPS) continues to rise, so too do the number of security issues that have arisen as a result of the wide variety of components used in CPS. The research presented in this article paves the way for the creation of an unique QuantumProtocol that operates on the Cloud and has the potential to be included into cyber physicalsystems. Various algorithms, such a key caching method and a secure key transfer algorithm, are created and implemented as part of the protocol design process. The suggested protocol is shown to improve CPS security over the cloud network in a quantifiable way in the simulation results.

Key words: Cyber physical systems, cloud computing, cryptography, quantum cryptography

INTRODUCTION

Cloud computing

A novel computing paradigm, the cloud computing, has become a viable solution on top of virtualization for commoditization of computing resources. Though it has potential to leverage individuals and organizations with plethora of advantages, there are strong security concerns over outsourced data. The existing security models are built with certain assumptions. The solutions like distributed accountability, provable data possession (PDP), Third Party Auditing (TPA) and so on are secure as long as the assumptions hold true. To ensure fool proof security for cloud storage security little research has been made on quantum key cryptography. Since the quantum key distribution is unconditionally secure we propose a new scheme known as CloudQKDP (Quantum Key Distribution Protocol for CloudComputing) which exploits the benefits of quantum mechanisms to secure cloud storage and data dynamics. We consider a case study in which three parties such as cloud server, data owner and trusted client have provably secure communications with our proposed scheme which uses random oracle model. Our empirical study revealed mixture of success and failurerates with private and public clouds respectively.

Need for Quantum Cryptography

When compared to traditional cryptography, Quantum Key Distribution (QKD) has properties that can make is unconditionally secure. The former is based on computational complexity of mathematical problem while the latter is based on laws of quantum mechanics. Cryptanalysis has been around which paves the way for breaking security of public key cryptography due to the availability of quantum computers in future. It does mean that quantum computers provide sufficient power to break the computational complexity in the mathematical problem used by public key cryptography. Therefore it is indispensable to use quantum key distribution along with best possible classical cryptographic primitives. As cloud users have concerns about outsourcing their data to remote cloud servers, cryptography plays a vital role in securing data transmission. Quantum cryptography when succeeded to be used for cloud storage and retrieval, it will be a paradigm shift in protecting data with unbreakable security.

STATE OF THE ART

Quantum Key Distribution Protocols

Transport Layer Security (TLS) and IPSec are widely used applications for Internet security. The TLS is based on Secure Sockets Layer for secure communication while the IPSec is a suite of protocols meant for ensuring that the communications over Internet Protocol (IP) are secure. According to Arkko and Nikander [2] the current policy mechanisms of IPSec are inadequate with respect to authorization. Oracle [3] states that the TLS has drawbacks such as inability to provide end-to-end solution. Mink, Frankel and Perlner [1] integrated QKD into the security applications such as TLS and IPSec using an additional support layer that helps in communication between QKD

and those security applications. Authenticated Key Establishment (AKE) is the take pertaining to cryptography which is achieved by QKD. QKD has been proved to be secure against adversaries using future computational improvements. Mosca, Stebila and Ustaoglu [4] described BB84 QKD protocol which is then integrated with traditional AKE models. Their experiments proved that QKD can withstand future advances in computing arena. They used both classical cryptography and QKD and tested long-term and short-term security of BB84.

Shih, Lee and Hwang [5] proposed two three party QKD protocols and claimed that they were efficient. However, later, Gao et al. [6] proved that those QKDPs are susceptible to dense-coding attack. The problem with these protocols is that eavesdroppers can use entangled quits in order to obtain session keys without introducing errors in ongoing communications. Cotler and Shor [7] proposed a new QKDP that works faster than the existing such protocols. The protocol increases key generation rate by using a single photon's spatio-temporal modes effectively. Fiber optic and line of sight channels were used to demonstrate the proof of concept.

According to Zeng and Wang [8] improved QKD that can verify identity of communicator and distribute quantum secret key concurrently. However, their QKDP has a distinct problem such as common key reservation. Chuan et al. [9] proposed a new QKDP with pulsed homodyne detection that makes use of weak coherent states. This protocol was proved to be robust to attacks such as Trojan-horse and intercept-resend. Huang et al. [10] proposed and applied a novel QKDP to Wireless Sensor Network (WSN). It was an agent oriented implementation of quantum communication for Wi-Fi network. With this the QKD could handle multiple users in the network. Brougham et al. [11] proposed a high dimensional QKDP that makes use of Franson interferometers. However, they concluded that usage of single Franson interferometer is not enough to have adequate security. Instead multiple interferometers cloud be a better solution for high – dimensional QKD.

Lim et al. [12] proposed a new device independent quantum key distribution mechanism that is compatible with Bell's theory with respect to inequalities between two parties. Thus they could overcome the problem of detection loophole attack. Dianati and All´eaume [13] described transport layer protocols used for QKD for the implementation of European project known as "Secure Communication Based on Quantum Cryptography".

Threats to Cloud Computing Security

According to Ted Samson the Cloud Security Alliance (CSA) identified nine top threats to cloud computing security. Data breaches are the first threat which causes a Virtual Machine (VM) to gain access to the cryptographic keys of another VM with ease. A single breach of security in one application can cause damage to all clients. Encryption can be used to avoid data breaches but when the cryptographic keys are compromised, the whole security is lost. Second threat is data loss which might be due to attacks launched by hackers to delete your data. In the process if the encryption keys are lost, it should be the worst case. Service traffic hijacking is the third security threat. When an adversary gains access to credentials, it could lead to hijacking of user's requests to illegal web sites that make use of the credentials. Insecure interfaces and API is the fourth threat for cloud security. The APIs that are vulnerable can expose applications to cloud security issues such as integrity, confidentiality, availability, and accountability. The fifth threat which is more frequent is denial of service attack which proves costly to cloud users as they are given services in pay per use fashion.

Malicious insiders are the sixth security issue that is difficult to address as the malicious insiders have legal access to data and services rendered. They can also misuse the keys stored in cloud storage. Cloud abuse is the seventh security problem that is practiced by hackers to break cloud security in order to launch various kinds of attacks such as sharing pirated software, propagating malware and so on. The eighth threat to cloud computing security is the lack of knowledge of cloud computing and security keys on the part of cloud users. Extensive knowledge when acquired can help cloud users to overcome this problem. Shared technology vulnerabilities are the very important threat to cloud security. When the vulnerabilities are shared, that causes havoc to the whole cloud computing phenomenon.

Secure Storage Solutions for Cloud

Cloud computing, a new model of computing, has become a reality which facilitates data owners to outsource their data to cloud besides providing various other services. However the cloud servers are treated "untrusted" by cloud users as their valuable data is stored in remote servers. There are many security concerns over the outsourced data and communications between the cloud server and cloud users. Many solutions came into existence in order to curb this problem. Lin and Tzeng [14] proposed a threshold proxy re- encryption scheme that secures outsourced data. Their security architecture is facilitated by number of storage servers and key servers. The storage servers store data while the key servers act as access nodes. The scheme supports encoding, encryption and forwarding. Each storage server and key server independently performs encoding and re-encryption and partial decryption respectively.

Provable Data Possession (PDP) is technique used to ensure integrity of outsourced data. Many PDP schemes came

into existence such as PDP [15], SPDP [16], DPDP – I and DPDP – II [17], CPOR – I and CPOR – II [18]. These schemes tried to make the data provably secure. However, recently, Zhu et al. [19] presented a cooperative PDP scheme in a distributed and multi-cloud environment. The scheme is provably secure which is based on hash index hierarchy and verifiable response. The scheme is also efficient in terms of minimizing computational costs and communication overheads. Proof of data integrity is another scheme proposed by Kumar and Saxena [20] which provide data integrity proofs besides supporting Service Level Agreements (SLAs) that can have mutual agreements between the service provider and service consumer.

Wang et al. [21] focused on cloud storage security by implementing a security scheme known as "Third Party Auditing" which audits data for integrity verification. The scheme supports batch auditing besides supporting data dynamics which can't be done easily with cryptographic systems.

Sundareswaran, Squicciarini and Lin [22] proposed a decentralized information accountability framework for cloud storage security. They made use of JAR programmable features in order to encapsulate user's data and security policies in JAR files and that possess mechanisms for distributed accountability. In all the cloud computing solutions there was more importance to data integrity rather than providing end to end security.

PRILIMINARIES

Quantum Cryptography and BB84 Protocol

Quantum cryptography is based on quantum mechanics where the qubit used in key distribution cannot be altered without the possibility of making changes to the original state. In order to exchange a sequence of bits randomly two parties such as Alice and Bob make use of quantum channel to ensure security in communication using one-time pad. When any adversary such as Eve attempts to eavesdrop, detection of it is possible with high probability. The BB84 protocol supports quantum cryptography where quantum channel is used by two parties to send qubits. However, the classical channel which is also used by them is insecure. Quantum states can be represented using different polarizations. The BB84 protocol for secure communication between Alice and Bob works as described here.

1. The random sequence of bits sent Alice are encoded and sent to Bob.
2. Bob is supposed to receive photons and decode them randomly.
3. Both parties compare some bits that have same basis. In the process the test is considered successful if the estimated error rate is less.
4. At the end, Alice and Bob can obtained a secret key using other bits after subjecting them to privacy amplification and error correction.

The communication process with respect to secure key distribution using BB84 protocol is as presented in Table 4.1.

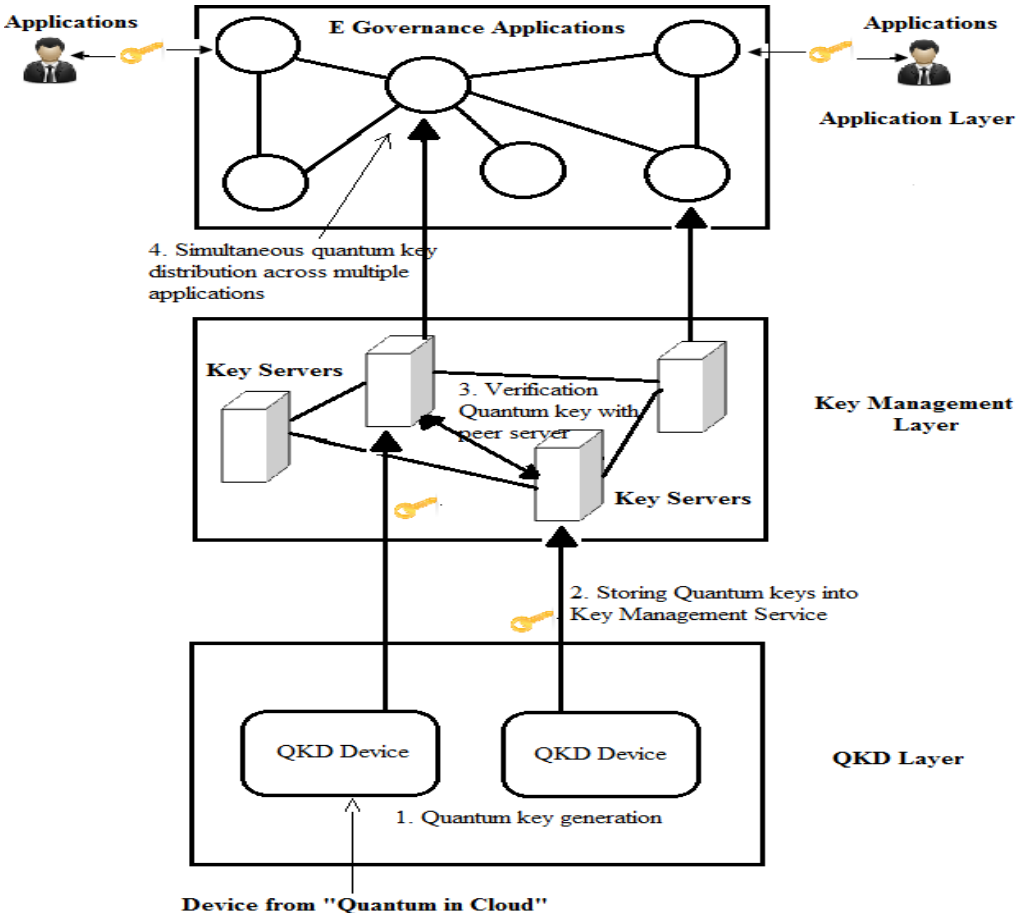
Table 4.1. BB84 protocol

Alice's String	**1**	**1**	**0**	**1**	**0**	**0**	**1**	**0**	**1**	**1**	**1**	**1**	**0**	**0**
Alice's basis	+	+	+	X	x	+	x	X	X	x	+	+	+	+
Alice sends	-	-	|	\	/	|	\	/	\	\	-	-	|	|
Bob's basis	+	x	+	+	x	+	x	+	X	x	+	+	+	+
Bob's string	**1**	**0**	**0**	**1**	**0**	**0**	**1**	**1**	**1**	**1**	**1**	**1**	**0**	**0**
Same basis?	**Y**	**N**	**Y**	**N**	**Y**	**Y**	**Y**	**N**	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**
Bits to keep	**1**		**0**		**0**	**0**	**1**		**1**	**1**	**1**	**1**	**0**	**0**
Test	**Y**		**N**		**N**	**Y**	**N**		**N**	**N**	**N**	**Y**	**Y**	**N**
Key			**0**		**0**		**1**		**1**	**1**	**1**			**0**

Conceptual Overview of the Proposed Model

The proposed secure key management model is a comprehensive solution to e- Governance in India. The proposal

encompasses end to end security among different layers involved in the e-Governance applications. E-governance applications are highly sensitive and they are to be protected from unauthorized access and also from all kinds of adversaries. Towards this end, in this sub section, a conceptual overview is provided for the proposed model. There are many communication hurdles due to internal and external attacks in the real world communication networks. Therefore, this proposal is aimed at providing a comprehensive model that can protect the interests of all stake holders of e-Governance. Secrecy and effective communication are given importance while designing the framework. Since the e-Governance applications involve many parties, they are to be protected under a secure domain. Towards this end, the proposed conceptual model is as shown in Figure 1. Various custom protocols were proposed to realize the model. For highly secure efficient key management, a technique is proposed that exploits quantum cryptography. Quantum device provided by "Quantum in the Cloud" [15], a quantum test bed, of University of Bristol isused for experiments.



Conceptual framework with quantum network for proposed e-Governance applications

As shown in Figure 1.1, there are three layers in the proposed framework namely Quantum Key Distribution (QKD) layer, key management layer and application layer. The QKD layer makes use of quantum device provided by "Quantum in Cloud" of University of Bristol. This layer is responsible to generate a shared random secret key that can be used by the parties involved. Pool of such keys is maintained by servers of the key management layer. Ultimately the application layer consumes the keys as and when required. Key management plays vital role in privacy and security of any communication network [12]. There is key management interoperability protocol named Key Management Interoperability Protocol [13]which has important role to play in distributed applications for key management. This protocol was introduced in key management layer is Organization for the Advancement of Structured Information Standards (OASIS) [14]. The security mechanism is described here. First of all, the web interface provided by "Quantum in Cloud" device is used to generate quantum keys. The keys are then handed over to key management service which is crucial for secure communications. The quantum key verification is done among the peer servers that are part of key management service. Then simultaneous quantum key distribution is made across different e-Governance applications that ensure the underlying operations to be made in highly secure fashion.

As shown in Figure 1.2, there are three nodes and two links that show effective and secure communication. The information passed through VPN is encrypted to avoid eavesdropping possibilities and other attacks. QKD devices form QKD layer that takes care of generation of random shared keys. The Key manager PC, key management server does have a Remote Procedure Call (RPC) done locally. Between node A and node B there are two channels

established. The classic channel is meant for transferring data while the quantum channel is meant for sharing key in secure fashion. They key management server is responsible to manage keys and provide them access to a group of privileged users. There is user management service that takes care of privileges being assigned to genuine users and tracking them from time to time. Since there are different devices and communication requirements are involved, it is essential to have many customized protocols to realize the proposed framework.

PROPOSED QKDP

In our previous paper we implemented a protocol that helps secure communities in e- governance applications. In this paper a part of that protocol is reused in the framework we proposed for cloud. The proposed protocol is named QKDP. QKDP is the underlying protocol in the framework proposed in Figure 1.

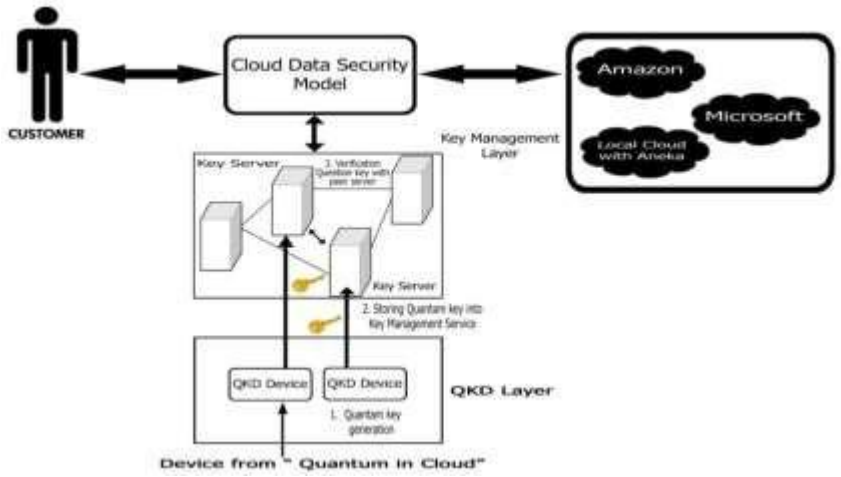


Figure 1.3 – Proposed framework for QKDP implementation

As can be seen in Figure 1.3, it is evident that the proposed framework has different layers. They are QKD layer, key management layer, cloud data security layer and cloud layer. The cloud layer is responsible to provide cloud services. The cloud data security layer is responsible to take care of encryption and decryption procedures using quantum and traditional cryptography. The traditional cryptography is for securing data while the quantum is to distribute keys in secure fashion.

The QKD layer is responsible to produce quantum keys. We used devices for real quantum key generation using "Quantum in Cloud" platform. The generated keys are maintained by key servers which are located in key management layer. The Quantum Cloud infrastructure is depicted in Figure 2. The cloud infrastructure includes application server and license server in which the application server is connected to various nodes. Quantum device QD is installed in application server where as the key generation and key distribution process is managed by the license server. The Quantum key distribution is taken place through the quantum channel in the form of Qubit's and the shared key is distributed through the classical channel across the clouds.

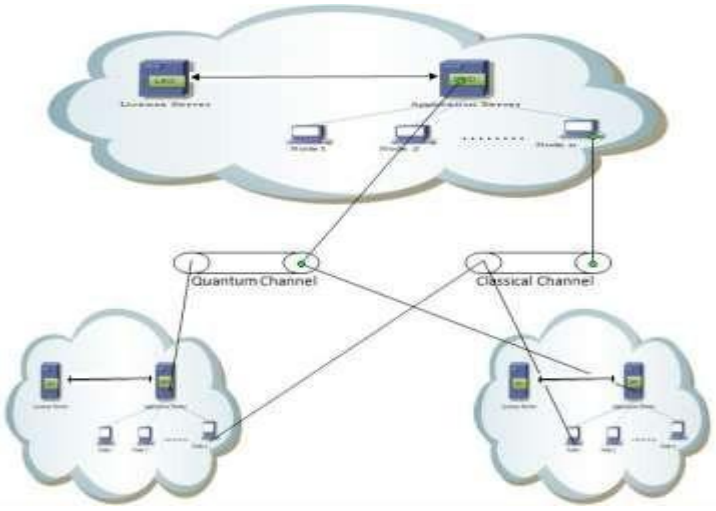


Figure 1.4: Quantum Cloud Infrastructure

The process is initiated at the cloud user end while sharing the document. Thedocument is encrypted using 3-DES schema and transmitted through IP-Multicast using QKDphenomenon. The key transmitted through the quantum channel where it is converted in to qubit and is transmitted based on various phases of polarization to the receivers end.

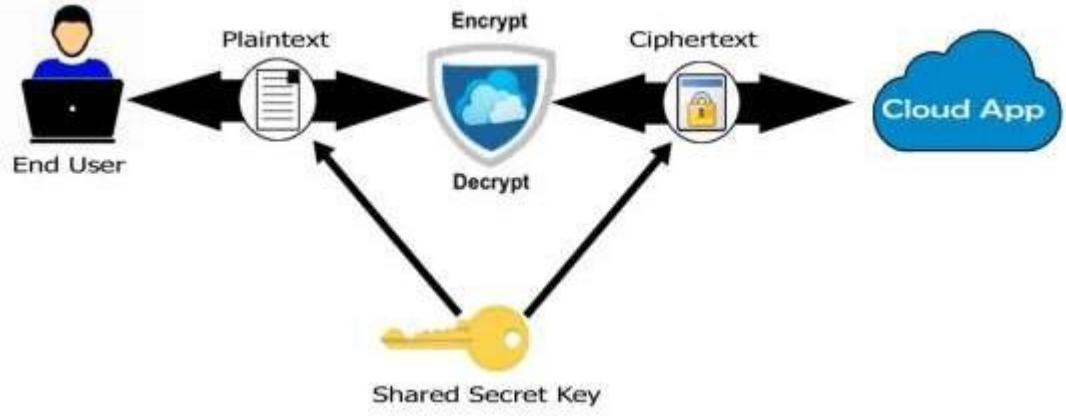


Figure 1.5 – Cloud data security model

This layer is in the proposed framework. It is elaborated here. It takes data from cloud user and encrypts it using Triple DES algorithm before sending it to cloud. In the same fashion, the data which comes from cloud is decrypted. However, in the proposed framework the key distribution is done using quantum channel for highly secure cloud communications. The process of communication within the Quantum channel is depicted in Figure 4.6.

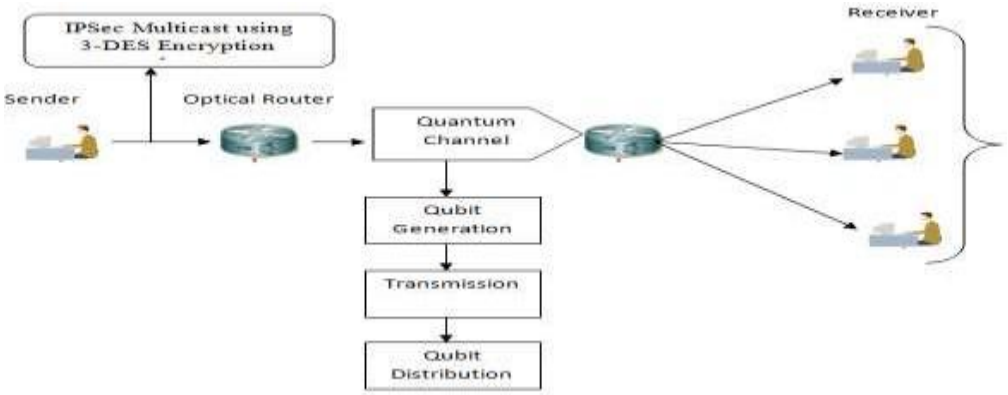


Figure 1.6: Quantum key distribution through quantum channel

The process of key distribution includes Qubit generation, Transmission of Qubit across the clouds and distributing it. The process of Qubit distribution is managed by Quantum key manager with the help of license server. Local host cache stores the generated qubits and they are transmitted across the cloud.

CONCLUSION

This paper presents a number of theoretical solutions aimed at facing the challenges of thenew cloud computation era. Addressing the problem of security and privacy in cloud environment two effective solutions were illustrated and it is observed through performance evaluation that the proposed solutions outperforms various security algorithms previously proposed for securing cloud. Firstly the work demonstrates a working model to authenticate the users in cloud using quantum cryptography and further for the experimental analysis the BB84 protocol is simulated using QKD simulator that establishes a secured quantum channel. In the second contribution a prototype is modeled to ensure the secured data exchange between various clients and centralized cloud server for this purpose we integrated 3DES and BB84 protocols that enable multilevel security based on the proposed key management framework. Further this could be extended to minimize the computation process of cyber physical systems.

REFERENCES

[1]. Jian Wang, Quan Zhang, Chao-jing Tang. (2006). Quantum key distribution protocolsusing entangled state. *IEEE*. p1355-1358
[2]. T. Hwang and K.-C. Lee. (2007). EPR quantum key distribution protocols with potential 100% qubit efficiency. *IEEE*. 1 (1), p43-45.
[3]. Shirantha Wijesekera, Dr. Sajal Palit and Dr. Bala Balachandran . (2007). Software Development for B92 Quantum Key Distribution Communication Protocol. *IEEE*. p1-5.
[4]. Fábio A. Mendonça, Daniel B. de Brito, João B. R. Silva, George A. P. Thé, and Rubens V. Ramos. (2007). Experimental Implementation of B92 Quantum Key Distribution Protocol. *IEEE*. p712-717.
[5]. Q. Wang1,2W. Chen2G. Xavier1M. Swillo1, S. Sauge1, M. Tengner1, T. Zhang2, Z. F. Han2G.
[6]. C. Guo2, A. Karlsson1. (2008). Robust decoy-state quantum key distribution with heralded single photon source. *ieee*, 1-2.
[7]. Dazu Huang and Zhigang Chen. (2008). Quantum Key Distribution Based on Multi- qubit Hadamard Matrices. *IEEE*. p333-337.
[8]. Mohamed ElboukhariMostafa Azizi, Abdelmalek Azizi and. (2010). Quantum Key Distribution In Practice: The State Of Art. *IEEE*.p1-4.
[9]. Ivan Capraro and Tommoso Occhipitni. (2007). Implementation Of A Real TimeHigh Level Protocol Software For Quantum Key Distribution. *IEEE*. p704-707.
[10]. Nabeel A. Siddiqui. (2007). QUANTUM-GRID INFINITESIMAL BIT CRYPTOSYSTEM. *ieee*, 1-4.
[11]. Mario Pivk,Christian Kollmitzer. (2009). SSL/TLS with Quantum Cryptography. *ieee*. 0 (0), 1-6.
[12]. Qing Xu, Manuel Sabban, Philippe Gallion and Francisco Mendieta. (2008). Quantum Key Distribution System using Dual-threshold Homodyne Detection. *IEEE*. p1-8. , 1-4.