A NOVEL ENCRYPTION STANDARD USING QUANTUM PRINCIPLES AND CLOUD

Miss. B. Vasantha kumari, Mr. N. Datta sai krishna, Mr. CH. Sai Phanideep, Dr. N. Srinivasu, Mr. B. Rajesh

Department of Computer Science And Engineering

Koneru Lakshmaiah Education Foundation, Vaddeswaram,Guntur,522501.

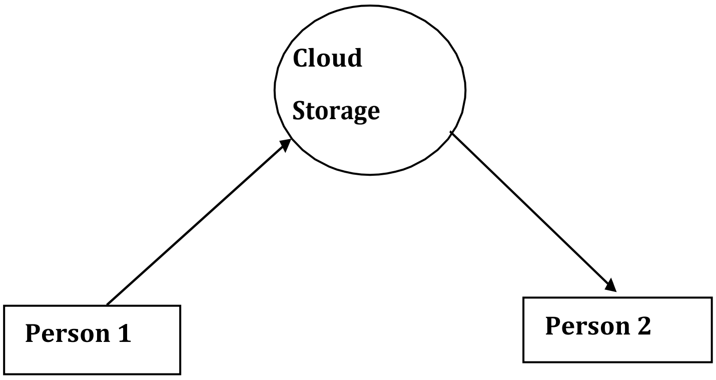
Email: borravasanthakumari0708@gmail.com , dattasai293@gmail.com, saiphanideep050199@gmail.com, srinivasu28@kluniversity.in, rajeshbingu@gmail.com,

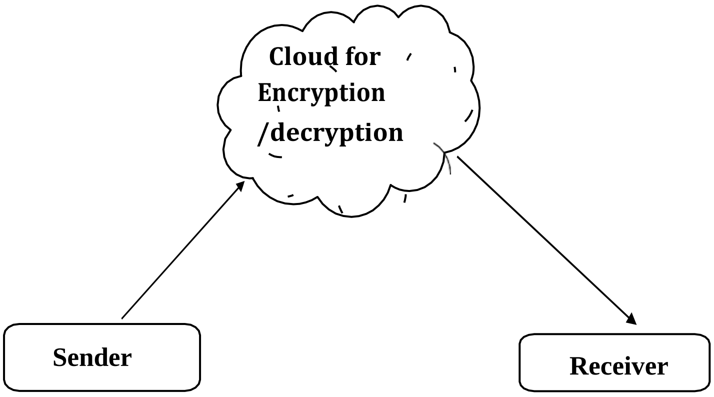
Abstract—**The project A NOVEL ENCRYPTION STANDARD USING QUANTUM PRINCIPLES AND CLOUD is mainly based on Quantum cryptography which is based on quantum mechanics property and as well as quantum key distribution. The key concept behind developing this project is to develop best security which can sustain many attacks by hackers and to provide the best encryption standard and can provide the toughest quantum digest that can't be read by anyone. Here in this concept we are using the Cloud to provide the service between two users or server to client or server to server etc. Here the cloud acts as the medium between communication and the cloud provides the services. The main use of this project is that no person can break the quantum security because it is very random in nature and secondly its digest is so small values which varies as floating values and thirdly we are using cloud as a middle party communicator so we can have full access of cloud to store large amount of data. Here in this concept we are using quantum principles to provide and to creation the encryption standard so that it gives a small value as the output of the digest and gives a very random output each and every time. The quantum key distribution offers solution for the key exchange methods. The quantum key acts as a confidential encryption standard. Here we are using the base of Qubits generation. Here in this project we are just using the base of quantum computing for creation of encryption standard.**

I. INTRODUCTION

The security now a days is being changing in day to day life. The Cybercrimes are also increasing in day to day life as it becomes a major crime in the world. Providing security had become a major problem in the current world. One of the concepts for providing security in a sophisticated way is Quantum cartography. But this process had not developed to the extreme for the public use. The concept developed by us uses Quantum principals to create a new encryption standard. The main methodology behind this concept is creating. A message digest or cipher text that can't be read that easily by the hackers and using large values which can provide additional security to this method. The whole set of encryptions is done in cloud so the cloud also acts as an interface between the users and provides additional security. This concept also provides an additional security to the Hash algorithms like Md5, Md4 etc.

The following diagram describes the basic architecture of the algorithm.

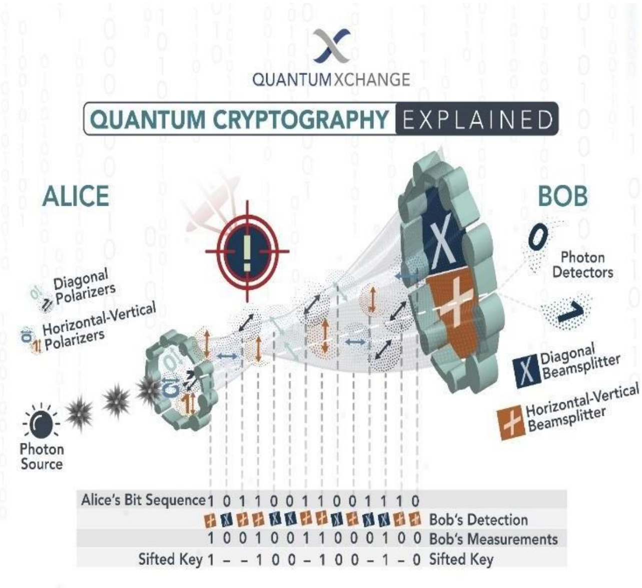




A. Quantum Cryptography

The science of exploiting quantum mechanical properties to perform tasks like crypto logical tasks. In quantum key distribution the simplest example of quantum cryptography is quantum key distribution which is main based on the key exchange which offers associate information theatrically secured resolution platform. The main advantage of the quantum cryptography lies within the incontrovertible fact that completes the cryptologic tasks that square measure proved or conjectured to be not possible. It is not possible to repeat or decode the knowledge that is encoded in the quantum states. If someone tries to attempt to browse the encoded knowledge then the state changes.

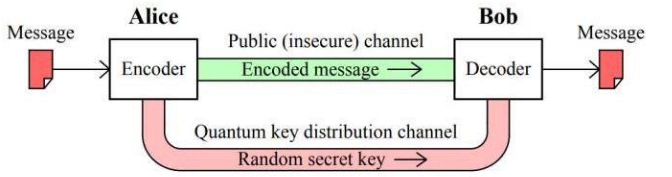
The basic architecture of Quantum cryptography is as follows


QUANTUMXCHANGE
QUANTUM CRYPTOGRAPHY EXPLAINED
ALICE
BOB
Photon Detectors
Diagonal Polarizers
Horizontal-Vertical Polarizers
Diagonal Beamsplitter
Horizontal-Vertical Beamsplitter
Photon Source
Alice's Bit Sequence 1 0 1 1 0 0 1 1 0 0 1 1 1 0
+ X + + X X + + X + X X + + Bob's Detection
1 0 0 1 0 0 1 1 0 0 0 1 0 0 Bob's Measurements
Sifted Key 1 – – 1 0 0 – 1 0 0 – 1 – 0 Sifted Key

B. Quantum key distribution

The best and the well-known developed application of the quantum cryptography is the quantum key distribution. Here in this quantum key distribution the key that is been shared between two people or two parties let us consider two people as Alice and Bob. In this mechanism the key is sent through a Photons in a safe channel of communication nothing but the quantum key distribution channel and the message digest or the message is been sent through the super and sub positions of the photons and by the Qubits which are more complex and flexible while transmission of the message if any person wanted to decode the encrypted message through these channels the super positions or the sub positions of the encrypted photons are changed and the authentication is received on both sides of the parties. The data of message digest is also changed because of the change happened to the photons and Qubits in the message communication system.

This architecture shows the communication between the parties in the key distribution system.



Here we can see separate channels for encoding message and for the random secret that is for the quantum key distribution channel.

C. Heisenberg uncertainty principle

This principle is proposed by Heisenberg in the year 1927 in this principle he states that the moment or velocity and the position of an object can't be determined exactly so this principle gives random values based on the position and moment of an object and provides randomness nature. Mathematical representation of the principle is as follows

$$\Delta x \times \Delta v\ x \geq h/4\pi m$$

Δx is the uncertainty in the position of the electron
$\Delta v\ x$ is the uncertainty in the momentum (velocity)
h = Planck's Constant
m = mass

in the same way If we know the position of an electron with high accuracy then its velocity will be uncertain. Similarly, if the velocity of an electron is known precisely then its position will be uncertain. The uncertainty rule is based on the defined paths and trajectories of the electrons.

Known formula of the Heisenberg uncertainty principle calculations

$$\Delta\ x \times \Delta v\ x = h/4\pi m$$

$$= (6.626\times10^{-34}\ \mathrm{JS})/(4\times3.1416\times10^{-6}\ \mathrm{kg})\approx10^{-28}\ \mathrm{m^2\ s^{-1}}$$

D. Wave functions

The fundamental constant mostly occurred in the quantum mechanics is the Planks constant which is given by Max Plank which is denoted by *h*. This common abbreviation ħ = $h/2\pi$, also known as the reduced Planck constant or Dirac constant.

The general form of wavefunction for a system of particles, each with position $\mathbf{r}_i$ and z-component of spin s_{zi}. Sums are over the discrete variable s_z, integrals over continuous positions $\mathbf{r}$.

For clarity and brevity, the coordinates are collected into tuples, the indices label the particles. Following are general mathematical results, used in calculations.

E. Planks constant

The planks constant comes under the mostly used quantum value proposed by Max Plank which is widely used in the wave functions. This constant describes the behavior of particles and waves on the atomic scale, including the aspect of light. The significance of Planck's constant in this concept is that it provides a wide range of randomization and random values so that randomness is maintained. Planck's constant *h* times the radiation frequency symbolized by the Greek letter nu, *ν*, or simply *E* = *hν* is the equation of the Plank's constant. The values of the Planks constant are given in the following table and this plays a huge role in the creation of the encryption standard.

Year	$h/10^{-34}$ J s	$u(h)/10^{-41}$ J s	Reference
1919	6.5543	100 000	Birge [5, 6]
1929	6.547	80 000	Birge [6]
1969	6.626 196	500	Taylor *et al* [44]
1973	6.626 176	360	Cohen and Taylor [12]
1986	6.626 0755	40	Cohen and Taylor [13]
1998	6.626 068 76	5.2	Mohr and Taylor [34]
2002	6.626 0693	11	Mohr and Taylor [35]
2006	6.626 068 96	3.3	Mohr *et al* [36]
2010	6.626 069 57	2.9	Mohr *et al* [37]
2014	6.626 070 04	0.81	Mohr *et al* [38]

I. EXISTING ALGORITHM

Quantum Fourier transform and Quantum Fourier sampling:

This is one of the most basic building blocks for the quantum algorithms in quantum computing. It is the part of many quantum algorithms mainly known as Shor’s algorithm used for factorizing and to compute the discrete and its time complexity is big oh of n^2 O(n^2) and its main property is to follow the Fact of unitary transformation.

Quantum Factoring and finding hidden structures:

The main idea of Quantum factorization is used calculating discrete logarithms and factorization of polynomial time complexity. It is major breakthrough in the field of quantum algorithms, because of its apparent speedup compared with the classical algorithms. This is well known because of its speedup in applications known

Grover’s algorithm and quantum random walks:

It is an another type of quantum algorithm to make use of random walk i.e. nothing but “Quantum random walk”. This addresses the particular problem for finding the different inputs for the function to get a accurate output. Its Time complexity is big oh of square root of N

Hamiltonian simulation algorithms:

Hamilton simulation algorithm is mainly focused on its structure or its behavior for the environment which it exists. Considering an example for Hamilton simulation algorithm used to find the structure of a particle and its behavior of its neighboring particles. Its first approach shown the implementation of time algorithm and it is referred as Hamilton simulation.

II. PROPOSED ALGORITHM APPROACH

The algorithm of this process is as defined below

A. The first step of this process is to take the input from the user

B. Second step of this process is to take the input message to the cloud system

C. The third step of this process is to take the encrypt this whole input message in the cloud to prepare a complex message digest using quantum principles.

D. The fourth step of this process is to send the message digest generated by the cloud to the receiver

E. The fifth step includes the decryption procedure of the obtained message digest

F. The sixth step includes the cloud services to decrypt the whole message in the cloud and to send this decrypted message to the receiver.

G. Here in this process the cloud acts as a medium between the sender and the receiver or the users

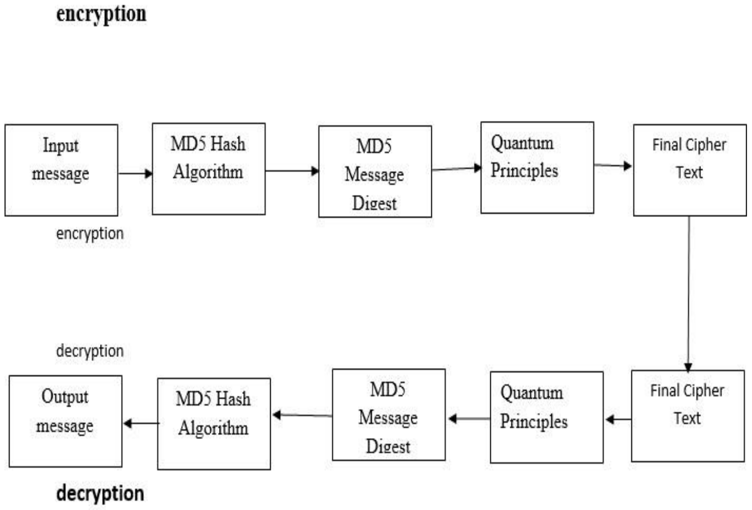
H. The whole set of the code for the encryption and the decryption is handled by the cloud servers and the users are provided with a direct attachment with the cloud system and there is no missing of the information.

I. And finally, the cloud even provides the services to store the information of the messages at a vast storage limits i.e. we can store a huge number of messages or information required and it adds an additional security to the system

Here we are using the concept of Heisenberg uncertainty principle and the encryption and decryption process will be done by using some of the quantum principles existing.

Here this concept is mostly based on the assumptions of the messages which are been sent from sender to receiver.

Our concept on developing the Encryption standard:



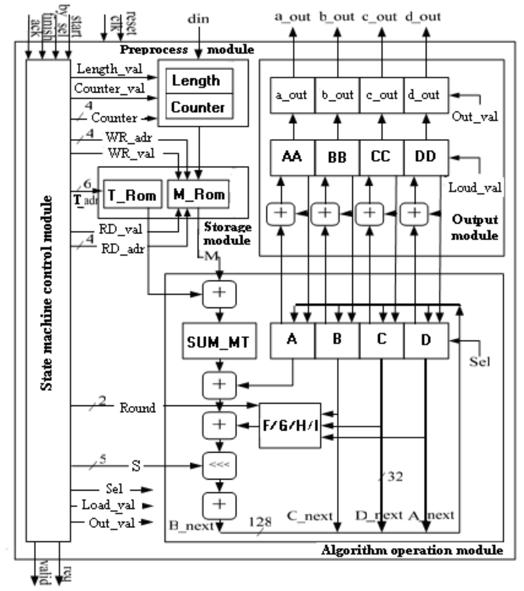
- This concept provides an additional security to the hash algorithms

About MD5 hash algorithm:

This is a hash algorithm developed Merkle-Damgard. It is a one directional cryptological operation or unidirectional cryptological operation. This algorithm provides a complex message digest and helps us in creating a secured way of message transfer with authentication.

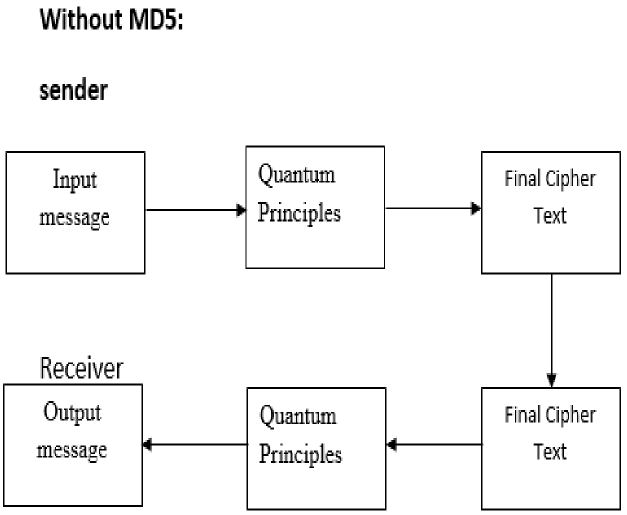
The MD5 hash operate was originally designed to be used as a secure cryptological hash rule for authenticating digital signatures.MD5 has been deprecated for uses aside from as a non-cryptographic confirmation to verify knowledge integrity and sight unintentional knowledge corruption.

This algorithm provides an additional security to the hash functions and this can be used as a customized version of the algorithm. This algorithm developed is customizable and flexible algorithm which can be adopted by any system and can be easily modified based on the needs and requirements.



Without Using MD5 Algorithm:

The architecture of the algorithm without MD5 algorithm is given in the below diagram



This concept can also be done without MD5 but it becomes a simple architecture. This can also be used for the process of encryption and decryption.

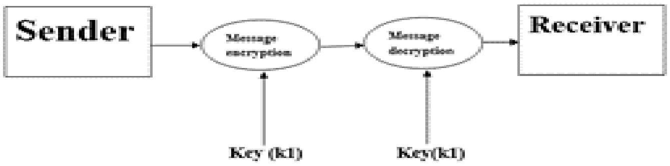
Key distribution concept of this algorithm:

A. The concept of key distribution is done by the message digest in the cloud and the cloud sends this cipher text to the receiver

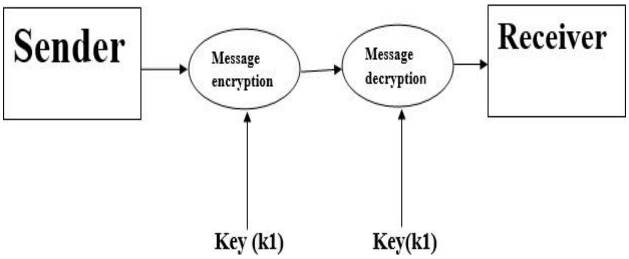
B. In this concept key is not used but it’s a typical assumption of the key

C. This gives a complex mechanism of the key

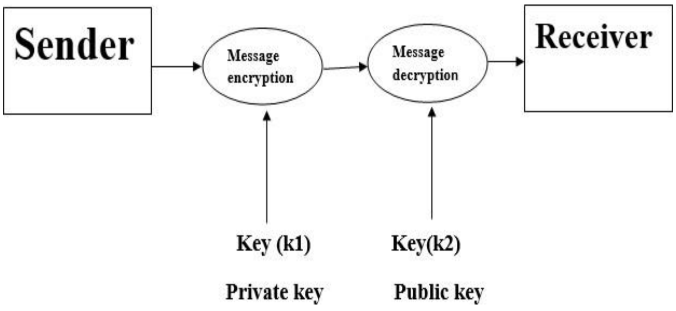
D. And this concept can be adoptable to any key mechanism and it can be used with keys also



Adoptable concepts:



This concept is adoptable with the public key encryptions and decryptions i.e. public key cryptography or Synchronous key distribution.



This concept also is adoptable for different keys to encrypt and decrypt the message using public key and private key i.e. Asynchronous key distribution.

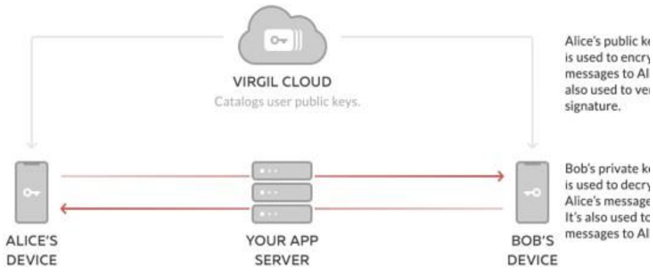
And this concept can also be adoptable for multiple keys to encrypt and decrypt the message like first encrypt with one key next decrypt with another key and again encrypt with another key etc. so to provide more security. That is Multiple key distribution. Finally, this concept can be adoptable with any key mechanism.

Amazon web services (AWS):

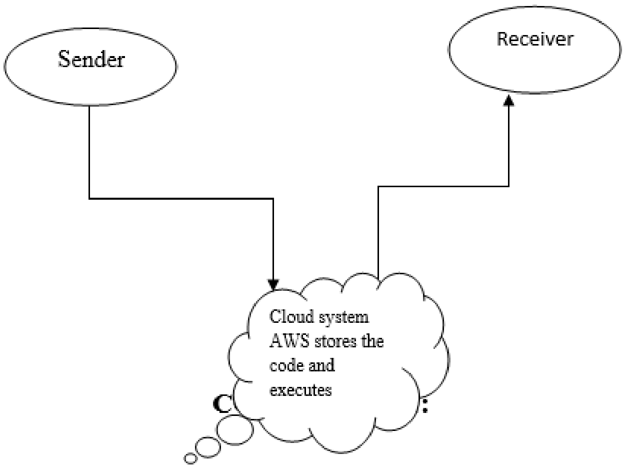
The amazon web services are one of the best leading services. These are one of the best on-demand services and on demanding best platforms to the users, companies etc. In this concept we are interacting with the cloud because this cloud servers or the AWS acts as the communicator between the sender and the receiver and this also provides an additional security to the architecture and as well as the algorithm.

This whole set of algorithm runs on cloud so that the services of the cloud are used in developing of this concept and provides additional security and additional storage to uses as cloud is well known in providing additional storage limitlessly based on user demand. Here cloud acts indirectly as an authentication sever for the users. The architecture of the cloud is as given below as follows.

CREATION OF ENCRYPTION STANDARD USING CLOUD:



Here we can see that the app server is connected to the cloud so that the connection between the two people Alice and Bob are done by the cloud and the connection between them passes through cloud only. Cloud acts a connectivity medium here.



Comparison:

The concept is been taken from the quantum principles. The algorithm which we had introduced is been fetched from our own assumption and from the quantum physics and formulas. The above papers which we had taken to reference are one of the top sophisticated quantum cryptography concepts which includes more investment of money and those concepts are not yet used for the public purpose and these concepts are so sophisticated and includes lot of money on this concept. As far as concerns the above concepts use quantum key distributions.

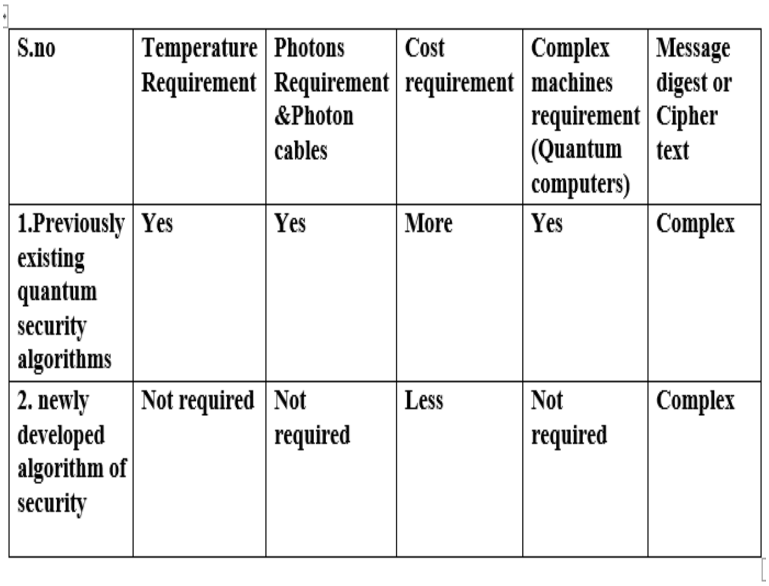
Because of this the more amount of money is used to create security and these concepts send photons through the cables and maintain the security. These photons require a low temperature to be generated and requires more cost not only the cost but it requires a high standard computer like quantum computers which can't be affordable and our concept uses just the quantum principles and tries to provide a high security encryption without photons and quantum computers. And our concept provides and additional security for the hash codes.

The concept developed in a way that it reduces the cost and provide a high standard encryption based on the assumptions of the quantum physics. Here we are using the cloud so that it provides an additional security for the algorithm and for the users to store the information and to retrieve the information at any time form the could and the further scope may include some concepts of open encryptions.

This concept is an open source for the key based encryptions and it can adopt to any key based encryption standards, this provides a vast range of customizability to the existing encryption standard. This concept has many advantages regarding the key distribution mechanisms like the symmetric key distributions and the asymmetric key distributions. This concept can be adopted with the multiple key mechanisms like using single, double or multiple keys while encryption and decryption. This concept can be easily adopted with the public and private key mechanisms like using pubic key for encryptions and private key for decryptions and vice versa.

Here from the comparisons we can say that the present concept can be easily available for all for public use and an we can have the full advantage of the Cloud mechanism and it can be used for storing and retrieval of the information and the messages can be stored and the users can have vast amount of storage and use the services of the cloud.

Comparison with the existing encryption mechanism:



S.no	Temperature Requirement	Photons Requirement &Photon cables	Cost requirement	Complex machines requirement (Quantum computers)	Message digest or Cipher text
1.Previously existing quantum security algorithms	Yes	Yes	More	Yes	Complex
2. newly developed algorithm of security	Not required	Not required	Less	Not required	Complex

The above table indicates the differences between the previous Quantum security systems and the new concept of Quantum security the differences indicates the advantages of the new quantum security developed in this project.

III. RESULTS

Expected result could be in this format.

Expected Input: (SENDER SIDE)

Hi

Expected Output: (RECEIVER SIDE)

Message digest=0.2650000000000000000000003200625

Hi

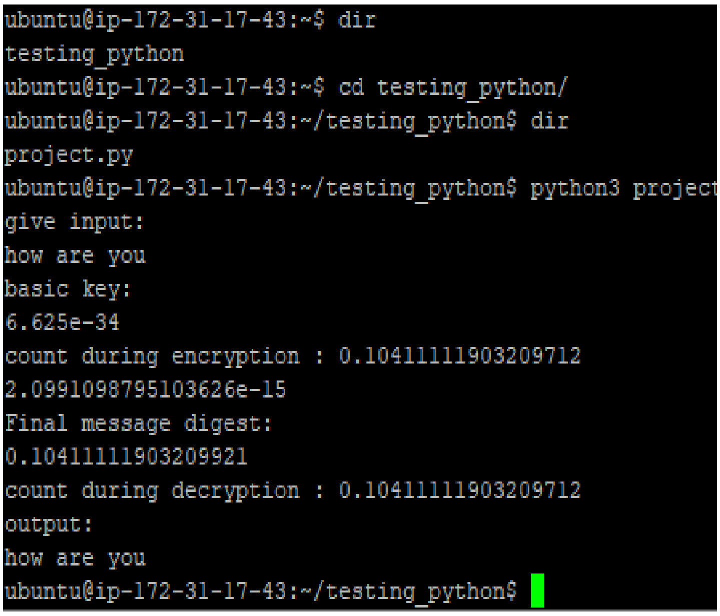
Expected Input: (SENDER SIDE)

How Are You

Expected Output: (RECEIVER SIDE)

Message digest=0.4290000000000000000000004254625

How Are You



```
ubuntu@ip-172-31-17-43:~$ dir
testing_python
ubuntu@ip-172-31-17-43:~$ cd testing_python/
ubuntu@ip-172-31-17-43:~/testing_python$ dir
project.py
ubuntu@ip-172-31-17-43:~/testing_python$ python3 project
give input:
how are you
basic key:
6.625e-34
count during encryption : 0.10411111903209712
2.0991098795103626e-15
Final message digest:
0.10411111903209921
count during decryption : 0.10411111903209712
output:
how are you
ubuntu@ip-172-31-17-43:~/testing_python$
```

IV. CONCLUSION

In this project, we have a tendency to expect the implementation of labour in chatting system that owner and users will act a lot of fluently.

This has been an essentially abbreviated and condensed raid the howling, and generally outlandish, world of quantum physics.

If some of elementary principles of physics were to be singled out from all of the on top of, they might in all probability be the twin wave-like and particle-like behavior of matter and radiation, and also the prediction of possibilities in things wherever classical physics predicts certainties. During this project we have a tendency to area unit making a brand-new secret writing commonplace that is predicated on quantum cryptography and that is a lot of advanced as that of the quantum secret writing commonplace that area unit gift within the gift day.

This project principally uses the Cloud services to urge in with the users and for the user's interaction. This methodology additionally |is additionally an efficient technique and also doesn't need high finish super computers.

This project takes the foremost benefits from the cloud services and uses its security as a further issue. This idea uses cloud services to store and retrieve knowledge or info. This project additionally acts as a further security for the Hash codes or hash algorithms that area unit gift thus far and helps in rising security.

The project is developed for many public uses and for communication reachability of the general public activity. The project is far appropriate and adoptable for several key distribution algorithms.

This secret writing commonplace additionally has abundant scope in future for development of an efficient advanced quantum cryptanalytic strategies.

V. FUTURE WORK

This algorithm can be used in multiple ways in future, it can be used as an alternative to the highly sophisticated Quantum cryptography and can be used in many messaging apps that can use cloud as a linkage between the users and can provide them storage. This concept also gives a new introduction to the open source encryption standards that could be modulated or customizable with any environment and platform and so that the encryption standard developed once can get additional changes and additional upgrades to sustain in future and can be adopted easily. And also, this provides beta developers or beta uses to create their own encryption standard for their own set of communication between different users that is different users have different sets of communication channels with other users. And here each and every channel is unique and different when communication with different users from a single user.

REFERENCES

[1] First edition – July 2018 ISBN No. 979-10-92620-21-4 Marco Lucamarini, Andrew Shields, Romain Alléaume

[2] Mehrdad S. Sharbaf Graduate School of Computer and Information Sciences Nova South Eastern University, Fort Lauderdale, Fl., 33314

[3] Joseph Russell, CISSP, Science Applications international Corporation O'Fallon, IL

[4] Hatim Salih, Zheng-Hong Li, M. Al-Amri, and M. Suhail Zubairy Phys. Rev. Lett. 110, 170502 – Published 23 April 2013

[5] Aparna Singh Department of Computer Science & Engg., SRGI, India IJCSMC, Vol. 6, Issue. 7, July 2017, pg.208 – 21

[6] Internet sources from ETSI company Technologies https://www.etsi.org/technologies/quantum-key-distribution

[7] Internet sources from the IEEE explorer https://ieeexplore.ieee.org/document/7544898/

[8] Internet source from the Research gate organization on quantum key generation, distribution and cryptography https://www.researchgate.net/publication/220484116_SECOQC_White_Paper_on_Quantum_Key_Distribution_and_Cryptography

[9] Internet sources from the Wikipedia regarding QKD https://en.wikipedia.org/wiki/Quantum_key_distribution

[10] Internet sources from the IdQuantique regarding QKD https://www.idquantique.com/resource-library/quantum-key-distribution/

[11] S. Gay, R. Nagarajan, N. Papanikolaou, "Probabilistic Model Checking of Quantum Protocols", *arXiv preprint quant-ph/0504007*, 2005

[12] C. H. Bennett, "Quantum cryptography: Public key distribution and coin tossing", *International Conference on Computer System and Signal Processing IEEE 1984*, pp. 175-179, 1984

[13] M. Elboukhari, M. Azizi, A. Azizi, "Verification of Quantum Cryptography Protocols by Model Checking", Int. J. Network Security & Appl, vol. 2, no. 4, pp. 43-53, 2010.

[14] "Effective security in social data security in OSNs" by Balakrishna, A.S.V., Srinivasu, N.

[15] "An Efficient Secret Sharing Scheme for n out of n scheme using POB number system" by Sreekumar et al.

[16] "Secure Cloud-Based Image Tampering Detection and Localization Using POB Number System" by Priyanka singh,B.Raman,N.Agarwal

[17] "Security in cloud computing: Opportunities and challenges" by Mazhar Ali, Samee U. Khan, and Athanasios V. Vasilakos.

[18] "Generalized secret sharing using permutation ordered binary system" by V. P. Binu and A. Sreekumar.

[19] Dan Bogdanov. 2007. Foundations and properties of

shamirs secret sharing scheme research seminar in cryptography. University of Tartu, Institute of Computer Science.

[20] “A novel secret sharing scheme using POB number system” by MP Deepika and A Sreekumar. 2016.

[21] KreˇsimirPopovi´candˇZeljkoHocenski.2010.Cloudcomputingsecurityissuesandchallenges.InProceedings of the 33rd International Convention. IEEExplore, Opatija. 344–349.

[22] Manoranjan Mohanty, Wei Tsang Ooi, and Pradeep K. Atrey. 2016. Secret sharing approach for securing cloud-based pre-classification volume ray-casting. Multimedia Tools Appl. 75, 11 (2016), 6207–6235.

[23] “Security in cloud Computing: Opportunities and Challenges” by M. Ali, S.U. Khan.

[24] “Entropy based CNN for segmentation of noisy color eye images using color, texture and brightness contour features” by Pathak, M., Bairagi, V., Srinivasu, N.

[25] “Multimodal eye biometric system based on contour-based E-CNN and multi algorithmic feature extraction using SVBF matching” by Pathak, M., Bairagi, V., Srinivasu, N.

[26] “Dynamic user management for secure cloud deduplication using enhanced checksum approach” by Srinivasu, N., Yashaswi

[27] “Energy efficient scheduling of virtual machines in cloud data center” by Akhila, B., Srinivasu, N., Varalakshmi, A.V., Samyuktha, T.R.

[28] “Multi-algorithmic texture feature extraction by fusing iris and sclera features for unconstrained images” by Pathak, M., Bairagi, V., Srinivasu, N.

[29] “Advanced hybrid approach to provide privacy for cross-site and XSS attacks in cloud computing” by Ranjeeth Kumar, M., Srinivasu, N., Reddy, L.C.

[30] “Dynamic and secure authentication using IKC for distributed cloud environment” by Kumar, M.R., Srinivasu, N., Reddy, L.C.

[31] “Fine grained multi access control via group sharing in distributed cloud data” by Ranjeeth Kumar, M., Srinivasu, N., Reddy, L.C.

[32] “Performance of multimodal biometric system based on level and method of fusion” by Pathak, M., Srinivasu, N.

[33] “Security analysis for control policy in OSNs” by Balakrishna, A.S.V., Srinivasu, N.

[34] “Des secured K-NN query over secure data in clouds” by Ranjeeth Kumar, M., Srinivasu, N., Reddy, L.C.

[35] “A dynamic approach to task scheduling in cloud computing using genetic algorithm” by Durga Lakshmi, R., Srinivasu, N.

[36] “CNB-MRF: Adapting correlative naive bayes classifier and MapReduce framework for big data classification” by Banchhor, C., Srinivasu, N.

AUTHORS PROFILE

Mr. B. Rajesh Asst. Professor
Department of Computer science K L Deemed to be University.

Dr. N. Srinivasu Professor
Department of Computer science K L Deemed to be University.