A NOVEL QUANTUM KEY DISTRIBUTION BASED
CIPHERTEXT POLICY ATTRIBUTE-BASED ENCRYPTION
MODEL FOR CLOUD SECURITY

B.N.V.MADHU BABU¹ AND Dr.K.RAJASEKHARA RAO²
¹Research Scholar, Department of Computer Science and Engineering, Rayalaseema University, Kurnool, Andhra Pradesh, India
²Director, Usha Rama College of Engineering and Technology, Telaprolu, Andhra Pradesh, India

Abstract- With the exponential growth of network bandwidth, computational resources and the popularity of internet, cloud security has become one of the interesting research area of cloud computing. Cloud computing services are used widely in different applications such as medical, defence, education, health etc, for data storage and elastic computing. Traditional attribute based encryption models are to small and medium size applications with limited attribute set. Also, users’ data access control mechanisms must satisfy the process of protecting data from unauthorized users as well as from third party providers. To overcome these issues, an improve geometric quantum based CP-ABE is designed and developed on small client server data applications. This proposed model has three phases; geometric key generation, client data encryption and data decryption at receiver end. Experimental results proved that the proposed model has high computation speed, storage overhead and secured key distribution compared to traditional ABE models.

Keywords- Attribute Based Encryption, Ciphertext policy based ABE, Cloud security.

I. INTRODUCTION

Cloud computing allows users to store their data remotely in cloud servers and these cloud servers are responsible for providing services according to their demand. With the exponential growth of cloud services, data servers are needed to be trusted as well as safe enough in order to store much confidential sensitive information. Numbers of cryptographic techniques have been proposed in the past few years to achieve data security in cloud. But with the rapid growth of technology, now-a-days data are stored in distributed cloud servers. Distributed cloud servers are data servers responsible for storing data in different servers which is by default exposed to other data owners. Additionally, the data owners cant control the hardware platforms directly. A basic encryption scheme is applied to encrypt the sensitive data and then store them in different cloud servers. If the cloud servers are compromised in any case, the confidential data will remains unsafe. This encrypted data can be easily shared throughout the network and some access control policies are implanted in order to add additional security to the cloud. In case of scalable access control, symmetric encryption or public key encryption are not feasible as compared to other cryptographic schemes. Hence, it is essential to implement a secure encryption system along with fine-grained access control mechanism for corporate data sharing among different cloud servers. Therefore, a new approach is developed by integrating both of the above mechanism which is termed as Attribute-based encryption scheme. Attribute-based encryption scheme can be defined as a public key based encryption technique which involves both the concepts of access control mechanism and encryption[1][2].

The cloud computing storage is implemented according to the users’ demand. The users are able to access their stored data from cloud server at any time. In recent era, vast amount of data are...
stored in cloud computing storage irrespective of their origin and nature. The security and privacy of those data has become our prime concern. In order to resolve this issue of privacy and security, many cryptographic algorithms are developed. Cloud security can be defined as the process of encrypting a message to an encoded form and decrypting it by the authorized users[3]. By implementing a secure and advanced cryptographic algorithm, extended security can be added to the sensitive data present in cloud servers. Unfortunately, the outsourced data are not within the controlling range of data owners. These data can be only controlled by cloud service providers. As all users have different access rights, fine-grained access control can be implemented on users of cloud storage systems. Many cryptographic approaches are developed in order to encrypt the confidential data efficiently. Again, the decryption keys are distributed among all authorized users and allow them to take part in the process of decryption. Cloud servers as well as the unauthorized users are not allowed to decrypt the outsourced data. The conventional public key encryption approach can be categorized under a coarse-grained encryption technique. Apart from symmetric cryptographic encryption approaches, public-key techniques share its public key without compromising in data confidentiality and data integrity. These public-key approaches are developed in order to transmit data securely from sender to the appropriate receiver. It is also responsible for storing confidential data and numbers of different applications. With advancement of cloud technology, the requirement of computing data in cloud also increases. All the conventional public-key cryptography algorithms do not support the evaluation of cipher text data in cloud[4].

In the year 2005, Sahai and Waters presented a new technique in order to add more security in cloud data. They termed their developed approach as attribute based encryption(ABE) technique. There are three major entities such as data authority, dataowner (or sender) and data user (or receiver). The authorities have the responsibilities to produce keys for data owners and users to execute encryption and decryption process successfully. The decryption process is carried out by accepting the encrypted data and the private keys generated by authority as input values. If the attributes of user’s private key matches with the attributes of encrypted data, the process of decryption is executed successfully. When the number of matching is same as the threshold value, the user’s private key will be allowed to decrypt the encrypted data. Let us consider an example containing set of disruptive attributes in encrypted data {MIS, Teacher, Student}. Let us assume that, the threshold value is 2. When the owner wishes to decrypt encoded data, the numbers of attributes in the private key must contain two or more attributes. Therefore, the data user must contain private key along with attributes, {MIS, Student} to execute the decryption algorithm and provide the original message for the above access control mechanism[5][6].

Traditional ABE approaches are developed for privacy preservation of cloud data on different cloud servers. An extended attribute based encryption technique includes a searching strategy for encrypted data. Hence, it is implemented in privacy preservation applications in the fields like finance, biomedicine and military database. Achieving the same level of security and performance along with other conventional techniques are more costly in terms of computational cost, storage cost and communication overheads. The major disadvantage of attribute based encryption technique is that, the user’s attributes are static in nature. In order to add a new attribute or modify an existing attribute, the user needs a new private key. As the data and computation are outsourced to a remote server, data integrity is required to be maintained and checked constantly in order to enhance the computation process. Data integrity can be defined as a property by which data are kept safe from unauthorized modifications and a slight change to data is noticed. Computation integrity involves the program execution as expected and data are kept unchanged from malware, an insider or a malicious user[7]. Data integrity must be verified at the data level and computation level.

The prime objective of the cloud based ABE model is to enhance the expressiveness of access policies through applying dynamic location attributes. In order to support the location attributes of cloud computing, multiple users are required to access these attributes and implement client-server architecture.
The main features of an appropriate cloud based attribute based encryption technique are described below:–

**Data confidentiality**

The user’s data should be in an encrypted form before uploading it on the cloud. Hence, the unauthorized users won’t be able to access the cloud data.

**Fine-grained access control**

The system is responsible for granting different access privileges to all users in order to access cloud data. The users included in a common group may or may not have equivalent access privileges.

**Scalability**

On increasing the numbers of authorized users, the system operates effectively. Hence, the numbers of authorized users can’t influence the overall performance of the system.

**User accountability**

There exist chances when an authorized user shares his attribute private key with other users who are not authorized. In such cases, it may create an issue of illegal key sharing in between unauthorized and invalid users.

**User revocation**

When an user quits the system, the algorithm takes back the access privileges provided to that user previously. The process of removing access privileges is known as user revocation. A user which is revoked is unable to store data, as its access privileges are revoked.

**Cloud Security Goals:** There are five major objectives of any cloud based cryptographic approach. Every security system must contain group of security functions which can assure the secrecy of the system. These functions are generally considered as security objective or security goals. The objectives are classified into five different sub-categories such as:-

1. **Authentication:** Authentication can be defined as the process of validating a person’s unique identity. In other words, both the sender and receiver are required to verify their identity before the communication takes place.
2. **Privacy/Confidentiality:** It makes sure that, the confidential information is only available to the authenticated receiver. It is also responsible for detecting a secure system. Only the authenticated users are allowed to access the confidential sensitive data.
3. **Integrity:** It ensures the receiver that, the received message is not changed and it is the same as original. The generalized form of integrity is message check sum at client and server side.
4. **Non-repudiation:** It makes sure that the sent message is transmitted by that particular sender only. Both the sender and receiver can’t falsely deny sending messages.
5. **Service Reliability and Availability:** As secure systems are vulnerable to different attacks, which may influence the availability and cloud service to the users.

Cloud computing environment in mostly insecure, as it is used worldwide. All the data are needed to be encrypted prior to uploading it on cloud. Several classical public key encryption approaches can be implemented to enhance security, but it also gives rise to some issues which are mentioned below:-

1. For the encryption process to be executed, data owners requires user’s public key.
2. The storage overhead is increased, as for a single plain text there exist many public keys.

Quantum key distribution (QKD) involves the shared secret key generation between two parties via secured quantum channel. QKD is widely used in various security algorithms for data confidentiality. QKD is derived from quantum physics for key generation and it is perfect solution, whenever it is used in different applications. Security proofs by their nature are logical, conceptual and mathematical indispensable for security correctness. Quantum key distribution to traditional standard cryptographic models is quite hard to implement and it is difficult to evaluate the possible
attacks. The main advantage of integrating quantum key distribution to ABE scheme is, it provides additional security to cloud data.

The typical quantum key distribution system is shown in figure 1. Only authorized parities of quantum key distribution are connected to each other through the quantum medium compared to classical channel. During the quantum key distribution process, A and B shared their quantum signals via the quantum channel and message exchange through the secured classical channel[8][9].

In this paper, we have proposed a novel quantum key distribution based ABE model on cloud computing. Therefore, the proposed CP-ABE approach will be able to give perfect solution to access control system through the process of consideration, distribution, access control and confidentiality.

II. RELATED WORKS

In the process of Public Key Encryption, two different keys are used for encryption and decryption process. Among two of these keys, one key is public and the other one is private. The public key is distributed publicly and the private key is only available to the receiver. All messages are encrypted with receiver’s public key and the process of decryption is carried out by the private key. This approach gives rise to very large key management overheads; hence it is not efficient enough for cloud environment. Cipher text-Policy Attribute-Based Encryption [7] technique resolves the below mentioned issues:- This approach detects a user along with its set of attributes instead of his identity. If the user’s attributes satisfy the corresponding access policies, then only the user will be eligible for the process of decryption. The CP-ABE scheme is better than that of public-key cryptography, because of its minimum overhead in the process of key management. When a particular private key of a user is compromised, then only data files of that specific user may be decrypted by considering attributes of the user. CP-ABE provides an enhanced version of security as compared to Symmetric Key Encryption techniques.

DES (Data Encryption Standard) DES algorithm is proposed in 1970s and it involves the basic concept of the Fiestel Structure. DES is a special type of symmetric and block cipher algorithm. As the symmetric key cryptography involves a common key, hence it is more vulnerable to attacks. If the key is compromised, then whole data stored in cloud is also compromised. In order to overcome the above disadvantages of symmetric key cryptography, public key cryptography is developed. It uses two keys:- one is a public key and another is private key. The public key is used in the process of encryption and it is made publicly available across the network. But, the private key is only used to complete the decryption process. Only the intended receiver must have its private key. In case the private key is being compromised, then only data related to that specific user are compromised and the rest of the data on cloud are safe. The public key cryptography is also known as asymmetric cryptography. The asymmetric cryptography is more secure than that of symmetric cryptography. But, asymmetric cryptography results relatively higher overheads and this makes the algorithm infeasible in terms of cost. Similarly, DES algorithm needs same key for both the process of encryption and decryption and hence categorized under the subcategory of symmetric key cryptography. Both the sender and receiver must be aware of the private key. The key length is 64 bits, where 8 bits are taken for parity check. It includes total 16 rounds of permutation process for the process of encryption. Literally, decryption can be considered as the exact opposite process of encryption [2]. Brute-force attack is a most commonly occurring attack in DES algorithm. Besides
this, there are also three other vital attacks of DES algorithm like: - a) Differential Cryptanalysis b) Linear Cryptanalysis c) Davies Attack.

Blowfish is also a symmetric block cipher algorithm that can be implemented for encryption. It accepts a variable-sized key, from 32 bits to 448 bits as input for the process of encryption. Blowfish algorithm is developed in the year 1993 by Bruce Schneier as a fast, free alternative to the previously developed encryption schemes. Blowfish is a variable-sized key block cipher. It is often implemented in such applications where key is not changed frequently. It is much faster as compared to most of the encryption approaches when applied on 32-bit microprocessors having relatively large data caches. [4]

Homomorphic encryption can be defined as the processing encrypted data on remote storage without decrypting it. It is considered as a vital approach in cloud. Homomorphic encryption checks the data confidentiality in order to resolve the security issue of storage or processing data by an untrusted third party. Cloud users are capable of using cloud services at any time and at any place via internet. Therefore, it fully utilizes the availability nature of cloud. Hardening and redundancy can be considered as two distinct approaches in order to enhance the availability of cloud system.

Secret Key (Symmetric) Cryptography (SKC): This type of cryptography takes same key for both encryption and decryption process. It is also known as secret cryptography (SKC). The overall process of encryption works as follows:- • The plaintext is encrypted by the process of encryption with help of key. Then, the produced cipher text is transmitted to the receiver who needs the same key in order to execute the decryption algorithm. Both the sender and receiver are aware of the key value. Stream cipher and block cipher are two widely implemented symmetric key algorithms

Identity Based Encryption (IBE):
IBE can be categorized under a public key encryption technique. Here, the public key contains some information related to key holder such as email address. The key authority provides a secret key which is merged with the public key. The data owner of the public key are allowed to decrypt the encrypted data with the help of this secret key.

Role Based Access Control (RBAC):
In this technique, access is granted to each and every role instead of individuals. If any individual is assigned with a role, then automatically all access privileges related to that role are inherited [39].

Attribute Based Access Control (ABAC):
It is a comparatively extended model to RBAC. Attribute Based Encryption is an encryption technique which is responsible for implementing fine-grained access control mechanism along with encryption technique. In this case, users with some attributes are able to read the data or parts of the data which the attributes grant access to [5]. The above method is compared with some other versions of ABE and detected a complex access control mechanism and decryption process.

The attribute based encryption technique involves the following entities like authority, sender and receiver. The senders’ keys take part both in the process of encryption as well as decryption. The data authority permits access of data users. There are total two key attributes, those are:- public key and master key attributes . The authority is responsible for controlling and managing both attributes. The conventional attribute based encryption approach is modified and two other techniques are proposed such as, Cipher-text Policy Attribute Based Encryption (CP-ABE) and the Key Policy Attribute Based Encryption (KP-ABE) . CP-ABE and KP-ABE are two extended approaches of conventional ABE.

Policy Attribute Based Encryption
It is an extended version of classical Attribute Based Encryption technique. Here, the access structures are associated with secret keys of users and the encrypted data are tagged with attributes. When the access structure of key is produced, the user can get access to the concluding set of attributes [10].

The main objective of CP-ABE is to manage the outsourced data sharing, but it also gives rise to two major disadvantages. At first, the data owner is required to completely trust attributes
authority. In the subsequent phase, the attribute revocation problem may lead to some additional problems related to granularities of revocation, poor scalability and high computational complexity. There exist a most common issue in this technique i.e., users’ public keys are required for the process of encryption by ABE algorithm. ABE can’t be implemented successfully in real world scenarios due to the access control rights of monotonic attributes.

**Traditional QKD using cryptographic models**

The main goal of quantum key distribution is to generate a key K, which is used to transmit bits from source A to destination B via quantum signals without a shared key value. The quantum key distribution process is shown in Figure 2. In this figure, BB84 protocol is used as key distribution using cryptographic model for secured data storage.

![Figure 2 QKD on Cryptography model](image-url)
Ardehali et al. [11] implemented an efficient quantum key distribution and enhancement to BB84 protocol which significantly minimizes error photons, therefore improving the protocol bit rate. Di Jin et al. [12] developed a fast convergent key distribution model using a dual quantum channel to reduce raw key error rate and to improve key efficiency during communication. Chong et al. [13] proposed a novel quantum key distribution based on BB84 protocol. This protocol enables the source to destination in a way that a trusted party cannot determine the shared secret key for mutual communication. Sarath et al. [14] proposed a novel quantum key distribution scheme to reduce the bit rate and to ensure secure key distribution.

III. PROPOSED MODEL

A cloud service provider can be self-interested, un-trusted and more vulnerable with respect to clients’ sensitive confidential information. Data security and data privacy has become the major concern for both cloud service providers as well as customers. Hence, most of the time customers do not want to transfer their confidential information to the cloud due to privacy and integrity problems. In order to enhance the data security and privacy, the users’ data are encrypted by quantum key distribution based CPABE before uploading them on cloud.

In this proposed model, a traditional KP-ABE model is integrated with basic quantum theory for secure data transmission. In the proposed model, geometric shaped quantum is used to secure the small cloud datasets from client user to the shared receiver user. Here, traditional KP-ABE scheme is used to communicate the cloud data with the receiver. In the proposed model, geometric polarization is used to generate the secret key using four angles from 0 to 180 angles. GQK-CPABE can be stated as a special type of traditional ABE which is responsible for encryption and decryption according to the attribute values. In this approach, both the secret key and cipher text depends on input attributes. The cipher text is decrypted by decryption algorithm, when attributes of user keys matches attributes of cipher text. If the number of matching is equivalent with the minimum threshold d, the decryption algorithm is executed successfully. This proposed scheme of CPABE involves an important feature which is known as collusion resistance. The users having multiple keys are allowed to access all sensitive information, when at least a single key satisfies access constraints. The associated access structure enables the encrypted data to select the appropriate key which is required to retrieve data. It can be stated that, user’s key associated with attributes are responsible to satisfy the access structure of encrypted data. The overall idea of this technique is almost similar to the classical ABE approach.
Geometric Quantum Key Distribution for KP-ABE Key Setup:
In this proposed approach, geometric shaped key generation procedure is designed and implemented on small cloud datasets. Here quantum key generation is used to find the shared key between the communication parties. In this model, geometric shaped structure is used to generate the key with four angular shapes such as 45, 90, 135, 180 degrees.

- **Step 1:** Client side user selects the random permutation element from the group which is a relative prime to selected element.
- **Step 2:** Client generates quantum basis and geometric shaped polarization for selecting the symbols during the security parameter transmission.
- **Step 3:** Client side user sends his generated basis key to the communication receiver through the insecure channel.
- **Step 4:** Receiver computes his basis and geometric polarization using the permutation group elements.
- **Step 5:** Receiver computes his polarization using the client polarization.
- **Step 6:** Receiver generate shared key and communicates to the client side user.
- **Step 7:** Client and receiver use the same shared key for secured data transmission with limited text data.

The GQKD based CP-ABE scheme also involves four basic algorithms like KeyGen, Decrypt, Setup, and Encrypt which are described below:-

**A. Setup Scheme:** It generates the master key (MK), QKD shared key and public key parameters (PK). The public key and master key can be generated as

$$\text{PublicKey}(Pk) = \{\text{MD5(GQKD(Sharedkey)), } \alpha = g^\alpha, \beta = g^\beta \}$$
MasterKey = \{g_2, e(g_1, g_2)^k\}

B. Encrypt Scheme: The encryption algorithm takes the original plain text message (M) as input and generates the desired cipher text. The encryption technique encrypts the message M using the access tree structure T. Let L be the set of leaf nodes in access tree structure, then the cipher text is generated based on the given access tree structure T as:

\[
\text{CipherText}(C) = \{r_1 = e(g_1, g_2)^k, T, r_2 = m^r\}
\]

\[
\text{forall } x \in X: C_x = k, r_2 = H(A)
\]

C. KeyGen Scheme: The KeyGen algorithm generates private key (PrK) using the attributes' set (A). The KeyGen algorithm takes set of attributes A, QKD(sharedkey) as input and generate secret key as output. This algorithm selects a random number r and rand_j for each attribute A_j and these random numbers are selected as the factor of QKD(sharedkey) and holds in Z_p.

\[
\text{SecretKey}(Sk) = \{ D(j) = k^{\text{rand} \cdot H(j) \cdot \text{rand}_j}\}
\]

D. Decrypt Scheme: It accepts private key (Sk, attributes’ set (A)), cipher-text (C, embedded with the access structure (T)) and public key (PK) as input. Decryption process is executed recursively. A recursive procedure is executed with three parameters cipher text, secret key, attributes set A and the node x from access tree T.

IV. EXPERIMENTAL RESULTS

All the experiments are executed on the real time Amazon AWS cloud storage with client configurations as Intel(R) CPU 2.13GHz, 4-GB RAM. This framework requires third party libraries Amazon Java SDK, Jama, Apache commons and Apache Math.

Table 1: Comparative analysis of encryption, decryption and computational time on proposed and existing models using geometric quantum key for 10KB data.

| Algorithms    | EncryptionTime (ms) | DecryptionTime (ms) | CommunicationTime (ms) |
|---------------|---------------------|---------------------|------------------------|
| ABE           | 8936                | 8453                | 4765                   |
| KP-ABE        | 7586                | 6976                | 4176                   |
| CP-ABE        | 7532                | 6834                | 3756                   |
| GQKD+CPABE    | 5893                | 6097                | 2943                   |
Table 1 illustrates the performance analysis of proposed model to the existing models in terms of encryption time, decryption time and communication time. From the table, it is observed that proposed model has low computational time compared to traditional models.

Figure 2: Performance analysis of key generation for the proposed model to the existing models on avg 10KB datasize

| Attributes | ABE   | KP-ABE | CPABE | GQKD+CPAB |
|------------|-------|--------|-------|-----------|
| 5          | 4528.87 | 4315.97 | 3787.97 | 4478.98 |
| 10         | 4476.87 | 3897.98 | 3684.65 | 3291.87 |
| 15         | 4284.76 | 3897.67 | 3546.75 | 3006.75 |
| 20         | 4386.86 | 3953.97 | 3764.97 | 3397.86 |
| 25         | 4495.97 | 3748.65 | 3674.46 | 3254.64 |

Figure 2 illustrates the runtime to generate QKD, private keys with different attribute sizes. The speedup is up to about 0.87 times approximately than the existing key distribution models.

V. CONCLUSION

This paper presents a novel quantum key distribution based CPABE with enhanced key generation and distribution procedures. Attribute based encryption models have exposed significantly essential requirement for cloud data security due to high computational accuracy. Existing CPABE models are analyzed experimentally to find its performance issues. Major issues such as key generation, encryption and decryption with network computation are enhanced using quantum based CPABE model. To overcome these issues, a novel quantum key distribution (QKD) based cipher text policy ABE model was implemented in cloud environment.

REFERENCES

[1] L. Ibraimi, Q. Tang, P. Hartel and W. Jonker, "Efficient and provable secure ciphertext-policy attribute-based encryption schemes", Proc. 5th Int. Conf. Inf. Secur. Pract. Exper., vol. 5451, pp. 1-12.

[2] J. Li, X. Huang, J. Li, X. Chen and Y. Xiang, "Securely outsourcing attribute-based encryption with checkability", IEEE Trans. on Parallel and Distributed Systems, vol. 25, no. 8, pp. 2201-2210, 2014
[3] J. Han, W. Susilo, Y. Mu, J. Zhou and M. Au, "Improving privacy and security in decentralized ciphertext-policy attribute-based encryption", IEEE Trans. on Info. Forensics and Security, vol. 10, no. 3, pp. 665-678, 2015.

[4] Junbeom Hur,"Improving Security and Efficiency in Attribute-Based Data Sharing",IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, VOL. 25, NO. 10, OCTOBER 2013.

[5] Zhiguo Wan, Jun'e Liu,"HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing",IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 7, NO. 2, APRIL 2012.

[6] J Bethencourt, A Sahai, and B Waters. Ciphertext-policy attribute-based encryption. In Symposium on Security and Privacy, SP "07, pages 321–334. IEEE, 2007.

[7] Mat’ e Horv ´ ath. Attribute-based encryption optimized for cloud computing. In 41st International Conference on Current Trends in Theory and Practice of Computer Science, SOFSEM "15, pages 566–577. Springer, 2015.

[8] Tang, Xiao (2006, April 18). Code for unbreakable quantum encryption generated at record speed over fiber. Paper presented at the SPIE Defense & Security Symposium in Orlando.

[9] FL Williams, Timothy J BSc (2006). Experimental advances in broadband continuous variable quantum key distribution. Unpublished bachelor dissertation. The Australian National University.

[10] S. Hohenberger and B. Waters, “Online/offline attribute-based encryption,” in Public-Key Cryptography - PKC 2014 - 17th International Conference on Practice and Theory in Public-Key Cryptography, Buenos Aires, Argentina, March 26-28, 2014. Proceedings, 2014, pp. 293–310.

[11] Ardehali, Mohammed, Chau. H.F., and Lo. H.K. (1998),"Efficient quantum key distribution.” arXiv preprint quant-ph/9803007.

[12]Chong, S.K. and Hwang, T., 2010. Quantum key agreementprotocol based on BB84. Optics Communications, 283(6),pp.1192-1195.

[13]Jin, D., Verma, P.K. and Kartalopoulos, S.V. (2008) ,”Fastconvergent key distribution algorithms using a dual quantumchannel", Security and Communication Networks.

[14] Sarath, R and Nargunam, S. (2016) ,“An efficientimplementation of BB84 quantum key distribution protocol”,Journal of Chemical and Pharmaceutical Sciences, vol. 9, no.1.