RESEARCH ARTICLE OPEN ACCESS

A Survey of Various Quantum Cryptography Schemes and Algorithm Implemented in Quantum Cloud Computing

Aditya Palshikar[1]

[1]ABMTC (American Business Management & Technology College) Zug, Switzerland

****

Abstract:

The rising concerns in the security of computing systems has led to development of various new algorithms. The improvement in current computing systems in cloud lead to huge growth in the security systems. Now-a-days as there is an increase in Quantum computing algorithm there is necessity that cloud security systems should adapt the new computing techniques and these techniques are very much useful and unbreakable compared to the traditional computer systems. There are different algorithms and techniques implemented for using quantum computing with cloud. The schemes involved in improving the current computing and security techniques has become a major need for today's technology. There are different shortcomings of cloud computation but we can avoid that using quantum preprocessing of the system because the current entanglement proposed systems will give a better security key architecture. So there is an implementation of quantum cryptography to ensure the transmission of user data in a proper way and to have a good security measure. It will avoid any eavesdropping and some man in the middle attacks which happen in the traditional systems. Here the main aim was to give a brief understanding on these type of systems and how quantum computing actually work in cloud infrastructure..

Keywords — **Cloud Computing, Cloud security, Quantum computer, Quantum Cryptography.**

****

I. INTRODUCTION

There are different advancements in cloud computing techniques. This technology helps in making good services and it also supports in manufacturing process. [1]Security and safety is the major concern which is present now in cloud computing for the passage of information. Usually the old systems were based on some RSA based systems but these systems are not good enough for quantum computers. Now the major need is to have a better systems for the protection of manufacturing systems done by cloud systems against the quantum computer attacks. Here we can propose a different system for encountering the attacks on quantum computing systems for the encryption on cloud. Now-a-days Cloud manufacturing is a big focus on overcoming of the security challenge. Quantum computer is also one of the major inventions for developing the current computer technology. As there are most of the systems developed for securing a system for the cloud manufactured products. [2]There is a design which is implemented on the cloud based environment and then it can be used for protection of communication in cloud manufacturing. There are different manufacturing process bit cloud manufacturing is a very new approach which is done for the advancement of the manufacturing modes. For keeping the information more reliable and much secure there are different authentication protocols which is used for cloud-architecture. There is a vast growth in computer systems with different types of servers and with much better services. The main process is to identify the correct user on a cloud infrastructure anytime when it comes to access. Security is the main obstacle in cloud computing as information is to be secured on a server. [3]And there is a good growth in quantum computers like implementation of quantum cryptography which is used for overcoming the drawbacks of traditional cryptography systems. As there is a lot of improvement in the power of computation these typical or traditional cryptography systems and key management techniques are very prone to the virus attacks, brute force attacks and sniffer software and these software's collect various information of the users that are very confidential. So there has been a practice kept from several decades for initiating the basis for cryptography science in this field of network communication.

And after several practices quantum cryptography has also evolved and it is a very good method for providing the secure communication. [4]There is a Quantum Key Distribution which is used for different practical applications using specific quantum theory. It is validated by the laws of physics and using the quantum cryptographic schemes. Here Quantum Key Distribution will help us to make sure to have proper security as compared to usual cryptographic techniques. [5]The laws of quantum mechanics says that quantum bits cannot be imitated for transmission and then Computational efficiency does not perform the eavesdropper because the key created using the QKD is highly secured. QKD has an ability to detect the eavesdropper which might be observing the data while there is any transmission. So there are different schemes that verifies the user by using some identities to grant access to the cloud services. These schemes have its own advantages and disadvantages like it make a combination of classical identities for authentication of the users. It also inherits the quantum states and the fundamental laws of quantum physics. [6]Cloud computing helps user to have a proper facility to use the resources in a very easy and cost effective manner. And there is a maximum utilization by using these shared resources then it enhances the computation capabilities. Then these capabilities result in shifting all the business to cloud services as it will boost up the process. But cloud computing has its own risks related to security. Organization cannot migrate their all resources, services and assets to third-party service providers. As there are lot of advantages using these services but still it's not much secure. [8]Now also cloud computing is still an early adoption stage of computation. Security only allows legit users to have an access to these sensitive data and for selected persons only there is permissions to access that data. Different challenges and issues has been arisen while having an implementation of the cloud services. As there are privacy concerns like lack of user control and unauthorized access or secondary usage. The record of identity of user should be maintained for the unauthorized and authorized access. [7]To manage these identity and access control is not so easy in the cloud environment because the owner domain and resources are having some controls and whatever the personal information is there cannot be surpassed. If we compare the traditional IT setup then we can see that cloud is very capable to handle users for different organization and too with different authentication. But if there is an employment of different security keys or authorization mechanisms then there can be different situations which will lead to have a security concerns. [9]These services are highly elastic and dynamic and IP address are also reassigned. But cloud needs a dynamic and uncompromising access control schemes so as to prevent any unauthorized access. And it should also check for identity management system to have a proper access of the user and control mechanisms. Protection of Identity is very important for authenticating the right user and following a key-agreement scheme for the single server and multi-server architectures.

So quantum security techniques is very useful for the eavesdropping strategy which is a passive attack in cryptography. There are different attacks like MITM, impersonation attack which can occur and due to this the QKD scheme doesn't that much power for attaining the unconditional security. Conversion of these type of active attacks in quantum key distribution we usually have the classical methods for these type of conversion. [9]To protect the applications from every passive and active attacks then there should be a proper implementation of the

QKD schemes and classical authentication protocol. But the main drawback is that this implementation is not much efficient. It basically degrades the efficiency of the scheme and make security better. So to overcome these things we are using the quantum authentication and key distribution for identifying the correct user.

II. LITERATURE REVIEW

Cloud Computing has allowed more data transfer to the cloud by users for different tasks like storage and other services which are related to cloud. [5]Mostly the data was first encrypted in some format then uploaded to the servers and this method was basically very useful in data and privacy protection. These data has to be retrieved using various methods and the process of retrieval should be fast and effective. Most of the researchers have found solutions on ciphertext retrieval which are based on cloud. There is an asymmetric key proposed which is having a quantum homomorphic encryption and it lets us quantum random walk on encrypted data. Asymmetric data can be used for quantum homomorphic encryption and it has different algorithms involved like key generation algorithm, encryption algorithm, evaluation algorithm and decryption algorithm. We can use this evaluation algorithm for the encryption of the data. But evaluation algorithms are basically depends on secret key, so the working is like first the client needs to upload the key to the server. As Quantum computing the new computing technique which is based on laws of quantum mechanics and it controls quantum information for computation. [6]So for the quantum computational models which has quantum circuits they are having their basics on quantum gates. So quantum circuits deals with some property of teleportation. Quantum teleportation is used for moving the quantum states in the absence of quantum communication channel which is having a sender or receiver. There is one key updating algorithm which is based on some set of communication rules. So quantum homomorphic encryption ciphertext retrieval is a scheme which is based on some search technique and first a search is applied on the ciphertext state then homomorphic ally retrieval process is being done.

Quantum Computer is having a vast storage and processing capacity and it can overcome any drawbacks of traditional computer. So there are entangled states or superposition of the sole quantum systems, and these systems have been described as collection of quantum bits or we can term it as a qubit. [8]There are different challenges related to these systems and one of them are like large quantity of information can be reduced using enormous entangled quantum systems but it is not easily accessed. So quantum computer algorithm guide a state to have a conversion in a simpler form so that it can produce the useful property of the information for its correct measurement. But the main problem is that quantum computers are hard to build and it requires a large number of alone qubits. And we also be needing a good grip on the quantum states. So here the basic idea is that to have a combination of quantum computers and the scientific applications. Various algorithm propose different advantages related to speed compared to the classical systems. It basically works on the quantum interface and entangled states in a way were specifically one or we can say that less quantum states will have a proper amplitude. As there are different manipulation of quantum states which are actually used for defining a quantum algorithm it can be used as different computational modes and along with the entangled superposition.

There are different general requirements for quantum computers hardware like it should consist of physical qubits and it should support coherent manipulation of Hamiltonian control along with gate expressions. [1]As computer architecture are defined using the levels of abstraction or we can term it as a stack it is functioning from the user interface. It also has different levels of quantum computer stack which are not cheap and they are designed in such a way that it is operated with entire stack along with codesigning. As there are different computational problems which are solved using quantum computers algorithms like number factoring and searching unstructured data. It basically get starts with high level of description and then they use a pseudocode. The algorithms are distinguished by using some abstraction and using number of qubits. As quantum algorithms can be conceptualized with a scope that it will outperform the classical algorithm and then we can decide the algorithm can shoot up of near term devices or not. There is a challenge that if they can have determination that algorithms which are used are very feasible for quantum advantage, it basically tells us that whether the algorithm is self-sufficient to compete with the classical algorithms.

III. PROBLEMS IN CURRENT SYSTEMS

As there are different systems on quantum computers which are deployed in cloud and the users are actually using those services by logging in using their normal internet. Nowadays there has been an implementation of Quantum Experience to have a proper access of 5-qubit quantum processor. [3]There are different experimentations done on these systems to have a protocols for quantum error correction, arithmetic and graph theory which are designed in that quantum chip. The experiments tells us that there is a detailed error analysis done to understand the system requirements so there is lot of noise generated while operating these quantum chips there can be a proper refining of these error statistics. But if we are not performing some error analysis then also we can say that experiments are more advantageous to noise and these simulation shows us the variability dependence. [5]As there are different counter measures for the post-quantum algorithms for protection of the cloud manufacturing because of the quantum computer attacks. So the traditional network works on the architectures which are based on RSA and elliptical curves cryptographic systems and these systems doesn't work well on the quantum computers. As there are different systems proposed to achieve confidentiality like post-quantum asymmetric-key encryption scheme for encryption of the message with proper generated session. There is also a post-quantum public-key signature generation mechanisms which can be used for retaining the security. There are some encryption schemes which generates signature and comes up with the post-quantum secure communication system. These designs are implemented on the cloud based environment which has encryption protocol and securing of the decryption system so that it can secure the communication for different users.

Different breakthroughs can be enabled using quantum computing but some of the quantum algorithms only claim to speed up theoretically but practically they are not yet implemented. [8]These algorithms have different challenges. So here the input data has a determination of different number of qubits and specific gates of a quantum algorithm. The implementation has some dependency on the SDK's that restricts the usage of set of quantum computers. [9]As there are limitation regarding the traditional systems then there are challenges regarding the execution of the different quantum algorithms. So to automate a process of selection of the specific quantum computers there are different methods like implementing the analyzers these analyzers are a part of network sharing and for the execution of quantum computer. The code can be analyzed to have a consideration of the properties like error rates, fidelity and connectivity of the qubits. And in our further use-cases there should be a removal of dependencies. Later on there should be a proper plan to have a proper deterministic implementations and approach.

There are tasks involved to have a proper understanding that a quantum cloud computer is running and there is no classical simulation process going on. [9]So the cryptographic verification is very necessary for quantum cloud computing. So there has been an implementation on 5-qubit and 16-qubit processors using some cloud computing architectures which are having concerns to the latest security techniques. The NMR processor is used to verify the scheme with the 1.4% error and using noise compensation implementing with standard techniques. So these all experimentation has led to the single proof-of-principal demonstration of the cryptographic verification scheme by implementing NMR processor. These experimentation shows us that the fidelity of the quantum cloud services is very much appreciated and it has to be improved in a major sense like it should be enabled to have a proper verification methods. There should be a proper connectivity between qubits and it propose an extra implementation overhead of these scheme. There is a strong dependence on the runtime of the systems and it makes it more vulnerable for the impractical attack to happen.

IV. CONCLUSIONS

The proposed methods on cloud computing with implementation of quantum computers have various implementation issues and these has to be overcome as the technology is arising day-by-day and the traditional systems will not work as expected to be worked on like previous security measures and techniques. For now cloud computing is majorly used everywhere and it has some security concerns related to user and the assets. Quantum computer is a very hypothetical concept which is to be used in place of these traditional systems for speeding up the process and have a better architecture as the cloud computing algorithms are working on traditional RSA key generating architectures. As there are security concerns in the systems quantum computers can overcome these difficulties by having a more optimistic illustrations of cloud systems. So there are new methods have been developed like quantum cryptography and blind quantum computing for securing the cloud computing techniques. So for the transmission of the data cryptography methods can be used with quantum computers and it can also be used for authentication of the users. Blind quantum computing can save the users from the eavesdropping or theses methods can be used for the unauthorized access prevention. So the main question arises here is that these systems are secure or not because theoretically the quantum computer can solve major problems using various algorithms and it can also work well on cloud. So the major challenges are only to develop these quantum computing systems and nothing else. It is said that a pure quantum computer can't come into existence as it is not possible to have a full quantum computing algorithms. There should be a proper logic gate implementations to have a control on qubit. But these systems will have major noise problems and there is not an implementation yet involved to go into the subatomic particles level of the systems. If we try to run any paradox of these calculation a single state system phase can't be found. So these are the whole disadvantages of the systems that it's too much ambiguous and quantum cloud computing is also having the same state.

REFERENCES

[1] Salm, Marie, et al. "A roadmap for automating the selection of quantum computers for quantum algorithms." arXiv preprint arXiv:2003.13409 (2020).

[2] Yung, Man-Hong, and Bin Cheng. "Anti-Forging Quantum Data: Cryptographic Verification of Quantum Cloud Computing." arXiv preprint arXiv:2005.01510 (2020).

[3] Wang, Lidong, and Cheryl Ann Alexander. "Quantum Science and Quantum Technology: Progress and Challenges." Am. J. Electr. Electron. Eng. 8.2 (2020): 43-50.

[4] Chen, Xi, et al. "Experimental cryptographic verification for near-term quantum cloud computing." Science Bulletin 66.1 (2021): 23-28.

[5] Rahaman, Mijanur, and Md Masudul Islam. "A review on progress and problems of Quantum Computing as a Service (QCaaS) in the perspective of cloud computing." Global Journal of Computer Science and Technology (2015).

[6] Bijapure, Shahzaib, and Yogita Borse. "A REVIEW ON QUANTUM COMPUTING AS A SERVICE (Qcaas) IN CLOUD COMPUTING."

[7] Devitt, Simon J. "Performing quantum computing experiments in the cloud." Physical Review A 94.3 (2016): 032329.

[8] Alexeev, Yuri, et al. "Quantum computer systems for scientific discovery." PRX Quantum 2.1 (2021): 017001.

[9] Gong, Changqing, et al. "Grover algorithm-based quantum homomorphic encryption ciphertext retrieval scheme in quantum cloud computing." Quantum Information Processing 19.3 (2020): 1-17.

[10] Huang, He-Liang, et al. "Homomorphic encryption experiments on IBM's cloud quantum computing platform." Frontiers of Physics 12.1 (2017): 1-6.

[11] Sharma, Geeta, and Sheetal Kalra. "Identity based secure authentication scheme based on quantum key distribution for cloud computing." Peer-to-Peer networking and applications 11.2 (2018): 220-234.

[12] Lund, Austin P., Michael J. Bremner, and Timothy C. Ralph. "Quantum sampling problems, BosonSampling and quantum supremacy." npj Quantum Information 3.1 (2017): 1-8.

[13] Yi, Haibo. "A post-quantum secure communication system for cloud manufacturing safety." Journal of Intelligent Manufacturing (2020): 1-10.