Impact Factor (SJIF): 3.632

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444

Volume 3, Issue 7, July-2016

Data Security in Cloud using Hybrid algorithm with Quantum Key Distribution

Priyanka S. Tuppad, P. S. Challagidad

Department of computer science and engineering, Basaveshwar engineering college, Bagalkot

Abstract --- Cloud computing is an Internet based technique where a huge amount of resources are shared like service. It is a Payment-based mold where the users can pay for what they use. Cloud computing is mounting gradually due to its ease of use and minimal management effort, many business organizations have coming forward to adopt cloud technology. At the same time cloud technology have lots of challenges, security is one among them which is considered to be a critical issue in cloud computing atmosphere due to which many organizations have fright in storing their data in the cloud. This may lead to the negative impacts on the adoption of cloud. To overcome this negative impact, the proposed work deals to provide data security in cloud computing using hybrid encryption algorithm with quantum key distribution.

Keywords: Cloud Computing, AES, RSA, Hybrid algorithm, Quantum Key, Google Cloud Platform.

I. INTRODUCTION

Cloud Computing (CC) is an Internet-based technique where common assets such as (software, storage, sensitive data and information) are provided to the customers on demand. CC is a computer paradigm that allows accessing of data and services from the datacenters of the cloud by any connected devices over the internet. Advantages of CC are Low computer costs, Improved performance, Low software costs, Easy software updates, Storage capacity, Data reliability, Universal data accessibility, Latest version availability, Supports group collaboration, Device independent. Because of these benefits each business holders and organizations wishes to store their data in the cloud. As cloud environment provides the services of storing and sharing of information and resources, it comes across threats and issues such as securing the data, integration of data and data breaches. In order to overcome these threats we need to encrypt the data or information that are stored in the cloud along with the security provided by the cloud owner.

The process of encrypting the data into non-readable form is known as cryptography [1]. This cryptography is classified into symmetric key algorithms and asymmetric key algorithms [8]. The symmetric key algorithm are said to be single-key encryption algorithms as it uses same key for encryption process and also for decryption process. Further this symmetric algorithms are partitioned into Block cipher symmetric algorithms and stream cipher symmetric algorithms. In block cipher category a block of data of fixed length is chosen for encrypting and decrypting processes. In stream cipher category single bit is encrypted and decrypted every time. The benefits of using symmetric key algorithms are it consumes less power, performs encryption and decryption fast. Algorithms such as: [DES] Data Encryption Standard, [AES] Advanced Encryption Standard, [3-DES] Triple DES lies under symmetric key algorithms. On other hand Asymmetric key algorithms are said to be dual key algorithms as it uses both private and public keys for encryption and decryption processes. Sender uses public key to encrypt the data during encryption process where as private key is used by receiver to decrypt the encrypted data. Algorithms such as [RSA] Ronald Rivest, Adi Shamir, Diffie-Helman algorithm for key exchange lies under asymmetric key algorithms. Hybrid encryption methodology contains the combination of symmetric and asymmetric encryption key algorithms. In this work, AES of symmetric key algorithms and RSA of asymmetric algorithms have been concatenated to encrypt and decrypt the data that are stored in the Google cloud. RSA asymmetric key algorithm is enhanced by adding quantum key distribution for generating encryption keys.

Quantum Key Distribution (QKD) [10], makes use of quantum mechanics in order to guarantee secure communication. It is used only to produce and distribute a key. It doesn’t involve the transmitting of any message data. Quantum key can be used with any encryption algorithm to encrypt and decrypt a message. QKD is simple to use. It requires fewer resources to maintain it. In this work, we are planning to implement the above mentioned hybrid encryption methodology in which the first said algorithm has drawback of inherent key exchange issue, encryption of large files is drawback of second algorithm. To overcome these draw back hybrid algorithm is used. Quantum key distribution is used to distribute the keys efficiently.

1.1 Types of clouds

Basically there are four types of clouds [6], they are:

- *Public cloud:* It is a type of the cloud, where in cloud services are made available to the users through an intermediate called as cloud service providers via an internet. The cloud itself controls and maintains the mechanisms of the services provided to the users. Generally these services are provided free during its free trial period and later it will be charged on the basis of pay as per use.

- *Private cloud:* This cloud provides many of the public cloud benefits, but only difference is the information is stored and maintained only within the organization.
- *Community cloud:* It is also a one kind of cloud where the information is maintained and administered by multiple organizations that have same goal. The authorization of access to the data that is resided in cloud is shared among members of organizations.
- *Hybrid cloud:* It is the combination of both public and private cloud. It is also known as systems of multiple clouds. These systems are interconnected in such a way that it allows users to move data and programs easily from one system to another system.

1.2 Cloud Service Models

- *Software as a Service:* This is a overhaul model which provide accessing ability to the user's and allow them to use an application and services that are hosted in the cloud.
- *Platform as a Service:* In this service model, users deploy their applications and software in the cloud by purchasing the access to the platforms that are hosted as a service in the cloud. Hardware equipments and communication channels are not managed by the users. Cloud platform has certain constraints within which users should implement their applications.
- *Infrastructure as a Service:* The characteristics of this service are to providing, controlling and managing hardware equipments and systems such as OS, software applications, storage device and internet connections. By using the facilities of this service, user can save his money by taking the hardware devices and other cloud services on rent on the bases of pay as per use instead of purchasing.

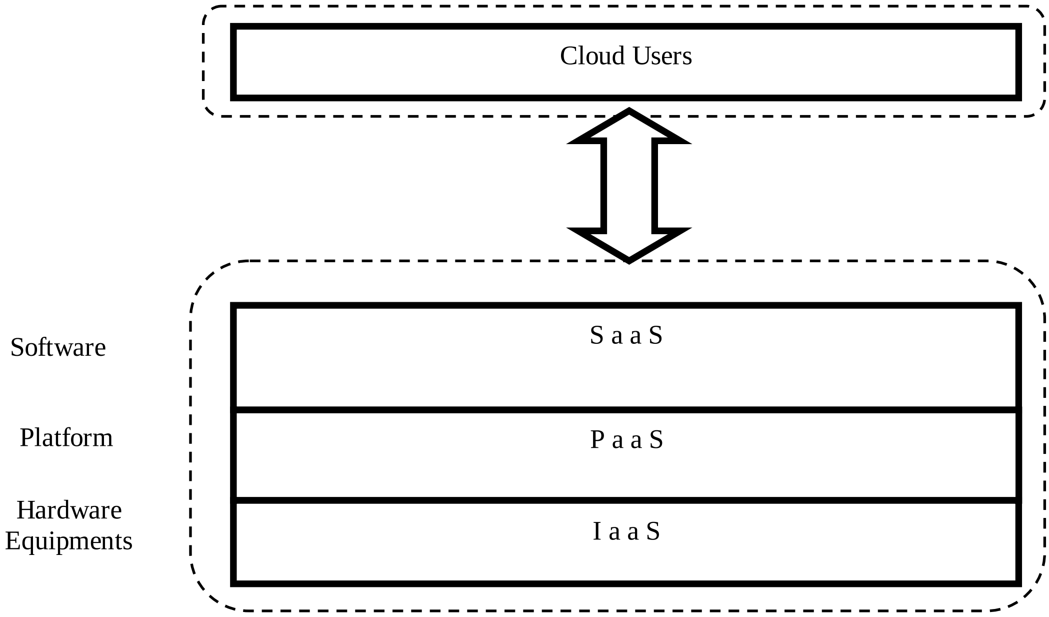

Figure 1.2 Cloud Service Models

II. LITERATURE SURVEY

Sufficient amount of research work has been done in order to determine security threats and issues with respect to the data stored in the cloud. During survey we came across various issues such as:

- *Data Integrity:* The data will be available on cloud so that anyone can access those data from anywhere in the world via the Internet. Cloud is unable to differentiate the stored data as sensitive data and as common data, due to this any user can access the sensitive data and this may lead to the lack of data integrity in cloud computing.
- *Data Theft:* As cloud services are cost effective and flexible to operate, the cloud vendors take server on lease from the cloud service providers. The customer will be unaware of all these internal things and there is a possibility that the data can be stolen from the malicious users.
- *Privacy Issues:* As vendors uses the server provided by the service provider, the vendor should assure regarding who is accessing the data and about the maintenance of the server. The vendors must guarantee that the customer's confidential information is secured from the attackers.
- *Infected Application/Data:* It is the duty of the vendor to keep on monitoring the cloud, thus preventing the unauthorized users from uploading the malicious injection or infected application on to the cloud which will lead to the corruption of the customer data.

- *Data Loss:* Data loss is considered to be very major problem in cloud computing. All of sudden if the vendor stops providing the cloud services due to legal or financial problems then the customers will face the problem known as data loss. As the vendor shut down his services, the customer's will be unable to access the data stored onto the cloud.
- *Data Location:* The customer's will be unaware of the location of his own data that are stored in the cloud. The vendors and cloud service providers never reveal the location of the stored data to the customer's. The cloud that contains the data might be situated in other country or anywhere else in the world.

III. PROBLEM DEFENITION AND PROPOSED METHODOLOGY

Cloud computing is an internet based technology where a huge amount of resources are shared as a service. Since the cloud computing is growing day by day because of its ease of use and minimal management effort, many business organizations have coming forward to adopt cloud technology. This technology have lot of challenges, security is the one among them which is a critical issue in cloud computing environment. So to guard against such data leakage an algorithm is needed. The proposed work plans to implement hybrid encryption algorithm with quantum key distribution in order to provide the security to the data in the cloud computing environment.

After literature survey the problem definition is concluded as **"Data Security in Cloud using Hybrid encryption Algorithm with Quantum Key Distribution".** The main aim of this project is to design and implement hybrid encryption algorithm that will differ from the existing algorithms.

3.1 PROPOSED METHOD

The security is critical issues in cloud computing because the third party auditor or the cloud owner or the malicious users may go for modifying the data stored in cloud datacenter. So security algorithms are needed to prevent this. Many security algorithms have been developed by the researchers but still scope exists to develop and design efficient algorithm to verify integrity of the user's data. The proposed work plans to implement hybrid encryption algorithm along with quantum key distribution concept in order to provide data integrity in the cloud computing environment.

➢ **Architecture of The Proposed Model**

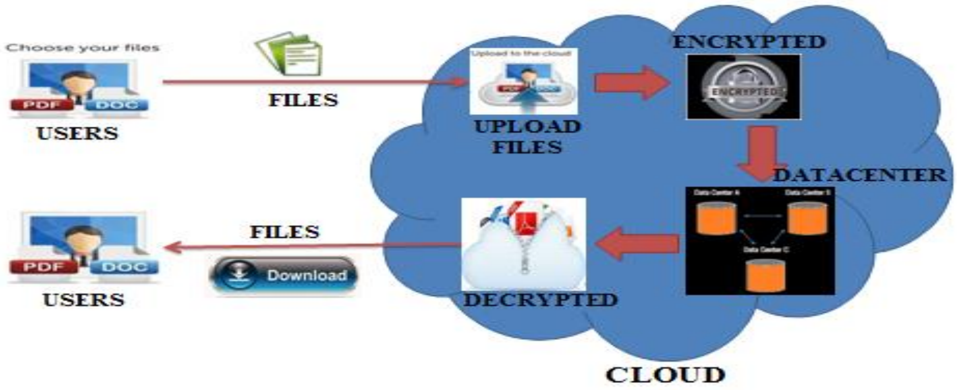

Figure 3.1 Architecture of Proposed Model

➢ **Steps:**

1. Files are uploaded onto the cloud by the users.
2. Those uploaded files are encrypted using AES & RSA with quantum key distribution algorithms.
3. Further encrypted files are stored in datacenters of the cloud.
4. At last, files will be decrypted and then downloaded by the users as per their requests.

➢ **AES (Advanced Encryption Standard algorithm) ([2],[7]):** Lies beneath the symmetric algorithm, wherever as RSA algorithm that lies beneath the asymmetric algorithm. AES could be a block cipher with a size of block length 128 bits. It permits for totally 3 different key lengths they are:128, 192, or 256 bits. Encryption consists of 10 rounds of processing for 128-bit keys,12 rounds for 192-bit keys, and 14 rounds for 256-bit keys. Apart of last round in every case, all other rounds are same. It also has the notion of a word and this word consists of 4 bytes, which is of 32 bits. Every phase of process works on the provided input array and generates an output array. Thus formed output state array by the previous round is rearranged into a 128-bit output cipher block.

- **Advantages of AES:**
- Implementation of AES is quicker and easier in both hardware and software system.
- It supports large size data encryption. It permits larger key size.

- **RSA (Ronald Rivest, Adi Shamir):** It is one among the foremost common public key encryption method. In this it make uses of public key and private key. Sender uses public key during encryption process. Whereas receiver uses private key during decryption process. In the proposed work, these public and private keys are generated and exchanged among sender and receiver by using quantum key distribution methodology [2].

- **Advantages of RSA with quantum key distribution**
- It allows high speed encryption, as it make use of quantum channel for generating and exchange of private keys and network communication channel for transferring data.
- Private keys are unaware to the end users.

The purpose of choosing hybrid algorithm is to overcome the inherent key exchange drawback of AES algorithm and the weakness of RSA algorithm i.e. unable to encrypt the larger files.

Table 3.1 Comparison between AES, DES and RSA [9]

Factors	**AES**	**DES**	**RSA**
Designed by	Vincent Rijmen, Joan Daemen , 2001	IBM, 1975	Ron Rivest, Adi Shamir, and Leonard Adleman, 1978
Key Length	128,192,256 bits	56 bits	>1024 bits
Cipher Block Size	Size of 128 bits	Size of 64 bits	Min 512 bits
Scalable	No	Yes	No
Algorithm Type	Symmetric Key	Symmetric Key	Asymmetric Key
Encryption Time	Fast	Medium	Slow
Decryption Time	Fast	Medium	Slow
Power Utilization	Less	Less	Very High
Security efficiency	Highly Secured	Secured Moderately	Least Secure
Key Usage for Encrypt & Decrypt	Uses Same Key	Uses Same Key	Different Key
Number of Rounds	10|12|14 Rounds	16 Rounds	Single Round
Simulating Speed	Fast	Fast	Fast
Hardware & Software	Fast	Better implementation of Hardware than Software	Less Efficient

IV. OUR CONTRIBUTION

Security plays a vital role in cloud computing environment. Though the cloud service provider provides at most security to the stored data, there may be chances of loss of data, attacks on data by malicious attackers, hackers or by third party auditors etc. In order to overcome these kinds of attacks and threats, our proposed work implements hybrid encryption algorithms. This method encrypts the uploaded and stored multimedia files. Hybrid encryption method includes the combination of Symmetric key encryption algorithm and asymmetric key encryption algorithm. By doing so the unauthorized users or hackers may not extract the data or information that are stored on the Google cloud.

The purpose of choosing hybrid encryption algorithm is to overcome the drawbacks of each other algorithms. AES algorithm that lies beneath the symmetric key encryption algorithms has the drawback of inherent key exchange issue as same key is used for both encryption and decryption processes. Because the key will be appended to the message itself. On the other hand RSA algorithm that lies beneath the asymmetric key encryption algorithms has the drawback that it can't encrypts the larger files.

QKD [10], quantum key distribution methodology is implemented in collaboration with RSA asymmetric encryption algorithm for generating both private and public keys. This methodology make use of separate channel known as quantum channel in which private and public keys are generated and exchanged between Alice and BOB i.e. between the sender and the receiver. Quantum channel is made up of optical fiber cable, hence it is not so easy for an attackers to extract the private and public keys from quantum communication channel. In normal RSA encryption algorithm generated private and public keys are exchanged between sender and receiver. In case of QKD the state generated using random bits and random basis is exchanged between sender and receiver. At both end secret keys are generated using those states and keys will be verified at each end. If keys matches then channel is safe message will be exchanged and then message will be transferred. Overview of QKD is as shown below.

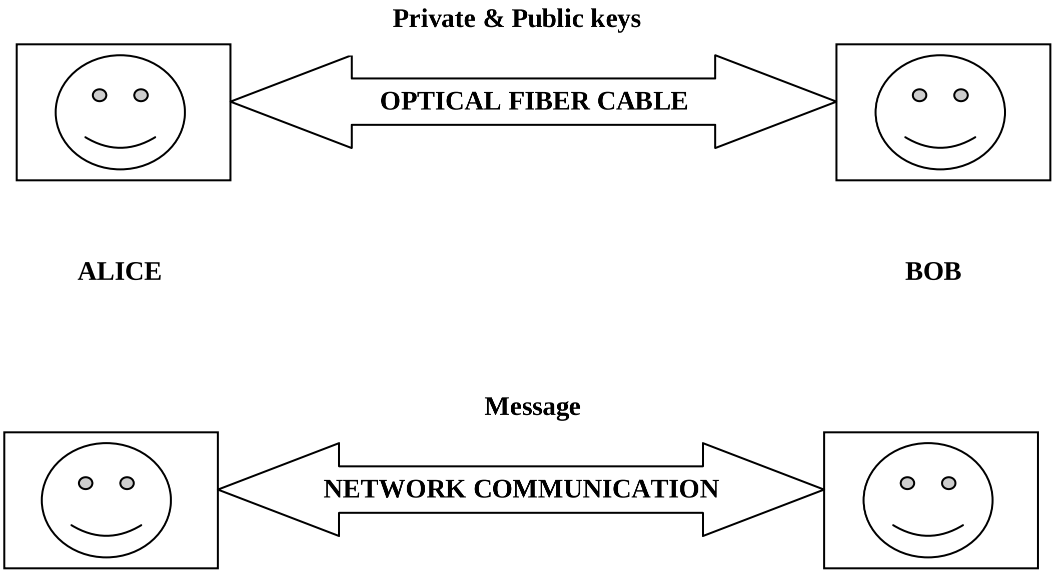

Figure 4.1 Quantum Key Channel, Network Communication Channel

- **Keys are generated and exchanged as shown below:**

1. Random bits for ALICE.
2. Random basis for ALICE.
3. Photon state generated at ALICE end (sender) in the form of UA: Upper Arrow ↑, RA: Right Arrow →, SUA: Slant Upper Arrow ↗, SDA: Slant Down Arrow ↘ .
4. Generated state is sent to BOB end (receiver).
5. BOB also generates state in the form of above mentioned arrows and sends it to ALICE.
6. Secret key is generated at ALICE end.
7. Secret key will be sent to BOB.
8. If matches, channel is safe message will be exchanged.
9. Finally message or data will be transferred.

GOOGLE CLOUD STORAGE [GCS]: It is a simple, low cost, effective and efficient storage, which provides a services to the users to store their data, information, applications anywhere from the world using an internet connected devices such as laptop, mobiles, desktop etc. This platform is said to be a Google cloud platform where in it provides the cloud services to the users. Initially it provides the services on free trial basis for certain period of time. Later it charges for provided services on the basis of pay-as-per-use concept.

Google cloud offers three types of products known as Standard, DRA and Near line to its users. All three products use same API and thus provides easy and convenient accessing services to the users.

Table 4.1 Google Cloud Products

STANDARD	DRA	NEARLINE
1. It provides higher level of durability. 2. 24/7 availability. 3. Better performance.	1. Medium level of durability and performance. 2. Lower grade of availability. 3. Hence costs low.	1. It provides higher level of durability with respect to backup, archiving and disaster recovery. 2. Low cost.

➢ **Features of Cloud Storage**

- **Durability**
  The google cloud storage platform is designed such a way that it provides 99.999% of durability. Several copies of data are stored over multiple locations. Ensures data integrity by performing checksums automatically.

- **Scalability**
  GCS is almost scalable, it supports all sort of applications such as small and big organizations application. It also supports peta-byte system.

- **Availability**
  Both standard and nearline cloud storages provides higher level of availability. DRA storage provides medium level of availability. Wherever as standard storage gives 99.999% availability in its monthly offer packs.

- **Reliability**
  A GCS guarantee succeeds of users write.

➢ **Steps for Deploying App on Google Cloud**

Before getting started with deployment process, we need to download and install java SDK and Apache Maven compiler plug in. The purpose of downloading and installing Apache maven is to build communication between client system and Google cloud. Maven plugin allows the required java SDK libraries automatically downloaded to your project that is going to be deployed on Google cloud.

➢ **Deploying steps are as follows:**

1. For deploying our app on app engine, we need to register our project in order to create project ID for our project, which will provide URL for our app.
2. Open Google cloud platform console, click on projects page and select create a new project.
3. Copy the above generated project ID and paste it on URL bar like src/main/webapp/WEB-INF/appengine-web.xml. It also provides the facility of setting app version.
```
<?xml version="1.0" encoding="utf-8"?>
<appengine-web-app xmlns="http://appengine.google.com/ns/1.0">
<application>uplddnld-1263</application>
<version>1</version>
<threadsafe>true</threadsafe>
</appengine-web-app>
```
4. Created application will be uploaded to the app engine of Google cloud by invoking mvn appengine : update command.
5. Finally our app is deployed and ready to use at http://<YOUR_PROJECT_ID>.appspot.com

V. EXPERIMENTAL RESULTS

Table 5.1 Results of Multimedia File Encryption using AES Encryption Algorithm

Multimedia Files	File Upload ID	Size of Enc File in Cloud	Runtime M Cycles	Average Latency
File Name: i1.jpg File Size: 8465 bytes File Path: E:\testing files\i1.jpg	1466711321755	8.28 KB	406	693ms
File Name: V1.mp4 File Size: 1201295 bytes File Path: E:\testing files\V1.mp4	1466710240848	1.15 MB	2,078	1,791ms
File Name: simple.pdf File Size: 856976 bytes File Path: E:\testing files\simple.pdf	1466710470951	836.91 KB	752	17,573ms
File Name: BIO_DATA.docx File Size: 11373 bytes File Path: E:\testing files\ BIO_DATA.docx	1466711044454	11.11 KB	1,201	603ms

Table 5.2 Results of Multimedia File Encryption using RSA with QKD Enc Algorithm.

Multimedia Files	Description of Steps
File Name: N1.txt File Size: 14 bytes File Path: E:\testing files\ N1.txt File Upload ID: 1466713464523 Size of Encrypted File in Cloud: 42 B Runtime M Cycles: 123 Average Latency: 626ms	Random Bits for Alice: 010001 Random Basis for Alice: +xxxxx Generated State: RA-SUA-SDA-SDA-SDA-SUA Generated State Sent to BOB State Sent by BOB: UA-UA-RA-RA-SUA-SUA Secret Key generated at ALICE end: 100010 Random Basis for Secret Key at ALICE: xxxxxx Secret Key State at ALICE end: SUA-SDA-SDA-SDA-SUA-SDA Sending Secret Key State to BOB Channel is Safe Keys are Saved Keys are uploaded to Server Private Key: ˜ý×!]/w)<r_D=³ÄfE>?³a□ fèƒˆ`Ç-„‰Y‹bƒDy Kzï‘™ôà3@76å ^>ÄØ×³–8☐-âƒ¬Ýþ žpsû©ÊøÀŠ‘ B • ,ü□)è/Âá2pììÃwæq□ ³O§eœ$){d¤žù³,çO
File Name: N5.txt File Size: 32 bytes File Path: E:\testing files\ N5.txt File Upload ID: 1466799412564 Size of Encrypted File in Cloud: 128 B Runtime M Cycles: 284 Average Latency: 1,052ms	Random Bits for Alice: 100000 Random Basis for Alice: ++xxxx Generated State: UA-SDA-SDA-SDA-SDA-SDA Generated State Sent to BOB State Sent by BOB: UA-RA-UA-RA-RA-SUA Secret Key generated at ALICE end: 001001 Random Basis for Secret Key at ALICE: xxx+x+ Secret Key State at ALICE end: SDA-SDA-SUA-SDA-SDA-SUA Sending Secret Key State to BOB Channel is Safe Keys are Saved Keys are uploaded to Server Private Key: `jSêÍ,z“ ¯ZïçÂTEvïÆÒ>‡ñ‡è› ´ðÈ»ña× ´¡›¤Ý • ¶/ @Ùkù Ôã¨ =ÚÄ9HçYøÑ¼½ Þì³Y ÜìÂ =0; Ý¶Öt s¢\Ð Ý&I ×ä ´“å’#ê>"””yl+”9PQ” ´€V‘ÂµÈ€m«æ+‹—’”ï&›

CONCLUSION

Inside the area of cloud computing atmosphere, safety measures acts a chief role. Now a day's number of users of cloud computing services has been rapidly increased. So the service provider of cloud need to justify the quality of their services and security aspects in such a way that the cloud users must feel satisfied. They have their own set of protocols, billing methods, flexibility, availability and supplementary parameters. The major thought dealt during this proposal is to secure files by performing encryption and thus making files in non-readable form and intelligible to all users. Implementing hybrid encryption algorithms over data or files provides the profits of less memory consumption and computation time compared to that of remaining encryption algorithms. The proposed approach is sort of helpful, as a result of it permits the user to stay away from the unlawful person as he cannot be able to read or scan the user's encrypted files. The concept of quantum key distribution also helps in automatically generating public and private keys with respect to RSA encryption algorithm. Future work deals with the applicable of quantum key distribution methodology to AES encryption algorithm.

REFERENCES

[1] Shakeeba S. Khan and R. R. Tuteja, 2015, "Security in Cloud Computing using Cryptographic Algorithms", International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization) Vol. 3, Issue 1, January 2015.

[2] Kalyani Ganesh Kadam And Vaishali Khairnar, 2015, " Hybrid Rsa-Aes Encryption For Web Services", International Journal Of Technical Research And Applications E-ISSN: 2320-8163, Www.Ijtra.Com Special Issue 31, September, 2015.

[3] Muhammad Kazim and Shao Ying Zhu, 2015, " A survey on top security threats in cloud computing" International Journal of Advanced Computer Science and Applications,Vol. 6, No. 3, 2015.

[4] Deepak Panth, Dhananjay Mehta and Rituparna Shelgaonkar, 2014,"A Survey on Security Mechanisms of Leading Cloud Service Providers", International Journal of Computer Applications (0975 – 8887) Volume 98– No.1, Jul 2014.

[5] Prakash Kuppuswamy and Saeed Q. Y. Al-Khalidi, 2014, " Hybrid Encryption/Decryption Technique Using New Public Key and Symmetric Key Algorithm", *MIS Review* Vol. 19, No. 2, March (2014), pp. 1-13 DOI:10.6131/MISR. 2014.1902.01©Department of Management Information Systems, College of Commerce National Chengchi University & Airiti Press Inc, March 2014.

[6] Mandeep Kaur and Manish Mahajan, 2013, "Using encryption Algorithms to enhance the Data Security in Cloud Computing", International Journal of Communication and Computer Technologies Volume 01 – No.12, Issue: 03 January 2013.

[7] Abha Sachdev and Mohit Bhansali, 2013,"Enhancing Cloud Computing Security using AES Algorithm",International Journal of Computer Applications (0975 – 8887) Volume 67– No.9, April 2013.

[8] Rashmi Nigoti, Manoj Jhuria and Dr.Shailendra Singh, 2013,"A Survey of Cryptographic Algorithms for Cloud Computing", International Journal of Emerging Technologies in Computational and Applied Sciences (IJETCAS). 2013.

[9] B. Padmavathi, S. Ranjitha Kumari, 2013, "A Survey on Performance Analysis of DES, AES and RSA Algorithm along with LSB SubstitutionTechnique", International Journal of Science and Research (IJSR), India Online ISSN: 2319-7064, Volume 2,Issue 4, April 2013.

[10] N.Vivek Chetty, Bikumalla Abhijith, Goli Nihar, and P.M.Durai Raj Vincent, 2013, "Modified Novel Quantum Key Exchange using BB84 Algorithm", N.Vivek Chetty et.al / International Journal of Engineering and Technology(IJET), ISSN : 0975- 4024 Vol 5 No 3 Jun-Jul 2013.