Scientific Journal of Impact Factor (SJIF): 4.72

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 4, Issue 7, July -2017

AN ENHANCED ATTRIBUTE BASED ENCRYPTION MODEL USING QUANTUM KEY DISTRIBUTION FOR INFORMATION SECURITY IN CLOUD ENVIRONMENT

B.N.V.MADHU BABU[1] AND Dr.K.RAJASEKHARA RAO[2]

[1]Research Scholar,Department of Computer Science and Engineering ,
Rayalaseema University, Kurnool,Andhra Pradesh, India ,
[2]Director, Usha Rama College of Engineering and Technology, Telaprolu, Andhra Pradesh, India

ABSTRACT:-*Cloud computing has a great demand because of advantages of deploying required computing capacity as needed at lower cost than working an owned computing infrastructure Cloud Computing is a flexible, cost-effective, providing business or consumer IT services over the Internet. but, cloud computing faces many risk because here services are offered by a third party, who may not be trusted sometimes in terms of security, Attribute based encryption (ABE)is a public key encryption algorithm which enables users to secure their data in the public cloud servers. Traditional ABE models are standalone applications with limited resource constraints, inefficient key generation and low processing speed. To solve these issues, An enhanced KP-ABE model using Quantum principal for key distribution to secure data in cloud environment.Here keys are generated and distributed using the concept of quantum principle by transmission of photons .these keys are used in attribute based encryption for encryption of data*

Keywords:, *key policy based ABE, Quantum principal for key distribution .cloud security*

1. INTRODUCTION

Cloud computing removes the investment of buying hardware and software and makes their concentration to improving function of the organisation, instead of managing the infrastructure. It provides Software as a Service (SaaS) which offers access to a complete software application which the cloud user accesses through a web browser or other software. Accessing the software in this manner eliminates or reduces the need to install software on the client machine and allows the service to support a wider range of devices. The software may in turn be hosted on a cloud platform or infrastructure It provides Platform as a Service (PaaS) which provides platform that allows cloud users to write applications and run within that platform, .The platform may in turn be hosted on a cloud IaaS.It provides Infrastructure as a Service (IaaS)- An IaaS cloud offers access to the raw computing resources of a cloud service. Rather than purchasing hardware itself, the cloud customer purchases access to the cloud provider's hardware according to the capacity required.

As Security concerns with cloud computing. The provider must assure that their infrastructure is secure and their clients' data and applications are protected.. Cloud security can be defined as the process of encrypting a message to an encoded form and decrypting it by the authorized users. By implementing a secure and advanced cryptographic algorithm, extended security can be added to the sensitive data present in cloud servers. but, 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.

Attribute-based encryption is a type of public-key encryption[1][2] in which the secret key of a user and the ciphertext are dependent upon attributes (e.g. the country in which he lives, or the kind of subscription he has).here, the decryption of a ciphertext is possible only if the set of attributes of the user key matches the attributes of the ciphertext. the security aspect of Attribute-Based Encryption is collusion-resistance: The concept of **attribute-based encryption** was first proposed by Amit Sahai and Brent Waters [2] and later by Vipul Goyal, Omkant Pandey, Amit Sahai and Brent Waters.[3] Recently, several researchers have further proposed Attribute-based encryption with multiple authorities who jointly generate users' private keys.

Ciphertext-policy ABE (CP-ABE)

In the CP-ABE, the design of public key will be more complex, thus security of the system is proved to be more difficult. The research work of CP-ABE is focused on the design of access structure.

Key-policy ABE (KP-ABE)

In KP-ABE, the owner of the data creates a master key. Using this master key, the owner encrypts the data in such a way that a ciphertext is labeled with a set of attributes. The private key given to others to decrypt the data is designed with a tree-based access structure which specifies which ciphertext the key can decrypt. The tree based access structure consists of leafs which are associated with attributes. Then a user is can decrypt a cipher text if the attributes associated with the ciphertext satisfies the user's key access structure . The KP-ABE system have an attractive solution to the audit log problem. Audit log entries could be annotated with attributes such as, for instance, the name of the user, the date and time of the user action, and the type of data modified or accessed by the user action. 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[3], 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[4]. based cryptographic approach. the security systems must contain number of of security functions which can assure the secrecy of the system. These functions can be 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.

The main objective of KP-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 chanels. The quantum key distribution process is shown in Figure below. In this figure, BB84 protocol is used as key distribution using cryptographic model for secured data storage.

QKD on Cryptography model

Ardehali .Implemented an efficient quantum key distribution and enhancement to BB84 protocol which significantly minimizes error photons, therefore improving the protocol bit rate. Di Jin 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 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] proposed a novel quantum key distribution scheme to reduce the bit rate and to ensure secure key distribution. Quantum key distribution (QKD) uses quantum mechanics to guarantee secure communication. It enables two parties to produce a shared random secret key known only to them, which can then be used to encrypt and decrypt messages. It is often incorrectly called quantum cryptography, as it is the most well-known example of the group of quantum cryptographic tasks.

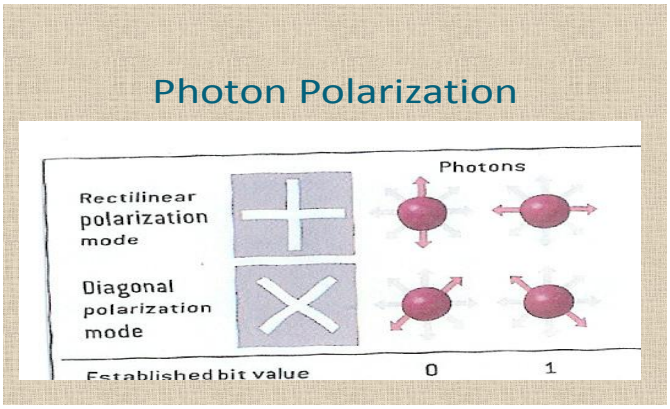
An important and unique property of quantum key distribution is the ability of the two communicating users to detect the presence of any third party trying to gain knowledge of the key. This results from a fundamental aspect of quantum mechanics: the process of measuring a quantum system in general disturbs the system. A third party trying to eavesdrop on the key must in some way measure it, thus introducing detectable anomalies. By using quantum superpositions or quantum entanglement and transmitting information in quantum states, a communication system can be implemented that detects eavesdropping. If the level of eavesdropping is below a certain threshold, a key can be produced that is guaranteed to be secure (i.e. the eavesdropper has no information about it), otherwise no secure key is possible and communication is aborted.

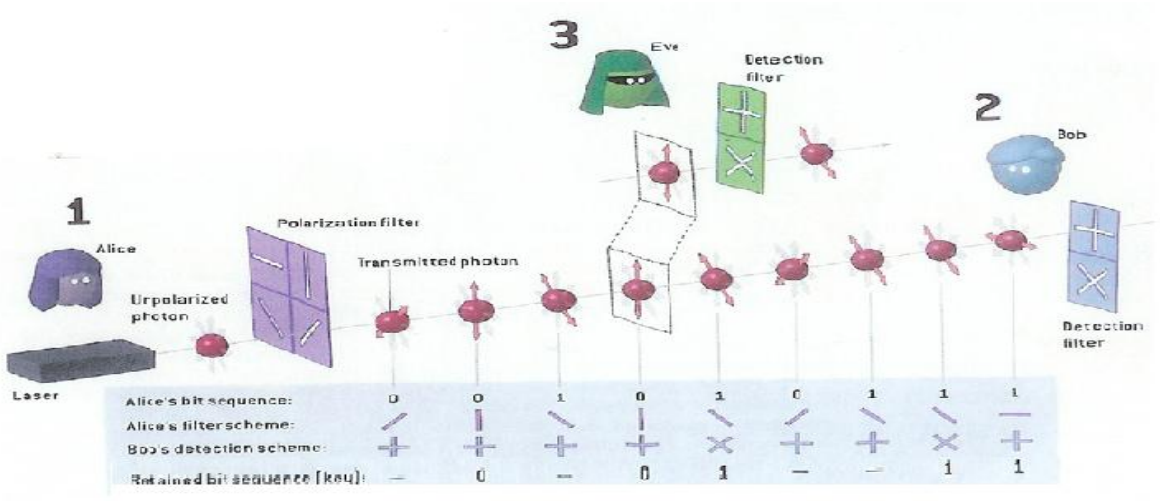
The security of encryption that uses quantum key distribution relies on the foundations of quantum mechanics, in contrast to traditional public key cryptography, which relies on the computational difficulty of certain mathematical functions, and cannot provide any indication of eavesdropping at any point in the communication process, or any mathematical proof as to the actual complexity of reversing the one-way functions used. QKD has provable security based on information theory, and forward secrecy.

Quantum key distribution is only used to produce and distribute a key, not to transmit any message data. This key can then be used with any chosen encryption algorithm to encrypt (and decrypt) a message, which can then be transmitted over a standard communication channel. The algorithm most commonly associated with QKD is the one-time pad, as it is provably secure when used with a secret, random key.[1] In real-world situations

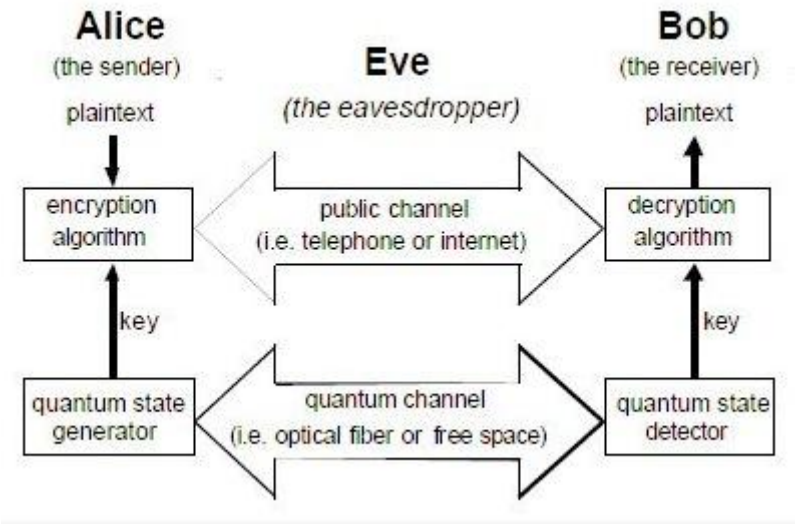
Quantum cryptography uses photons to transmit a key. Once the key is transmitted, coding and encoding using the normal secret-key method can take place. But how does a photon become a key? How do you attach information to a photon's spin?

This is where binary code comes into play. Each type of a photon's spin represents one piece of information — usually a 1 or a 0, for binary code. This code uses strings of 1s and 0s to create a coherent message. For example, 11100100110 could correspond with h-e-l-l-o. So a binary code can be assigned to each photon — for example, a photon that has a vertical spin (|) can be assigned a 1. Alice can send her photons through randomly chosen filters and record the polarization of each photon. She will then know what photon polarizations Bob should receive.





When Alice sends photons to Bob using an photon gun, she'll randomly polarize them either the X or the + filters, so that each polarized photon has one of four possible states: (|), (–), (/) or (\ ) . After Bob receives the photons, he decides whether to measure each qubit with either his + or X filter — he cannot use both filters at a time. Bob has no idea of what filter to use for each photon to retrieve the bit, so he uses any one filter to retrive for each qubit. After the entire transmission, Bob and Alice have a discussion about the transmission through another channel



PROPOSED MODEL

An enhanced key policy-attribute-based encryption[11] model using Quantum key distribution for data security in cloud environment . In order to enhance the data security and privacy, the users' data are encrypted by quantum key distribution[12] based KPABE before uploading them on cloud. Our proposed model has three phases; QKD based key generation, data encryption and data decryption. In the first phase, key setup and shared key are generated using the QKD. In the second phase, user's encrypted data are uploaded to the cloud storage using KPABE and shared key. Similarly, each user decrypts the encoded data from the cloud storage using the decoding process with QKD based KPABE as shown in figure . In the decoding process, user's encoded data from the cloud is decrypted using the proposed QKD based KPABE decryption model. In this case, the data owner has restricted amount of control on data, whereas the cloud service provider gains full control over it. Hence, the data owners also demand full access and control over their data all the time.

QKD-KPABE 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 KPABE 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.

Cloud Server:
Amazon Elastic Compute Cloud (Amazon EC2) provides variable-sized computation capacity in the cloud. EC2 provides simple and easy web-scale computation for developers. A user-friendly interface is available for configuration of hardware capacity needed to the finest detail, with a very little amount of effort. The above interface is responsible for inclusion and deletion of instances. EC2 instances are placed in Virtual Private Cloud (VPC) by permitting the customer to determine which instances should be disclosed to internet. In order to handle both inbound and outbound network access, security groups and network ACLs are implemented. To monitor and keeping track of these EC2 instances, Amazon introduces CloudWatch web service. CloudWatch is responsible for efficient resource utilization, demand patterns and operational performance. High performance computing (HPC) offered by Amazon handles customers having complex computational workloads. In case of Amazon EC2, users are permitted to choose an operating system, load it with a traditional application, setting network access rights, cloning that instance and including computing power.

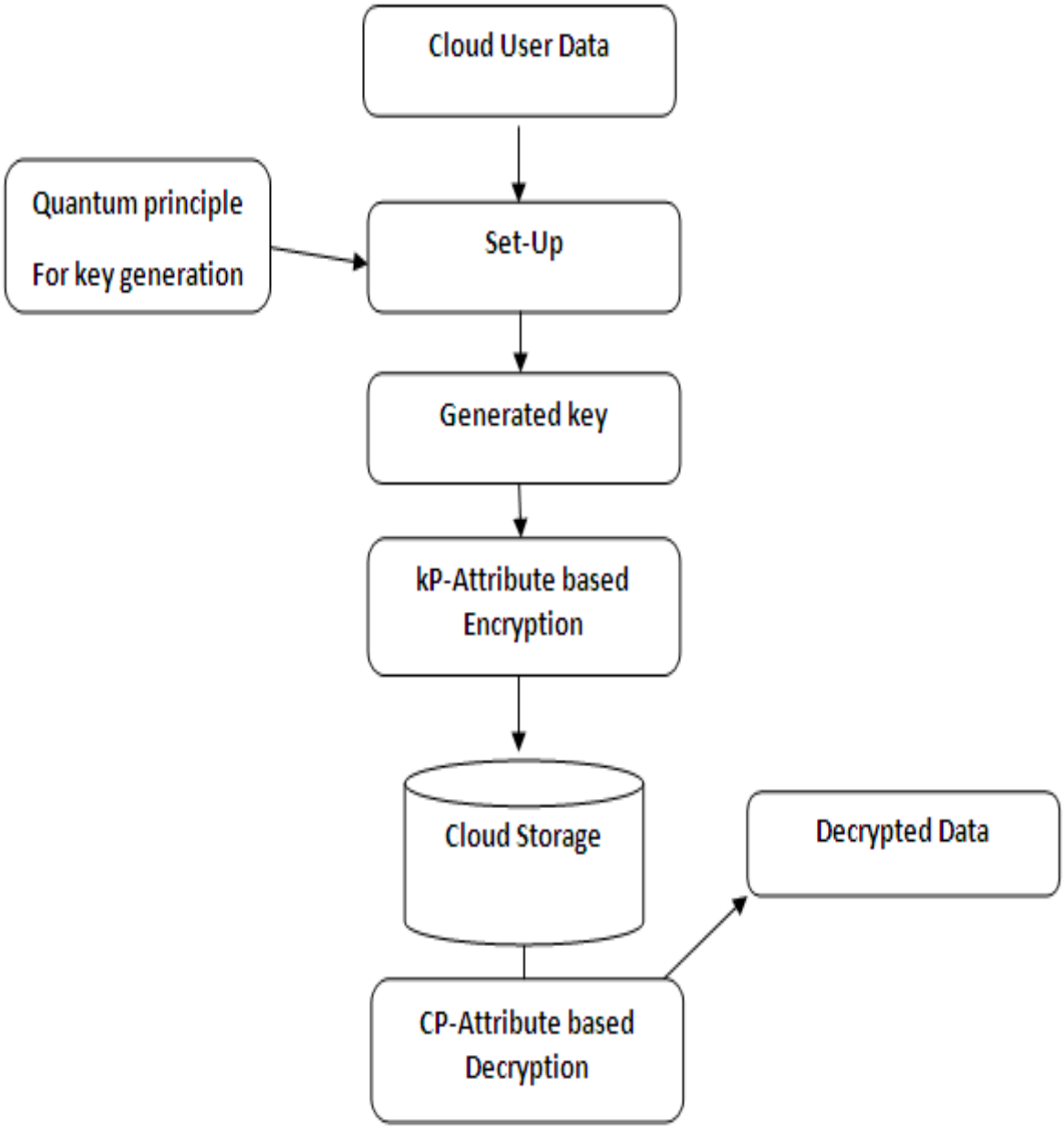


Figure 3: Proposed Model

Quantum Key Distribution for Key Setup and Generation:
quantum key distribution (QKD) requires communication channels such as quantum channel and a normal data channel. The sender and receiver both require random generators from the cyclic group and a set of basic and polarizing qubits. In this model, we have used BB84 authentication protocol to prevent the quantum channel being attacked during communication by the man-in-the-middle attacks. The basic steps used in the proposed QKD are shown in Figure 4.

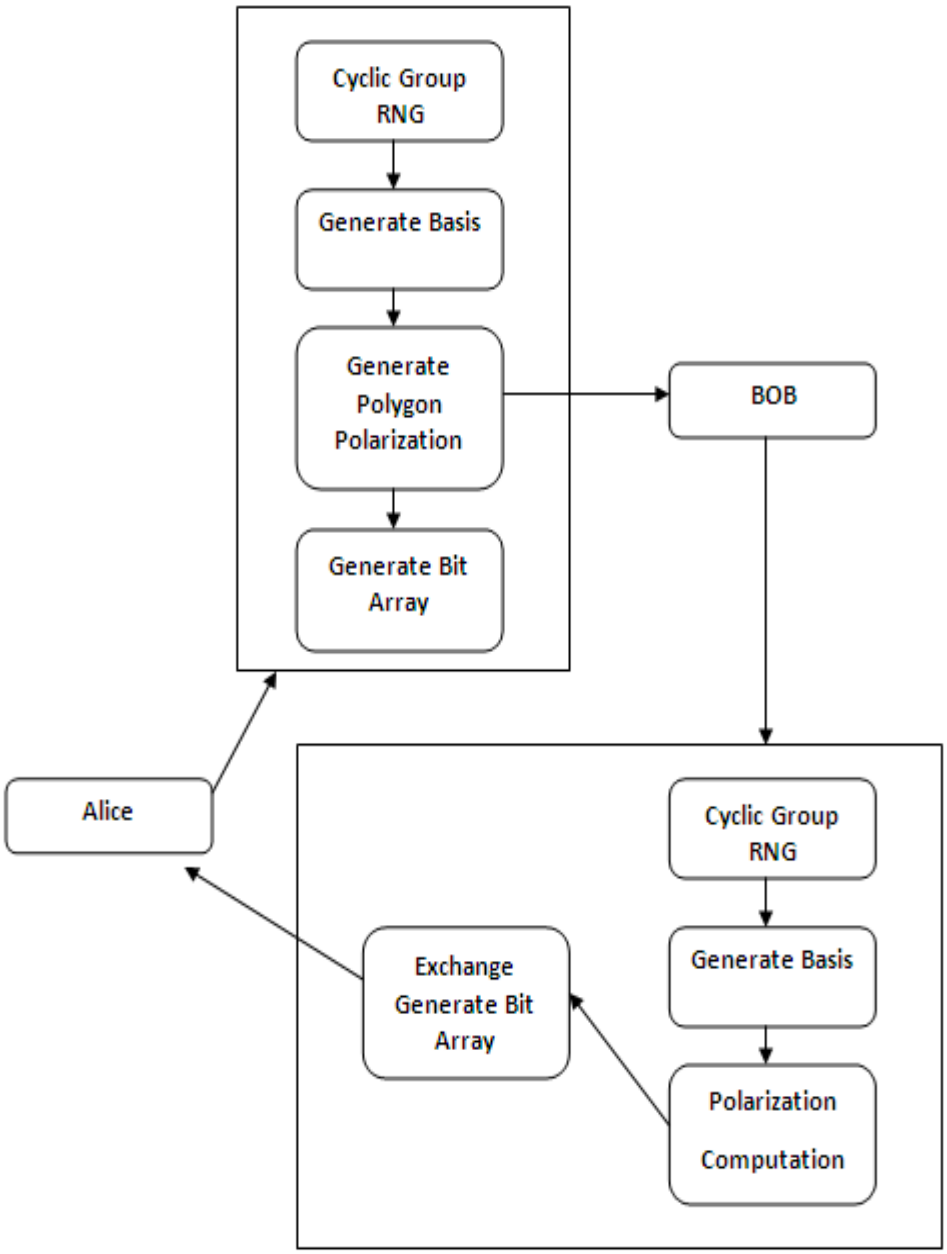


Figure 4: Proposed Polygon Polarization Based QKD

Step 1: Alice selects user specified dynamic bit vector using cyclic group generator.
Step 2: Alice generates random basis and selects the polarization states using figure 5 and 6.
Figure 5 shows the different polarization angles selected in each polygon shape edges.
For example: if the selection of polarization is case-1, then labelled A, B, C, D edge angles are selected as polygon polarization states
Figure 6 demonstrates the basis selection using the random selection of PP(case(i)).
Step 3: Alice send computed polarization to Bob.
Step 4: Bob generates random basis using the different cases of polygon polarization.
Step 5: Bob measures polarization using Alice polarization and Bob basis.
Step 6: Bob generate shared key and sends to Alice.
Step 7: Using shared key, both Alice and Bob communicate with each other through cloud server.

CONCLUSION

We are aiming to integrate a system with Quantum key distribution and Key policy-attribute based encryption that gives an efficient security for the data in cloud environment.

REFERENCES

- [1].International Journal of Private Cloud Computing Environment and Management "Identity based secure authentication scheme based on Quantum Key Distribution for cloud computing" by Geeta Sharma1 and Sheetal Kalra1 1 Department of Computer Science and Engineering, Guru Nanak Dev University.
- [2]. https://en.wikipedia.org/wiki/Quantum_key_distribution
- [3]. https://en.wikipedia.org/wiki/Key_(cryptography)
- [4]. https://simple.wikipedia.org/wiki/Key_generation
- [5]. https://en.wikipedia.org/wiki/Public-key_cryptography
- [6]. "A Survey on Attribute Based Encryption Scheme in Cloud Computing" by Minu George, Dr. C.SureshGnanadhas, Saranya.K published in International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 11, November 2013
- [7]." Multi-Authority Attribute Based Encryption" by Melissa Chase Computer Science Department Brown University Providence , RI 02912 mchase@cs.brown.edu.
- [8]. "Analysis and Security based on Attribute based Encryption for data Sharing" by Ms. Snehlata V. Gadget Dept. of Computer Engineering, University of Pune, Pune, India published in International Journal of Emerging Research in Management &Technology ISSN: 2278-9359 (Volume-3, Issue-3) March 2014
- [9]. **"**Threshold Cipher text Policy Attribute-Based Encryption with Constant Size Cipher texts" by Aijun Ge, Rui Zhang, Cheng Chen, Chuangui Ma, and Zhenfeng Zhang.
- [10]. "Privacy-Preserving Decentralized Cipher-Policy Attribute-Based Encryption" by Jiangsu Provincial Key Laboratory of E-Business, Nanjing University of Finance and Economics, Nanjing, Jiangsu 210003, China.
- [11]. https://pdfs.semanticscholar.org/5da9/eaa24ba749f1ae193800b6961a37b88da1de.pdf
- [12]. https://www.wired.com/insights/2014/09/quantum-key-distribution/
- [13]. cs.brown.edu/~mchase/papers/multiabe.pdf
- [14]. https://en.wikipedia.org/wiki/Universally_unique_identifier
- [15]. securitycerts.org/review/cryptography-confidentiality.htm
- [16].https://www.usenix.org/.../integrity-checking-cryptographic-file-systems-constant
- [17]. Searchsecurity.techtarget.com/definition/nonrepudiation
- [18].https://www.ibm.com/support/knowledgecenter/SSB23S_1.1.0.14/.../s7symm.html
- [19]. searchsecurity.techtarget.com › Encryption technology › Network security
- [20]. https://simple.wikipedia.org/wiki/Cryptographic_hash_function

