International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 5 Issue 6, September-October 2021 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Quantum Cryptography Approach for Resolving Cyber Threats

Madubuezi Christian Okoronkwo[1], Onwuzo J. C[1], Gregory E. Anichebe[2]

[1]Department of Computer Science, Michael Okpara University of Agricultural, Umudike, Nigeria
[2]Department of Computer Science, University of Nigeria, Nsukka, Nigeria

ABSTRACT

The research work focused on the future of the internet security transaction without allowing unauthorized user from accessing the secret document. The system was implemented with python flask framework been the lightest micro framework. The quantum key distribution generator model used is the BB84. Users can create account one the sender and other receiver then peered together in single communication channel. The sender attach file and send it in an encrypted manner to be received by receiver on presenting the same quantum key used for encrypting it. Once the eavesdropper click the link of the protocol, an alarm is raised and the system quantum key is change instantly and committed into the database. The other application is the Quantum Simulator, this application is used for generating a simulation for a quantum cryptography.

KEYWORDS: *Quantum Cryptography, Simulation, Encryption, Cyber threat*

How to cite this paper: Madubuezi Christian Okoronkwo | Onwuzo J. C | Gregory E. Anichebe "Quantum Cryptography Approach for Resolving Cyber Threats" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-5 | Issue-6, October 2021, pp.783-791, URL: www.ijtsrd.com/papers/ijtsrd46458.pdf

IJTSRD46458

1. INTRODUCTION

Internet security information has been designed and analyzed with the game method that affects online danger. The goal is to transmit information on the support channels without providing opportunities to reach the recipient's information. [1] [2]. This is a security science with people's security and easy-to-read harmonization. Encryption has arrived at radio networks, TV, TV, television and communication, and communication networks such as online transactions, web labels, e-mails and phones, important species, society, politics and communication lines Personal arrived. City

When sending channels/network, the best way to protect sensitive missions in the media is encryption. The purpose of programming is to guarantee security by non-approved third parties, but most of the algorithms can be broken, and information researches by pirates with sufficient time, desire, and the resources it can do so. Anonymous users use unknown formulas, our benefits. Traditional/classic approaches are encoded. The encoding is sent to a single style by sending base smoking messages to change the originality of the message. Extended messages are sent and the final recipient opens the message and selects a message. Buller coding code this is a good quantum mechanical model with a technological area (encryption/decryption). The first idea is "3" of the undermined manuscript that Stephen Vanner is not documented in 1970. However, this topic was seen in the only personal version of Benz in 1984 [4]. The main purpose of cryptography is difficult to perform traditional encryption (encryption/decryption) and quantum function. Quantum encryption devices mean quantum mechanics such as limit and quantum theory without quantum. The encryption systems and traditional protection are not yet high quantum cryptographic calculations for physics safety. The use of quantum encryption has been completed. There are many successes and improvements in quantity quantities and applications. The successful QKD programs have been guaranteed and unconditioned. Furthermore, the physical rules between unconditional security users encryption. Quantum encoding is based on the original uncertainty of Heisenburg, which can be viewed as a specific number of physical properties, which can simultaneously prevent the display from other values [5]. Use quantum photographs to move encrypted photons or large content. Each photon known as Cubit holds a little quantum. To get Qubits, you need to identify the photon of the polar recipient. Preparing photons of the general state to correct the information encoded in these photons following each security error. This approach is called small distribution and secret key to quantum key. For several decades, the elevators have had several small coding studies. Many NID group researchers can provide high-speed QKD documents. Take more than 4 million bits per kilometer [6]. Recently, research groups have sufficient speed for video transmission encryption in the [7] system to view more phases of grease. After the next purpose sequence. The implementation uses Quantum to identify the Internet, simple encoding, invitation, sender and future and subsequent encryption and identify after shipping information.

2. Theoretical Background

Encryption is an interesting technology that crosses the presentation material to believe in unnecessary parts. Let's take a look at how PGP works with friendly PGP (or GPG for your Open Source). I want to send your message so you can encrypt you in one of these applications. This message is the following.

Wuwdpglju9loonkbvf4vxspqgqzltcz7lwochdm5ksqlzt fttttw.Q6gvh8simlc3w6dohl2fdgvdo7sdv7g1z7pcnzfl p0lgb9acm8rzobi n5ske9cbvlvfgmq9vpfzzwzlodhcu7 / 2thg2drw3gqfz3swvwce7g. Mnivp5jgpcl4fgdp / xuywpk6ndlwairelthjf = pab 3 after encoding, the message is confused by random signals. However, you can understand the original message, equipped with secret traffic that has been sent to you.

2.1. KEY Triple DES

Before using 3TDE, the user generates a 3DS button, there are three different buttons 2 and 3. It means that the correct key contains 3 de 3 x 56 = 16 bits. The encryption method is the following

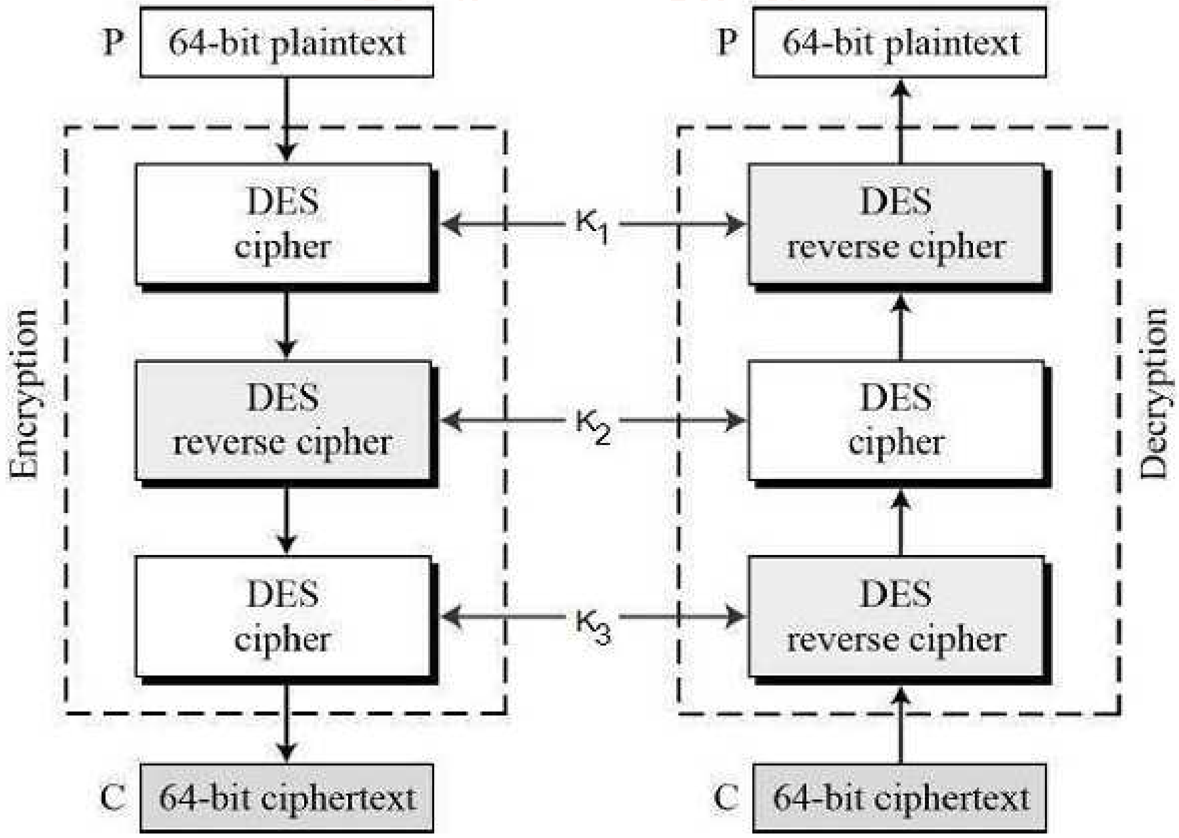


Figure 2.1 Three Triple Encryption DES

Encryption process: The following is the decryption coding people with a button. Sequence with a key 1. Finally, step 2 The output is encrypted in one of the 3. Export the text code Level 3. The decoding of the coded text is the insertion process. The user is disassembled with the first 3 and then encrypted in 2, and finally, 1 has been decoded. This triple design can be used as a coding process from 3D applications, so you can use the same amount of 2 and 3. This guarantees the previous compatibility. (2 TDS) is synchronized at three times three times the variable, but replacement 3 is 1. In other words, the user encrypts the Beletex block with 1 and decrypts the two keys, and closes again. Therefore, 2 TDS has a 112-bit key. The triple system is much safer than DS, but this process is very slow compared to the programming with one of them. (Https://www.tutorialspoint.com/crypptyography/trile_des.htmmmm, 2018)

2.2. Review of Related Literature

Browishhms makes 64-bit blocks (for example, Aess 128 bit) (for example Aess 128 bits), in particular HTTPS protocol attacks. In 2016, Swee 32 identified an attack using basic failures to improve (programming text) for zero in 64-bit blocks (programming text). [9] GnuPG projects are used to block encryption files and reduced the size of the group. More than 4 GB [10]. [1]

What is known as a weak key is known to be in contact with the reversal replacement of the permanent fish roller attacks? Bit Briefish Tower Tower is programmed in contact with this attack. [12] [13] Bruce Senir It is advisable to run a country twice. [2]

Simulation is known to be available following the development of online applications. Of course, some simulations are essentially used as simulated simulations with simulation simulation simulation. ProjectQ [9] is independent and this is a better dragon. Other fluid simulations [10] (presence) and QX [11] are closed. Currently, quantum simulation is easily acquired with QTIP [12]. This is not particularly designed for simulation, but small networks are sufficient to simulate. Quippt is a very simple way to extend Simulcon to work in an ideal qot and a friendly place. Insight, for example, error debugging should be executed correctly. In Python, the Quantum Samarner information community was written as the popularity of this language, and if you want to make it easy. The simylone's internal gesture is also complicated even for Peton [14]. Simulchron simulation can be measured in two ways as described in figure. 2 In the second part, we explain an overview of a single design and an internal work. In the third part, we discuss the integration with the CCU interface. We offer two simple examples to use Simularankron in the Python CCU library in the fourth section. Other examples can be found, programming and online API documents [15] Programming. Finally, we will discuss future progress and simlarner accessories. Researchers were able to modify many documents at the work of the project. Consider the risk of the future security of Internet security. The current systems are fully used by the practical algorithm/model/encoding. This means that the encoding model can understand and modify that the formula code is divided. Internet security, in particular financial transactions for information negotiation and intensive protection. The final coding model failed. This research stimulates the payment of information / electronic devices to improve user access to unauthorized access. There is a shortcut for coding.

3.1. ANALYSIS OF SYSTEM

Current systems speak more than traditional encryption algorithms. Current systems include communication traditions with very secure information with human custom. There is only the only receiver to have a tool to decode this message. No matter how the text is particularly safe (sports function). [3] The purpose of a traditional code is to suck that each code may not be disturbed by reading the meaning. This encryption method must be used to decrypt the programming process that can be encoded and decoded so that the original text can be recovered and read. The results of the process are that it is necessary to agree on the issuer process and future programming before connecting the code. For the re-use of programming methods, the different keys are known and encrypted, and encrypted, so it is not easy to decrypt every useless receiver, even if it is not easy to replace. This key must notify the current transmitter between the current transmitter and the beneficiary of the information, and is one of the weaknesses of traditional encryption.

3.2. Proposed System

Supplement System guarantee simulation cyber danger future danger the first protocol proposed to distribute the first quantum key quantum Benett and jill ba third in 1984. [9] is also known as bb 84. This system is based on individual particles or photons. Classic bits were encoded by photon polarization. Before supporting the BB 84 system, we would like to provide a small mechanical description used in the fact and the photon registry. Let's start with the impulses of extreme light. There is a fume for every impulse. Vertical (900) or horizontal (00) is related to the small mechanical encoding associated with ¬ or. And polarizations are also known as quantum countries (carriers), are mainly in the Hilbert region according to all photons. Programming systems are needed for communication. The ability to get the real bob bit is 0.75, and the rest displays a simple account that can be wrong. The 75% Bob Time, while six 25% of the time, get 75% of Alice's work [4]. This is the BB 84 protocol. If EVA exists, it is identified to measure photons to be sent to Bob. Eva does not successfully obtain 75% bits, but other photons are damaged. You can view the right bob bit with 0.625. Errors are 0.375 [6]. As a result, you can find standby because the incorrect price next to Bob is increasing. In many levels of contact between Alice and Pope, it is possible to describe the BB 84 protocol. Each step is described in Oya. Details of the BB 84 protocol with ideal public channels are not regulated for normal noise. This is not a real situation, but the protea is a courier, a quantity and usually defined in the type, so if noise occurs in the environment, it is the last thing you need to be light. Step 1: Accidentally send your photos and send them to Bob Bias. For example, send a set of 110101001. For each bit, it is random (or å or Å) as shown in Figure 3.1. Subsequently, the photon is polarized based on the mentioned codex.

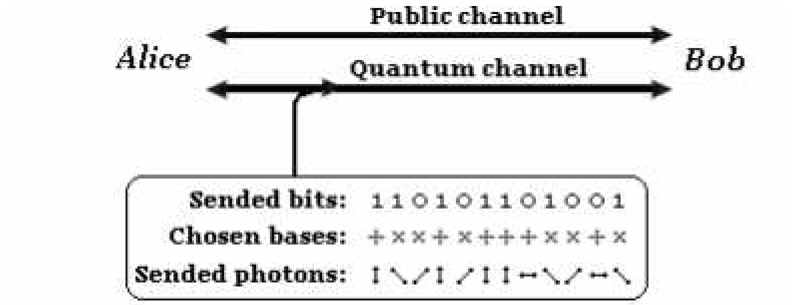

Public channel
Alice
Quantum channel
Bob
Sended bits: 110101101001
Chosen bases: +××+×++++××+×
Sended photons: ↕↘↗↕↗↕↕↔↘↗↔↘

Figure 3.1 Alice sends the photons, each one coded in a randomly chosen basis.

Step 2: Bob, is randomly selected for each receiver for photon extinction. If you choose the same base as Alice, I have an appropriate situation and explain. If another base is selected, you get the possibility of 0 or 1. Therefore, there are several errors, but some bits are completely random processes, as appropriate. The measurement of bob and random processes is indicated by a game. 3.2. Order the interpreted bit size. Even the unreleased keys are called. Therefore, the total key of Alice is the first series of bits sent to Bob (image #).

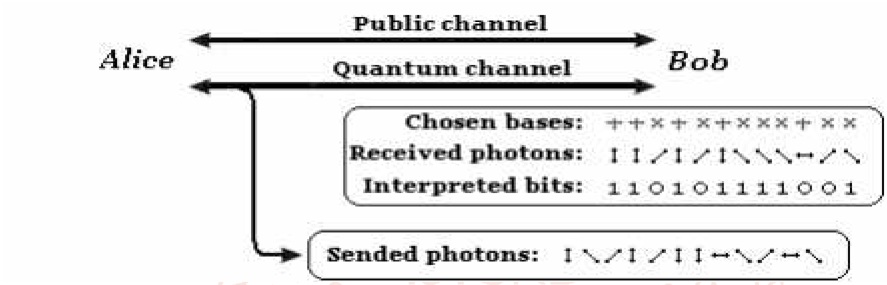

Public channel
Alice
Quantum channel
Bob
Chosen bases: ++×+×+×××+××
Received photons: ↕↕↗↕↗↕↘↘↘↔↗↘
Interpreted bits: 110101111001
Sended photons: ↕↘↗↕↗↕↕↔↘↗↔↘

Fig. 3.2 Bob receives each photon with a randomly chosen basis.

Step 3: Use public channels to discuss Bob Alice, a room you have. These results do not say that measurements have announced that the total key is used to receive all futon Alice respectively. If you use the same criteria of each photon, he replies with the Bob agreement. If this was not found, it is not the same, the opposite is declared. This is shown to a measure. 3.3. Alice and Pop, then delete the bit from the uncertain button from non-compliant rules, get a small key-Logy (Figure 3.3).

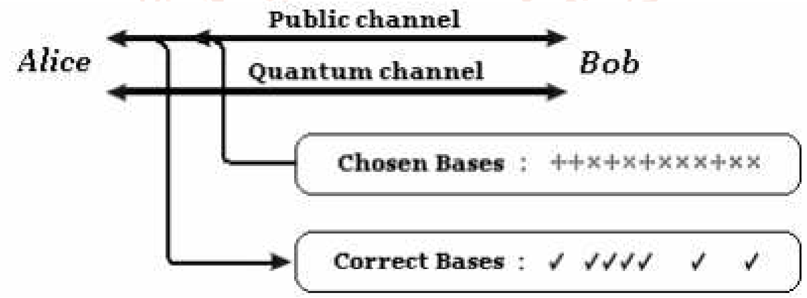


Fig. 3.3 Alice's and Bob's discussion over a public channel.

Therefore, if you use Alice, you need to share the same button or fumes. In theory, the key screen is a secret key. However, this happens when it comes to ideal tests. In real mode, changes in the photonic fiberglass environment or some photons are damaged by false errors during the night. As a result, the Alice and Burger Bob buttons do not match.

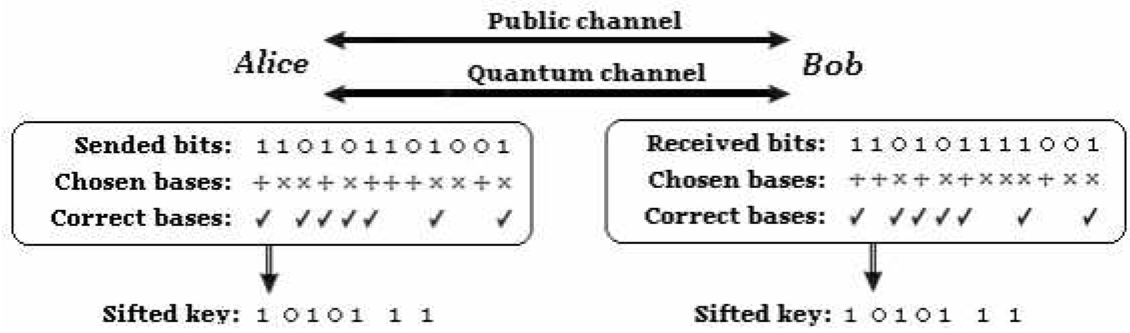

Public channel
Alice
Quantum channel
Bob
Sended bits: 110101101001
Chosen bases: +××+×++++××+×
Correct bases: ✓ ✓✓✓✓ ✓ ✓
Received bits: 110101111001
Chosen bases: ++×+×+×××+××
Correct bases: ✓ ✓✓✓✓ ✓ ✓
Sifted key: 10101 1 1
Sifted key: 10101 1 1

Fig 3.4. Alice and Bob extract the sifted key separately

After the three important steps of BB 84, Alice and the POP protocol are not the same keys during operation. In this case, there are different frequencies of post errors based on random samples (each section of the RAW button) of the RAW button on both sides. Use the error correction method to get an intermediary key without errors with a normal touch. Finish, improve privacy, ie selecting the subset of brokerage bits. It takes place in the data relating to the number of errors that may occur during the night because the compromise is partially approved [4]. The steps described here are common for other QKD protocols. Details also include EPR and QKD B29 protocols. The B22 protocol can be reduced to BB 84 and the EPR protocol uses quantum-related molecules compared to photon pairs produced by some particle reactions. Various protocols and QKD details are described in the modification method defined in [4, 5, 7].

3.2.1. Proposed System Architecture

The system architecture or system architecture is a conceptual model that determines more structures and behaviors. [8] An architecture description is a formal explanation and system view that maintains the structure and behavior of the system. In system configuration, system components may include advanced expanding systems such as public system work. The architecture description is an effort to attract languages to explain the structure of normal governance.

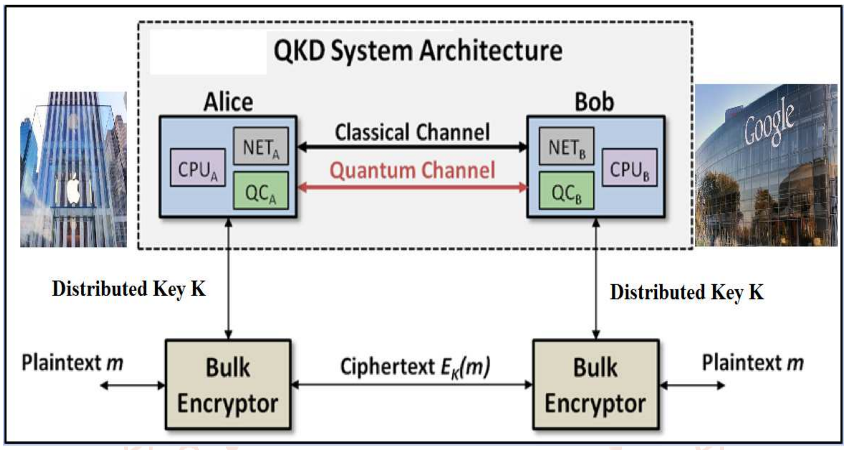


Figure 3.5 Proposed System Architecture

3.2.2. Comparing Existing System and Proposed System

Coding is a precious way for the long protection of the protected computer. Technology, modern and modern modernity must be performed sufficiently and must be possible. Encryption is used to encrypt scientific data and confuse data. Since anyone cannot read from any other non-recovery, the confidential information of the user can transfer networks that are not safe (for example). Further information and messages are connected and safe transport and algorithms have a cryptography generation. The algorithm is listed as additional information if not trusted. This approach is listed as encoded.

Table 1 Comparison of types of Cryptography

Features	Quantum cryptography	Classical cryptography
Basis	Quantum mechanics	Mathematical computation
Development	Infantile & not tested fully	Deployed and tested
Existing Infrastructure	Sophisticated	Widely used
Digital Signature	Not present	Present
Bit rate	1Mbit/s avg.[10]	Depend on Computing power
Cost	Crypto chip €100,000[11]	Almost zero
Register storage (n bit) at any moment	one n-bit string	2^n n-bit strings
Communication Range	10 miles max.[9]	Million of miles
Requirements	Devoted h/w & communication. lines	S/w and portable
Life expectancy	No change as based on physics laws	Require changes as computing power increases
Medium	Dependent	Independent

3.3. Design Methodology

Design methods are a complete design approach that can include many philosophies, theories, processes, and technology. In some cases, the type of design is connected to architecture or graphics. It could be a normal way to implement all designs. The following types of design methods are designed. This search is a design tool used to design Microsoft Word 2013. The app offers adjustment and other symbols.

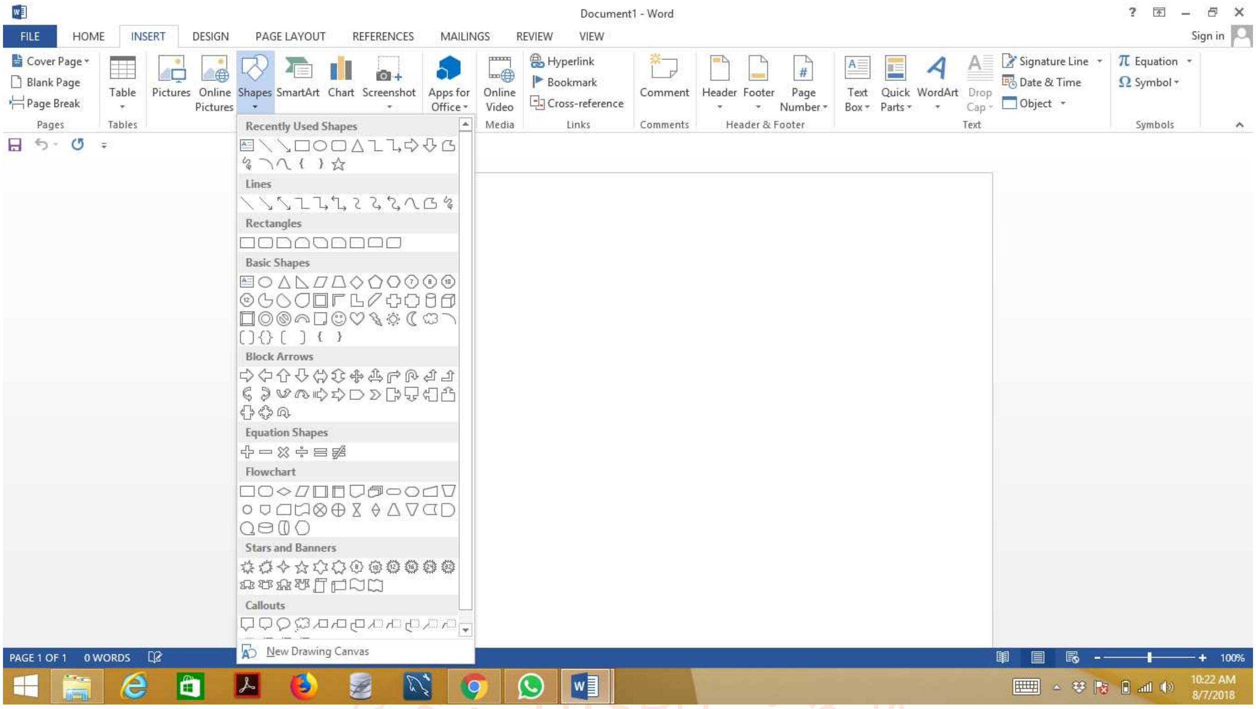


Figure 3.3: The Design Tool

3.4. Design of Proposed System

Design methods are a complete design approach that can include many philosophies, theories, processes, and technology. In some cases, the type of design is connected to architecture or graphics. It could be a normal way to implement all designs. The following types of design methods are designed. This search is a design tool used to design Microsoft Word 2013. The app offers adjustment and other symbols

3.5. Data Collection Method Used

Data collection is an important aspect of search results. The results of non-traditional data results may eventually cause invalid results. The data collection method varies with the assessment of the entrance. At the end of these levels, a collection of other volume methods and collection of canopy data. This section describes this research that various methods are different in the process of data acquisition. For each record, the best data collection method is determined by the properties of each method. There are several ways to collect data for analysis. The choice of this method depends on the type of data collected. Add data quality or quantitative.

Analysis of Data Collected

S/N	Questions	Responses	
1	Have you used Quantum Cryptography for encrypted file exchange; YES or NO	4	2
2	Which method; QKD or Traditional Yes/No	3	3
3	Was the traditional process easy; Yes or No	2	4
4	Did you face difficulties in the use of QKD for encryption and exchange; YES or NO	1	5
5	Would you like to use QKD for file encryption and exchange; YES or NO	5	1
6	How is the distance between the sender and receiver; is far away than 3 miles YES or NO	6	0
7	Do you think the QKD method is better than the Traditional method YES or NO	3	3

Demographic Data Representations

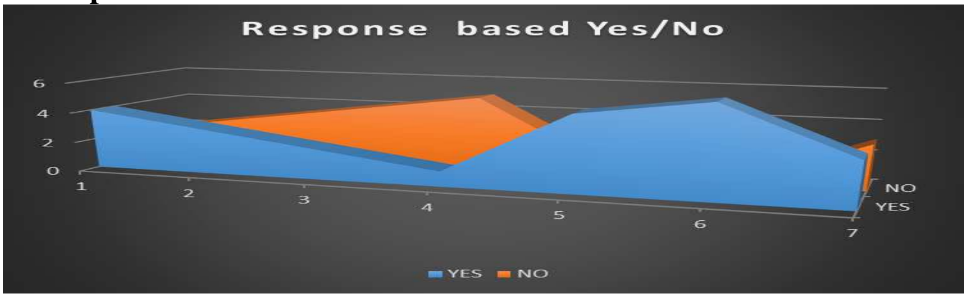


Figure 3.5 Demographic Data Representations

From the above data analysis, it is deduced that the Yes response over No response is high and requires the change of the system from the existing to the proposed system.

3.5.1. Block Diagram of the Proposed System

A block diagram is a systematic plan displayed by blocks associated with a row where the main component or the main activity block is displayed. It is made significantly in physical design engineering, electronic design, and software design, and process drainage system. Cluster projects are usually used at high levels and have less detailed explanations to define general concepts without specific examples. Details of the implementation of electrical components and implementation of the physical structure concerning the graphic planning and the plane used in electrical engineering.

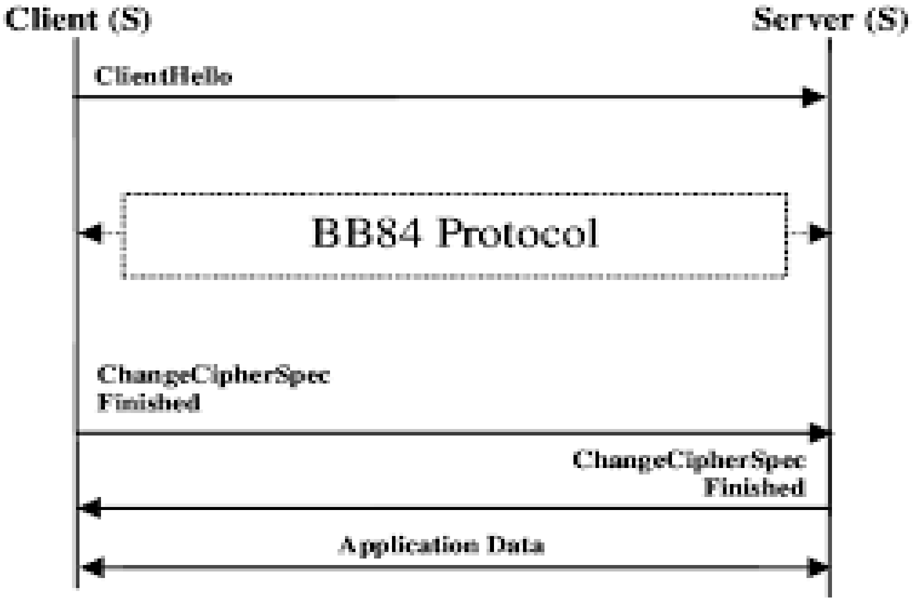


Figure 3.6: Block Diagram of the Proposed System

4.1. IMPLEMENTATION OF NEW SYSTEM

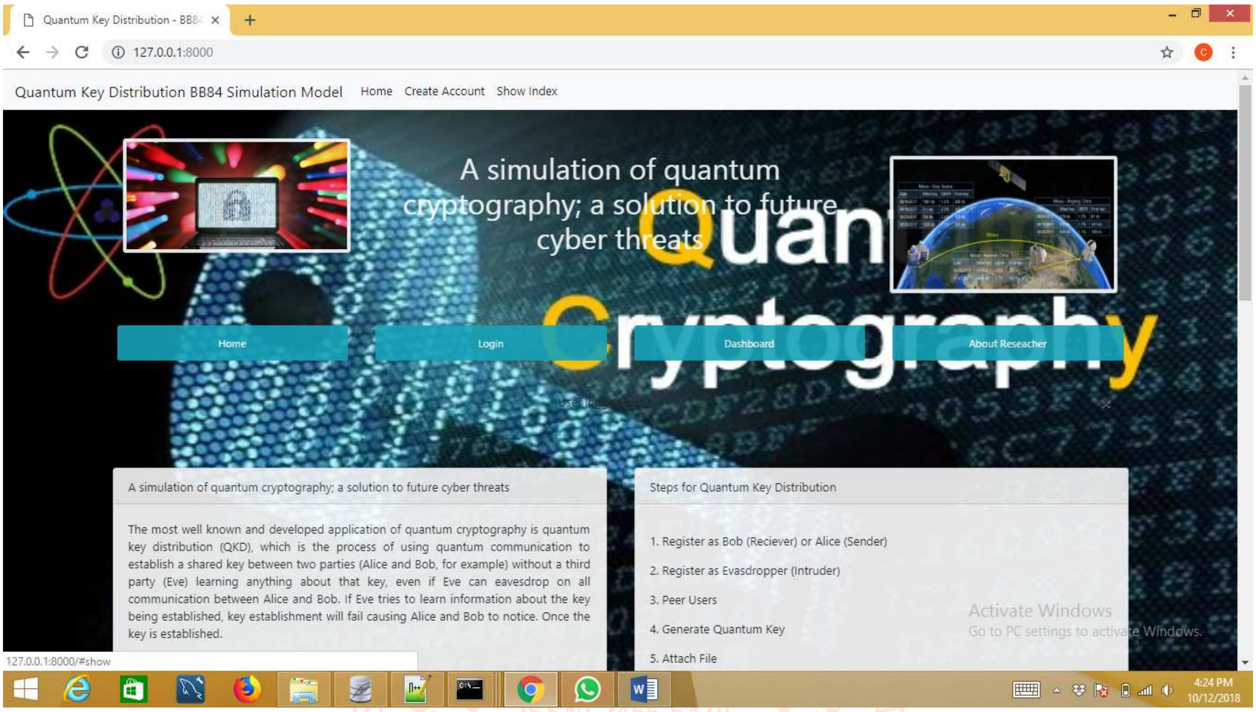
Simulation of research work Quantum cryptography. The solutions for future risks for computer hazards are better approaches to avoid failures obtained in all traditional systems. Quantum coding ideas were obtained from quantum physics engineers. When there is a change in the channel or the system, it speaks of sending senders and messages. If you try to attack a channel/system that the sender and future use, immediately accessible through the alarm and change the security system. When designing a new system, some factors are in mind to obtain a standard design standard. Develop a system that accepts channel encrypted channels or opens the contents of the database and decides the third user or user unauthorized to determine the third or unauthorized user. System design to determine user-user or unauthorized user includes system design. Develop a system. Develop a system. 'Obstacle. System design users can add and share the same series of divisions in small keys. Design system design of the first analog user ID and controls QKD KAKI. The design of the system can simulate the ability to combat the overall process of future Internet security and the risk of the future Internet.

4.2. Decomposition and Cohesion of the High-Level Model

It is designed by the design and planning of the organization and organizational problems designated by commands and commands in commands and controls and are designed by most researchers, from software developers and technical projects designed by organizational and systematic problems. Basic properties of unit analysis, high adjustment, and low stabilization. Consistency is a scale of work capacity. It is said that the highresolution modules and the consulate are irrelevant to other independent units. The link between the two units is between two coordination or coordination. Complete research activities are divided into important units. Wear quantum and quantum simulation. This is the most important factor in the proposed system. These two main components apply to the following components: this is a quantum keys generator.

4.2.1. Main Menu

The main command menu or main system is several components that work together to reach the goal. This means that the second menu is available. This system contains a response display and the home user interfaces display to create a connection from the main menu account of the control center. After creating an account, scroll down the Dashboard button on the user profile page (Send Side / Receiver). Once you have saved the user as a transmitter/receiver, the user can correctly enter the forum from the set of other connection systems to implement quantum simulation or quantum simulation.


Quantum Key Distribution - BB8
127.0.0.1:8000
Quantum Key Distribution BB84 Simulation Model
Home
Create Account
Show Index
A simulation of quantum cryptography; a solution to future cyber threats
Quantum Cryptography
Home
Login
Dashboard
About Reseacher
127.0.0.1:8000/#show
4:24 PM
10/12/2018

A simulation of quantum cryptography; a solution to future cyber threats

The most well known and developed application of quantum cryptography is quantum key distribution (QKD), which is the process of using quantum communication to establish a shared key between two parties (Alice and Bob, for example) without a third party (Eve) learning anything about that key, even if Eve can eavesdrop on all communication between Alice and Bob. If Eve tries to learn information about the key being established, key establishment will fail causing Alice and Bob to notice. Once the key is established.

Steps for Quantum Key Distribution

1. Register as Bob (Reciever) or Alice (Sender)
2. Register as Evasdropper (Intruder)
3. Peer Users
4. Generate Quantum Key
5. Attach File

Activate Windows
Go to PC settings to activate Windows.

Fig 4.1 Main Menu of New System

4.2.2. The Submenus

The submenu is where you are dealing with the system. The inutile workflow is a predefined environment promoted by the meaning of the system and wealth. There may be various subtitles used to display the menu in another list in the system. The subsystems of this app are complete programs and quantum simulations. Through this list of small quantum applications, a list of roses. NS. After adding a button, add a quantum connection, colleague, files, and files in the last file. As soon as quantum cryptography is simulated, as well as quantum simulation. You can save the simulation process in a video file.

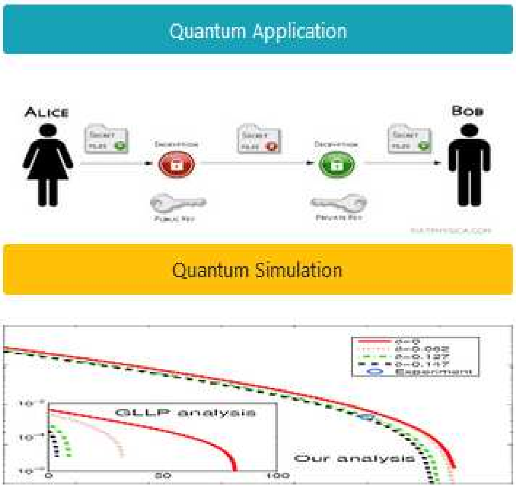


Fig. 4.2 Major Submenu

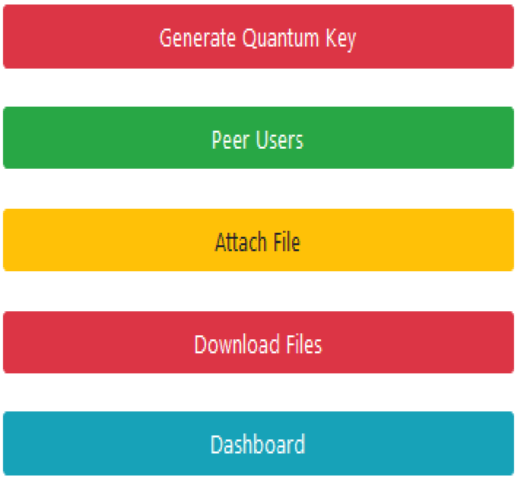


Fig. 4.3 Quantum Application Submenu

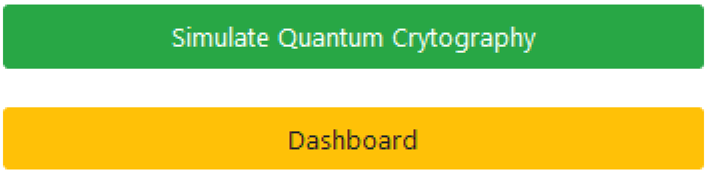


Fig. 4.4 Quantum Simulation Submenu

5. CONCLUSION

Looking for quantum encryption solutions for the simulating Cyber threat solution future provides a systems that prevent users from illegal online transactions or file payments and users who would want to access distributed facilities. In this, System tests and approval are performed. This application is the first real model of the system to checkmate the risk of the future Internet. The platform is equipped with a python bottle frame and an SQLite database. Spiral models are used based on models for the production of the proposed system. Simulation platform is the practical future, to perform the entire system. The quantum key is as quantum file code Refuge and two users (Alice and Pop). The file is connected to Alice, we need to encrypt the small key created for Bob.

REFERENCES

[1] C. E. Shannon, Bell (2018) Quantum Cryptographic Task (Syst. Tech). J. 28

[2] N. L¨ukenhaus, Phys. Rev. A 61, 052304 (2000). Quantum Simulation

[3] Madsen, Mathias http://informationtheory.weebly.com/presentation-topics.html

[4] Hannu Jaakkola and Bernhard Thalheim. (2011) "Architecture-driven modelling methodologies." In: Proceedings of the 2011 conference on Information Modelling and Knowledge Bases XXII. Anneli Heimbürger et al. (eds). IOS Press. p. 98

[5] Bouwmeester, D.; Ekert, A.; Zeilinger, A. (2000): The Physics of Quantum Information, Springer-Verlag, Berlin

[6] Gisin, N.; Ribordy, G.; Tittel, W.; Zbinden, H. (2001): Quantum cryptography, arXive e-print quant-ph/0101098

[7] Kitaev, A.Y.; Shen, A.H.; Vyalyi, M.N. (2002): Classical and Quantum Computation, AMS

[8] Lomonaco, S.J. (1998): A Quick Glance at Quantum Cryptography, arXive e-print quantph/9811056.

[9] Bennett, C.H.; Brassard, G. (1984): Quantum cryptography: public key distribution and coin tossing, Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, IEEE press. [This is the "BB84" protocol of C. H. Bennett and G. Brassard: *Quantum cryptography: Public key distribution and coin tossing*, originally in proceedings of IEEE ICCSSP; 1984]

[10] Dave Wecker and Krysta M. Svore. LIQUi|>: A Software Design Architecture and Domain-Specific Language for Quantum Computing. 2014.

[11] N. Khammassi, I. Ashraf, X. Fu, C.G. Almudever, and K. Bertels. QX: A high-performance quantum computer simulation platform. Design, Automation & Test in Europe Conference & Exhibition (DATE), 2017, pages 464{469, 2017.

[12] J. R. Johansson, P. D. Nation, and Franco Nori. QuTiP: An open-source Python framework for the dynamics of open quantum systems. Computer Physics Communications, 183(8):1760{1772, 2012.

[13] Python. https://www.python.org/.

[14] Twisted. https://twistedmatrix.com/trac/.

[15] SimulaQron. http://www.simulaqron.org.