Quantum Cryptography in online Banking

Anoushka Rastogi and Shilpi Sharma

June 3, 2020

Quantum Cryptography in Online Banking

Anoushka Rastogi[1], Shilpi Sharma[2]

Amity University Noida, Uttar Pradesh[1, 2]

Anoushkaanu123@gmail.com[1],ssharma22@emity.edu[2]

Abstract-The new data innovation is turning into a significant factor especially in banking sector, like Internet banking is the most current conveyance channel for retail banking administrations. In this paper we see the security of these online banks through Quantum cryptography using quantum key distribution protocols like Brassard and Bennett 1984 model with the gist of some research works already done in this field and also most important the global analysis that how the world would be welcoming this technique with open arms.

Keywords: **QKD, Quantum cryptography, online banking.**

I.INTRODUCTION

Cryptography is an asset to the technology, it provides us highly secured platform for transaction in financial department or the security from eavesdropper in defence and soon so forth. In this paper we would be talking about one of the most prominent kind of cryptography i.e. Quantum Cryptography for baking sector. This Quantum cryptography is the study of making most of the use of quantum mechanical properties to perform cryptographic undertakings. The most popular case of quantum cryptography is quantum key distribution[1].Which offers a data theoretically secure solution to the key exchange problem.

Banking organizations are looking to effectively guard delicate information that is held at each point simultaneously. Regardless of whether that is by means of cell phones, through applications, by means of their inside system or through sites.

Banking enterprises are looking to effectively guard subtle information that is held at each point all the while. Regardless of whether that is by means of cell phones, laptops,Pcs or any digital medium.

They will likewise be hoping to add expanding levels of shielding to databases that hold key client and transactions ordain that the offenders are looking for and furthermore to ensure themselves against market jeopardy and financial catastrophe.

Nowadays, most of the prominent banks like JPMorgan and Barclays are now relying on this technique.

This significant advancement could absolutely supplant different types of secure information assurance, for example, block chain have very high chances to be replaced.

Quantum encryption will empower banks to send information which is practically unhackable over a quantum arrange. Quantum cryptography utilizes a framework called quantum key distribution otherwise called QKD which guarantees encrypted messages and its keys are sent independently. In the event that these messages and keys are altered, or altered in any capacity, they are naturally destroyed.

Now, both the sender and the recipient are notified.
As indicated by look into attempted by Juniper Research, Cybercriminals will take 12 billion records in 2019, trailed by a stunning evaluated 33 billion records in 2023.

Cybercrimes are a worldwide issue and a developing number of organizations turning out to be casualties every day....

In Quantum cryptography - The investigation of security prerequisitesit deals with security of the communication system..[8]

In Normalization of quantum key appropriation and the ETSI normalization activity ISG-QKD Here we dissected QKD as a cryptographic crude and how it very well may be joined with one-time-cushion encryption.[9]

In Express assault on the key in quantum cryptography (BB84 convention) arriving at the hypothetical mistake limit Q c ≈ 11% . It is the proof of the bb84 model security.[10]

In 802.11i Cipher Key Distribution Using Quantum Cryptography In this paper, it presented an improved rendition of the Quantum handshake, a plan incorporating quantum key appropriation in 802.11 systems proposed by our past works.[11].

In Execution of secure key dissemination dependent on quantum cryptography.again it shows the security of the bb84 model.[12]

In A Trusted Third-Party E-Payment Protocol Based on Quantum Blind Signature Without EntanglementAll the requirements regarding blind signatures have been fulfilled.[13]

In Quantum computers put block chain safety at danger.quantum may chance the security of the blockchain for the second yet it will without a doubt secure this too.(1 way work).[14]

II. LITERATURE REVIEW

In this section we will discuss about the various conclusion derived from the papers read as part of the background study.

In An Online Banking System Basis on the Quantum Cryptography Communication.It provides with the safest method of online banking unlike the earlier ones.[2]

In Quantum Key Distribution: Blessing or Condemnation?Basically it contains the QKD model as well as the BB84 model had been cleared.[1]

In Exchange and Identity Authentication Security Model for E-Banking: convergence of Quantum Cryptography and AIThe e-banking system is introduced to quantum cryptography for better authentication. [3]

In Verification in Online Banking method through Quantum Cryptography.It provides with high certainty of safety to online system.[4]

In An overview on quantum cryptography and quantum key distribution conventions.QKD is the overall basis of this paper and its protocols which helps in quantum cryptography.[5]

In E –Payment System Using Visual and Quantum Cryptography.Again the importance of e-payments residing quantum cryptography[6]

In A powerless visually impaired mark conspire dependent on quantum cryptographyIt deals with the blind signature scheme correlation with EPR technique.[7]

In Disconnected Arbitrated Quantum Blind Dual-Signature Protocol with Better Performance in Resisting Existential Forgery Attack.The signature is now more secure than the previous ones.[15]

In ENSURING SECURITY OF FINANCIAL TRANSACTION BY USING QUANTUM CRYPTOGRAPHY

IV. METHODOLOGY

The basis of this cryptography i.e. Quantum cryptography is Quantum Key Distribution quantum Key Distribution (QKD) is a rising cyber security innovation which gives the way to two topographically isolated gatherings to develop "wholehearted security" symmetric cryptographic keying material. In contrast to conventional key distribution methods, the security of QKD lays on the laws of quantum mechanics and not computational complexity.

The QKD origin was from the first cryptographic invention which took place in 1960 by Stephen Weisner of conjugate encoding in which it is a tool which create the fraud proof bank notes. This idea was better explained by the examples taken by Charles Bennett by it was not considered feasible as it was for ahead of the time at that time.

QKD method was basically the transmission between the sender (Alice) and the receiver (Bob) through cryptographic channel and it was considered as secure against eavesdropper who was happened to be deaf as this makes audible noises while encrypting data in room and this proposed by IN BANKING ENVIRONMENT. The power of a given cryptosystem depends basically on the mystery of its (private) key and the trouble with which the converse of its single direction function(s) can be determined. Despite what might be expected, quantum cryptography is a strategy for sharing mystery keys, whose security can be officially illustrated.[16]

BRASSARD AND BENETTE (BB84) in 1984.

BRASSARD AND BENETTE 1984 MODEL:

Step1 –

Alice and Bob verify with one another to authenticate they are speaking with the known party. Normally, this verification is practiced with the lesser known Wegman Carter validation method to meet QKD's unquestioningsecurity guarantee. Also, not at all like most digital frameworks which validate just while starting transmission QKD frameworks regularly use a value-based verification conspire where validation happens after each progression (or a grouping of steps) as per the particular framework execution.

Step2 –

During quantum exchange, Alice construct single photons, known as quantum bits or "qubits," in one of four polarization states |↔⟩, |↕⟩, |⤢⟩, or |⤡⟩.This photon polarization is then randomly chosen. Then these photons are transmitted from quantum channel to bob at other end where the loss percentage is expected to be more than 90 % ,this happens because there is a transmission of one photon from very long distance, this causing in limiting the transmission of photon from Alice’s side. Let’s assume the photon has been received by bob, now its paramount for bob to select the measurement basis randomly if the encrypted value is correct (0 or 1) this is considered as high level of certainty but if the value is incorrect then the originally bit will be destroyed.

Step3 –

Bobs detection will sift to eliminate the incorrect ones. 50% of bob's detections will be sifted because of incorrect matching. this results in a shared shifted key also called as" raw key",in both Alice and Bob roughly a large portion of the size of Bob's underlying set of identifications.

Step4 –

Normally, an irregular level of bits are chosen and looked at over the old style channel.The estimatederror rate is used to inform the error reconciliation technique (step 5), and can also be used to conduct an initial security check. This step is very crucial because QKD can't differentiate between the noise or malevolent intervention. Now if the faulty rate is more than 11% then the raw key is repudiated.

Step5 –

Error reconciliation is performed at Alice and bob's raw key Due to device non-idealities and physical disturbances during quantum exchange, physical disturbances during quantum exchange, expected error rates are typically 3-5%.this technique specialize bi-directionalcorrection algorithms (e.g., Winnow, Cascade, or Low-Density Parity-Check) which reduces the chance of leakage of the information to the eavesdropper The errorreconciliation step results in a formalized Quantum Bit Error Rate (QBER), is again compared with 11% rate if this exceeds then the key is repudiated.

Step6 –

The main motive of this step is to check that no sensitive information regarding secret key is leaked may be from non ideal laser which produces multiple photons The entropy estimate is then passed to the privacy amplification step, which ensures that information is leaked and there is no information leaked to the eavesdropper.

Step7 –

It employs advanced information theory techniques such as a universal hash function to produce a more secure final shared secret key.

Step8 –

Last step delivers the keys to the owner if they pass the symmetric crypto key test at last it is then considered one the most secured channel for the exchange of data, money etc.

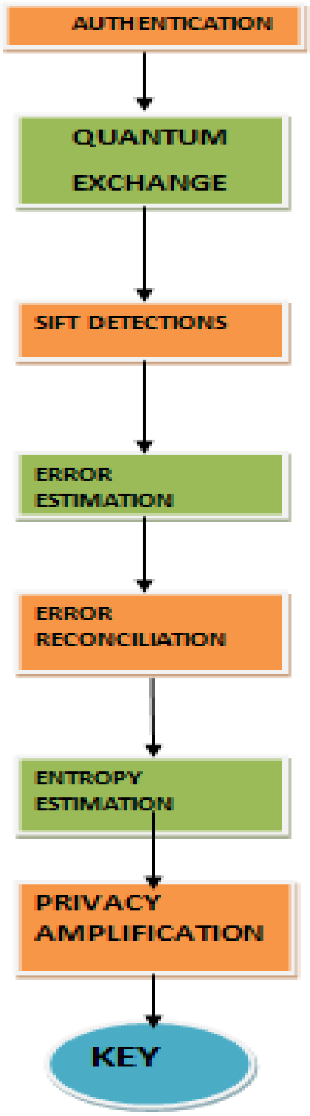

Fig1:The basic model of BB 1984 model.

QUANTUM CRYPTOGRAPHY IN ONLINE BANKING:

Step1 –

AUTHENTICATION IN ONLINE BANKING:

In web based financial networks, banks must guarantee that clients have a sense of security when utilizing internet banking transactions .They can control the authentication level as it takes to enter their destinations. They can refrain and terminate cyber attackers by making it very hard to have accomplishment in acquiring deceitful access to a client's record.

Step2 –

QUANTUM CRYPTOGRAPHY IN ONLINE BANKING

These days, Banks and financial departments utilize either symmetric cryptography or asymmetric cryptography. In any case, because of the appearance of complex innovation and cryptanalysis methods, security arrangements are not completely secure. As computers become all the more remarkable, encryption and decryption keys must be longer so as to hold the degree of trouble. So exchanges could be defiled and adjusted without the knowledge of the bank. This creates a genuine trouble since cyber attackers and malicious associations could benefit of the rupturing and hijack. Making sure these financial departments attains most of the security.

One of significant worries in web based banking is a security danger. This segment talks about on primary difficulties in internet banking for example validation. Since most web based financial applications utilize some pass-code or PIN for business transaction settlements. Analysts have been effectively engaged with improvement of made sure about techniques for web based banking over the Internet. Validation is significantly progressively delicate issues in online banking. The banking industry is managed and checked by governments and web based financial need to guarantee controllersof security for their customer. Some of the most prominent companies have been taking care of the authentication of online banking system such as MagiQ Technologies, New York; idQuantique, Geneve and SmartQuantum, New York .

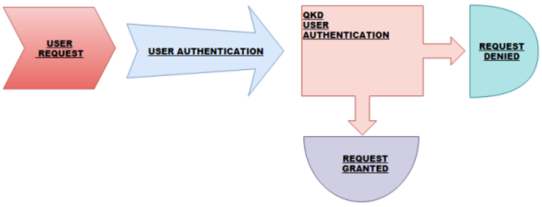

Fig 2:This is how online banking using works using quantum cryptography.

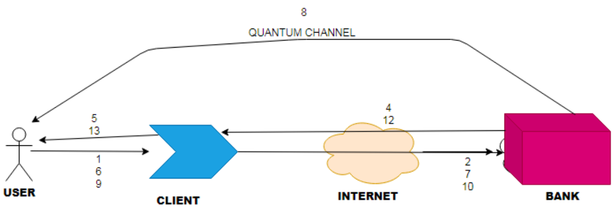

Fig 3: This shows the path how it works.

1. Create sign in ID and password.
2. Convey sign in ID and password.
3. Authenticate sign in ID and password.
4. Convey system option.
5. Available system option.
6. Negotiation request.
7. Convey negotiation request.
8. Quantum key distribution.
9. Create quantum code.
10. Convey quantum code.
11. Authenticate quantum code.
12. Convey negotiation justification.
13. Available negotiation justification.

V. IMPEMENTATION ANDRESULTS

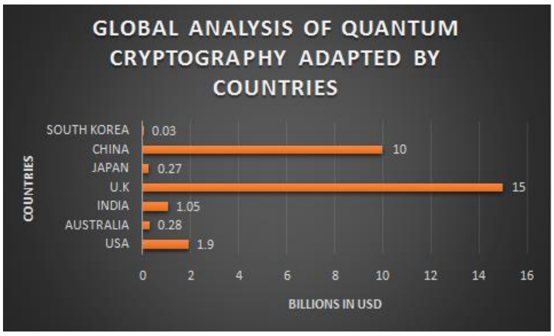

Fig 4:Globalanalysis of quantum cryptography adapted by countries.

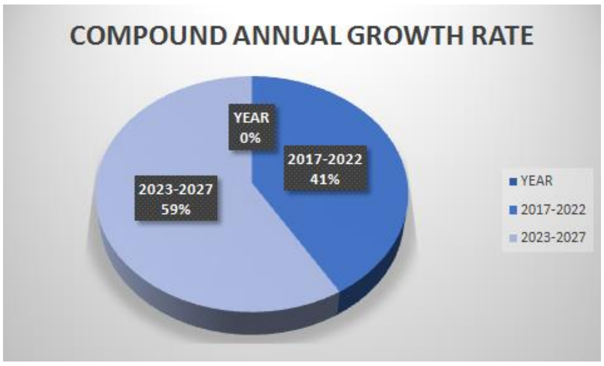

Fig 5: This compound annual growth rate.

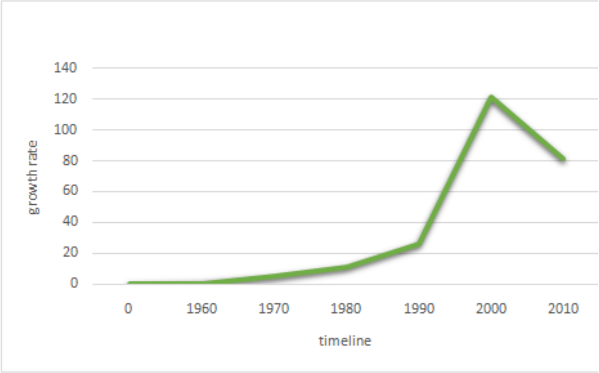

Fig 6: This shows the timeline of quantum cryptography from year (1960-2020).

VI. CONCLUSION

From above research it conclude that security is utmost important to everyone whether we talk about financial,defence or any other department. It has been predicted that in future cybercrime would definitely be at its peak we didn't secure our system today,billions of database could leaked and this could be the business of many companies. Quantum Cryptography is very cardinal method of securing our web based transactions as it authenticate the user as well and for banking system it is a boon as we all know that because of this epidemic i.e. CORONA VIRUS has topple most of

VII. FUTURE SCOPE

The world to recession and now people would definitely turn up to these techniques for their security of credentials. Now here comes about the future of this technique it has very luminous future as large amount of work is still going on this and we shall see more and more work regarding this cryptography .Many countries like England had already invested 15 billion dollars and china has been investing 10 billion dollars. India has invested 1.02 billion dollars. Thus, this shows **Quantum Cryptography** has very brilliant future.

REFERENCES:

[1] L. O. Mailloux, D. D. Hodson, M. R. Grimaila, C. V McLaughlin, and G. B. Baumgartner, “Quantum Key Distribution: Boon or Bust,” J. Cyber Secur. Inf. Syst., vol. 4, no. 2, pp. 18–25, 2016, [Online]. Available: https://www.csiac.org/journal-article/quantum-key-distribution-boon-or-bust/.

[2] R. gui Zhou, W. Li, T. tian Huan, C. yi Shen, and H. sheng Li, “An Online Banking System Based on Quantum Cryptography Communication,” Int. J. Theor. Phys., vol. 53, no. 7, pp. 2177–2190, 2014, doi: 10.1007/s10773-013-1991-7.

[3] R. Muzzammel, Intelligent Technologies and Applications, vol. 932. Springer Singapore, 2019.

[4] A. Sharma and S. K. Lenka, “Authentication in online banking systems through quantum cryptography,” Int. J. Eng. Technol., vol. 5, no. 3, pp. 2696–2700, 2013.

[5] L. Gyongyosi and L. Bacsardi, “A survey on quantum key distribution,” Infocommunications J., vol. 11, no. 2, pp. 14–21, 2019.

[6] P. A. Shemin and K. S. Vipinkumar, “E –Payment System Using Visual and Quantum Cryptography,” Procedia Technol., vol. 24, pp. 1623–1628, 2016, doi: 10.1016/j.protcy.2016.05.166.

[7] X. Wen, X. Niu, L. Ji, and Y. Tian, “A weak blind signature scheme based on quantum cryptography,” Opt. Commun., vol. 282, no. 4, pp. 666–669, 2009, doi: 10.1016/j.optcom.2008.10.025.

[8] M. Niemiec, “Quantum cryptography - the analysis of security requirements,” Ict. 2009 11th Int. Conf. Transparent Opt. Networks, pp. 2–5, 2009, doi: 10.1109/ICTON.2009.5185137.

[9] T. Länger and G. Lenhart, “Standardization of quantum key distribution and the ETSI standardization initiative ISG-QKD,” New J. Phys., vol. 11, 2009, doi: 10.1088/1367-2630/11/5/055051.

[10] S. N. Molotkov and A. V. Timofeev, “Explicit attack on the key in quantum cryptography (BB84 protocol) reaching the theoretical error limit Q c ≈ 11%,”

JETP Lett., vol. 85, no. 10, pp. 524–529, 2007, doi: 10.1134/S0021364007100116.

[11] T. M. T. Nguyen, M. A. Sfaxi, and S. Ghernaouti-Hélie, “802.11I Encryption Key Distribution Using Quantum Cryptography,” J. Networks, vol. 1, no. 5, pp. 9–20, 2006, doi: 10.4304/jnw.1.5.9-20.

[12] M. Elboukhari, A. Azizi, and M. Azizi, “Implementation of secure key distribution based on quantum cryptography,” Int. Conf. Multimed. Comput. Syst. -Proceedings, pp. 361–365, 2009, doi: 10.1109/MMCS.2009.5256673.

[13] X. Guo, J. Z. Zhang, and S. C. Xie, “A Trusted Third-Party E-Payment Protocol Based on Quantum Blind Signature Without Entanglement,” Int. J. Theor. Phys., vol. 57, no. 9, pp. 2657–2664, 2018, doi: 10.1007/s10773-018-3787-2.

[14] A. K. Fedorov, E. O. Kiktenko, and A. I. Lvovsky, “Quantum computers put blockchain security at risk,” Nature, vol. 563, no. 7732, pp. 465–467, 2018, doi: 10.1038/d41586-018-07449-z.

[15] H. W. Sun, L. Zhang, H. J. Zuo, K. J. Zhang, and C. G. Ma, “Offline Arbitrated Quantum Blind Dual-Signature Protocol with Better Performance in Resisting Existential Forgery Attack,” Int. J. Theor. Phys., vol. 57, no. 9, pp. 2695–2708, 2018, doi: 10.1007/s10773-018-3791-6.

[16] S. Ghernaouti-Hélie and M. A. Sfaxi, “Guaranteerring Security of Financial Transaction by Using Quantum Cryptography in Banking Environment,” Commun. Comput. Inf. Sci., vol. 3 CCIS, pp. 139–149, 2007, doi: 10.1007/978-3-540-75993-5_12.