IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 7, July 2022

DOI: 10.17148/IJARCCE.2022.11704

Secured Cloud Data Storage Encryption Using Post-Quantum Cryptography

Esther S. Alu.[1], Kefas Yunana[2], Muhammed U. Ogah[3]

[1,2,3]Department of Computer Science, Nasarawa State University, Keffi, Nigeria.

Abstract: Cloud computing is evolving daily for securing large data in diverse industries and organizations. The two major challenges about cloud storage are reliability and security. Clients cannot entrust their data to another company without any assurance that they can access their information anytime and no third party will be granted access to it. Data can also be requested from the cloud by the users. However, uploading data in the cloud faces some security issues due to cyber threats and prevalent fraudulent activities. With advancement in technology and research, different solutions have evolved to protect cloud data. Cryptographic techniques utilizing different encryption mechanisms are used to protect the data and ensure its integrity. The existing cryptographic techniques are classical and vulnerable to attacks by quantum computers. In addition, the classical computers utilizes multiple algorithms for encryption and decryption which takes time to encrypt and decrypt a file. In this paper, we presented an optimized new security mechanism using post-quantum cryptography to provide block-wise security to cloud data storage irrespective of the size of the file uploaded or downloaded.

Keywords: Cloud computing, Quantum Cryptography, Cryptographic algorithms, Cloud storage.

1. INTRODUCTION

Globally, a lot of people are using the internet for diverse purposes such as data storage, e-commerce transactions, forex trading, cryptocurrency business, electronic voting, e-governance and other e-transactions. The need for intense security arises due to the prevalence of cyber-attacks in the existing space. The whole world is surrounded by smartphones, laptops and other ICT gadget which consumes data daily. During and after the break of Covid-19, online activities boosted and many individuals and organizations discovered the benefits of operating online without physical convergence. Data is said to be prioritize and needs enhanced protection from attacks, fraudulent activities and unauthorized access.

Cyber security involves the employment of tools and procedures to protect the integrity of computers, software, networks and data against thefts, attacks and risks. Security breaches can occur in various ways like system vulnerability, system failure, theft, unauthorized access etc. Every IoT devices faces the risk of being. Several researches have been carried out improving data security during transmission using different encryption and decryption cryptographic techniques [3]. The study also proposed the use of features like Two Factor Authentication in securing all applications. Intense education should be encouraged by data users as it is pertinent to understand system vulnerabilities and advise various countermeasures accordingly. In the same vein, existing computers employ cryptography techniques which include symmetric-key cryptography and asymmetric key cryptography where keys are used to scramble data for authorized usage only.

Currently, the Rivest Shirma Adleman [14] and Elliptic Curve cryptographic techniques solves algebraic problems with long factorization and complex mathematical computations using both public and private keys in such a way that the private key (secret key) cannot be derived from the public key through brute force attacks in a reasonable amount of time using classical conventional computing. Attacks are computationally expensive and at such rendered ineffective. With the advent of post quantum computing, these underlying assumptions, upon which classical securities are built becomes untrue. Quantum computers can derive the secret key from a public key in a reasonable time frame. With recent technological development and quantum computers, threats of cryptanalytic attacks poses serious impact on the security of computer systems, making traditional cryptographic schemes obsolete. This study proposed a solution to optimize the encryption and decryption mechanisms and to improve the security of conventional cloud data transmission and storage by using quantum-based algorithm. Using quantum cryptography, will protect the data from possible attacks by quantum computers.

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 7, July 2022
DOI: 10.17148/IJARCCE.2022.11704

A. Cloud Storage

Internet has evolved and large data volume keeps accumulating making it difficult for data owners to store such volume of data in a personal computer. However, some users purchase hard drives and other external storage devices to store these large data. As cloud computing continue to advance, cloud storage is an aspect of cloud computing where data are saved to an off-site storage system maintained by a third party. Instead of saving user data/information to the computer's hard drive or other local storage device, it is saved to a remote database with the internet providing connectivity. Cloud storage offers numerous advantages over traditional data storage. For instance, if a user store data on a cloud storage system, the user can gain access to the stored data from any location with internet connectivity. The user does not need to carry his computer or physical storage device from one location to another in order to access the information. Some common examples of cloud storage are google drive, gmail, hotmail and yahoo [16].

A typical cloud computing system experiences a significant workload shift where local computers no longer involve in heavy lifting when running applications. This is handled by network of computers that make up the cloud, reducing user's demand on hardware and software. However, the user's computer needs a web browser and the cloud network to access the cloud [16]. Despite the advantages of implementing data storage in the cloud, the issue of security becomes a concern to every cloud users. The questions are: who owns the data in the cloud and how secured is the storage?

2. RELATED LITERATURES

In 2016, [7] implemented quantum algorithms for data security. The authors also presented a simulation of BBM92 protocol with user interface and real quantum encryption system application with grid computing. The BBM92 quantum protocol was chosen for the analysis due to its proven superior performances with regards to greater speed of the key transmission, due to a longer permitted distance between legitimate users, was simulated by means of a graphical interface that emphasizes the role of Heisenberg uncertainty principle and the concept of quantum entangling used in order to design and implement the quantum distribution of the encryption key.

In 2016, [8] proposed a quantum cryptography security model in mobile cloud computing in order to high data privacy and security. In the proposed model, quantum keys are distributed to users' phones in two phases; Firstly, existing classical optical network has been transformed as quantum distribution network conveniently through multiplexing technique, the BB84 quantum key distribution protocol realized based on decoy state is adopted; Then, the security authentication protocol based on the quantum keys and distance-bounding HKQ was put forward, and through the near field communication (NFC) technology, quantum keys are transmitted into the security storage area of users' phone in the trusted area. Mobile users can get access to data on the cloud through quantum secret keys, protecting users' data and privacy.

Nejatollaji et al. [6] surveyed trends in lattice-based cryptographic schemes, current fundamental proposals for the use of lattices in data security, software and hardware implementation challenges and emerging needs for their adoption. The survey also provided informative idea to allow the reader to focus on the mechanics of the computation ultimately needed for mapping schemes on existing hardware or synthesizing part or all of a scheme on special-purpose hardware.

Shahin and Ahmad [5] proposed a method that utilized quantum key distribution with Kerberos to secure the data on the cloud. The study gave detailed description of the model for quantum key distribution which makes use of Kerberos ticket distribution center for authentication of cloud service providers. The proposed model was compared with quantum key distribution and it was discovered that faster computation with less error rate was achieved.

A. Classical Cryptography

Cryptography is described as the field of science which establishes a connection between parties involved in communication without the third party interference. Some basic features in modern cryptography are Data integrity, authentication, non-repudiation and data confidentiality uses in activates such as e-commerce, Automated teller machines (ATMs), computer passwords and other applications [17]. Classical cryptography involves converting the plain text into scrambled codes various machine learning algorithm. Classical cryptography are broken down into:

1. Symmetrical cryptography– This algorithm uses shared keys for encryption and decryption. In symmetrical cryptography the keys used for encryption and decryption are same [2]. Here, the sender and the receiver utilizes the same secret key to encrypt and decrypt message during transmission. For instance, in a communication between two parties, Alice and Bob, the sender Alice can encrypt a plaintext using her shared private key while Bob can decrypt the

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 7, July 2022

DOI: 10.17148/IJARCCE.2022.11704

message using the same shared key. The key which is also referred to as the secret phrase must be kept secret, meaning that only the two parties involved in the communication (Alice and Bob) should know it. Therefore, the need for an efficient way for exchanging secret keys over communication channels becomes a challenge. However, asymmetric cryptography became necessary to solve the problem of key distribution in symmetric cryptographic techniques. The most famous symmetric algorithms are Data Encryption Standard (3DES) and Advanced Encryption Standard (AES).

2. Asymmetrical cryptography – This belongs to a more complex cryptographic technique that uses key pairs for encryption and decryption. In asymmetric cryptographic algorithm, key pairs cannot be exchanged between the sender and receiver because each party have its own private and public key. For example, in the communication between Alice and Bob analyzed above, if Bob decides to encrypt a message, Alice would have to send her public key to Bob, which Bob can use in encrypting the message. Then, Bob will transmit the encrypted message to Alice who then decrypt the message with her private key (See Figure 1). Hence, the message is encrypted with a public key and only the person in possession of the private key can decrypt the message. With this, asymmetric cryptographic algorithms are less vulnerable to cyber-attacks and users can transmit or communicate messages safely. Despite the existence of both symmetric and asymmetric cryptographic techniques, data breaches keeps rising exponentially, creating limited computational ability and its incapability to handle big data. Although, classical cryptographic algorithms are based on mathematical models and these suffers security backslashes of brute force attack, factorization problem etc. As a result, technological advancement in classical cryptography has proven to be unsafe for data privacy and security. Hence, a transformation towards an emerging technology called Quantum cryptography [2].

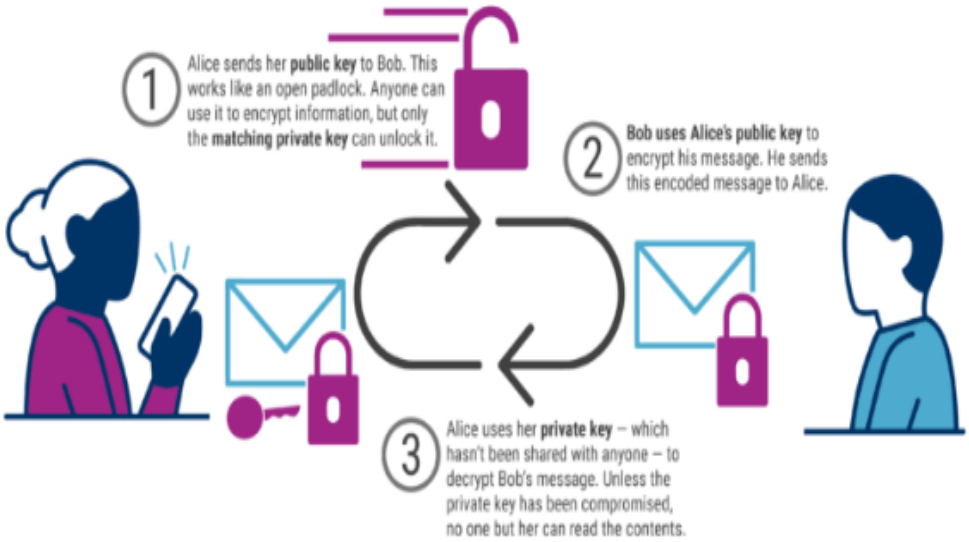

Figure 1: How Public Key Encryption Works [13].

B. Quantum Computing

In the near future, classical computing will be replaced by quantum computing, thereby compromising the confidentiality, integrity and availability (CIA) of computing systems and networks. To prevent data breach, unauthorized access and black hat hacking, there is need for an enhanced cryptosystem called 'Quantum Computing'. Quantum computing theory firstly which was first introduced as a concept in 1982 by Richard Feynman, has been researched extensively as the destructor of the present modern asymmetric cryptographic algorithms. Unlike complex mathematical encryption method, quantum computers uses quantum cryptography which employs the principles of quantum mechanics to encrypt data, making it unhackable. In the discussion in section (2.10 where Alice and Bob has to send messages by utilizing public keys cryptography in classical computers, in this case, quantum cryptography uses the principles of quantum mechanics to send secure messages.

Hence, Alice and Bob who want to send message to each other without any third party interference. With Quantum key distribution, Alice will send Bob a series of polarized photons through a fiber optic cable. Peradventure a third party tries to listen in the conversation between Alice and Bob, he has to read each photon to gain access to the message and pass the same photon to Bob. By reading the photon, the third party alters the photon's state which also introduces errors to the quantum key (See figure 1). Alice and Bob will be alerted that someone is eavesdropping and the key has been infiltrated, so they can discard the key. This means that a photon cannot be read, forwarded or duplicated without being

ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 7, July 2022

DOI: 10.17148/IJARCCE.2022.11704

detected. Thus, Alice will have to send Bob a new key that has not been compromised. The future of cyber security is seeking for the need of unbreakable encryption. With the advent of quantum computers, the integrity of encrypted classical systems are at risk. However, quantum key distribution and other post-quantum cryptographic algorithms offers effective solutions to safeguard all futuristic information.

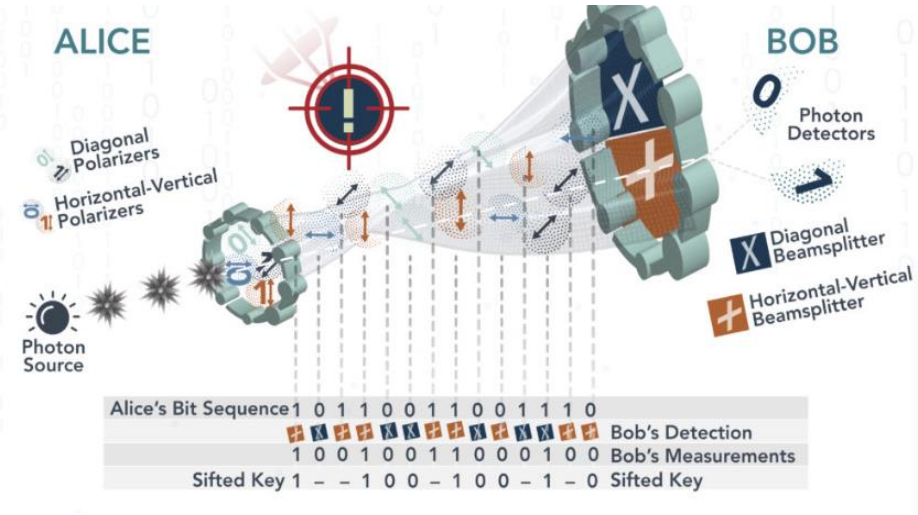

Figure 2: How Quantum Encryption works [15].

C. Post-Quantum Cryptography

Post quantum cryptography implies new classical algorithms that would be designed to be quantum resistant and replace the current public keys scheme. Quantum cryptography is a revolution in the field of network security which utilizes the principles of quantum physics for secure data transmission between sender and receiver [18]. It is the latest and advanced branch of cryptography, whose principles lays on two quantum beliefs: Heisenberg's uncertainty principle and Photon polarization principle [18]. Heisenberg's uncertainty implies that some pairs of physical properties are related in a way that the measurement of one property may hinder the person from knowing the other simultaneously. Particularly, the selection of what direction to measure affects all successive measurements. As a result, when an unpolarized light enters a vertically aligned filter, it absorbs some of the light and polarizes the rest in the vertical direction. A subsequent filter tilted at some angle 'q' absorbs some of the polarized light and transmits the rest, giving it a new polarization [3]. This led to the development of a quantum key distribution protocol called BB84. Quantum encryption utilizes the principles of quantum mechanics to encrypt data, transmit it in a way that cannot be hacked and the decrypt messages encrypted with quantum or classical cryptography. Quantum encryption makes it easy and safe for two parties to communicate with a random common bit sequence which only they can know. The most researched mathematical-based post-quantum cryptographic implementation includes:

i) Lattice-based Cryptography

Lattice-based Cryptography is a recent development in cyber-security which helps to strengthen the existing weak cryptographic measures and undirected security protocols as well as tackling Quantum-Computation, which had been a major challenge over such a time where quantum computers are a reality and can be a resource of misuse too, despite having it wonderful uses [10]. Its construction is based on the presumed hardness of the lattice problems. Lattice- based cryptography describes primitive cryptography that involves lattices in construction as well as security. These constructions based on lattices are currently useful in the auspices of post-quantum cryptography. Lattice-based cryptographic mechanisms pose resistance to classical and quantum computer attacks unlike the most widely used and famous cryptographic mechanisms like PKI (Public Key Infrastructure), ECC (Elliptic Curve Cryptography, Diffie-Hellman etc, all of which are vulnerable to Shor and Grover's algorithm of quantum computers. However, many lattice-based constructions are considerably secured under the speculation that well-studied computational lattice problems cannot be solved efficiently. In a research by [9], the need to generate hard instances of lattice problems arose to improve the security needs was presented. Initially, enhanced security was implemented of which the average-case of several problems in lattice-based cryptography seems equivalent to the worst-case in comparison with other issues [11]. In all, lattices exhibit potentials to avoid the crypto attack launched by any quantum computers i.e Quantum Computationally secure.

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 7, July 2022
DOI: 10.17148/IJARCCE.2022.11704

ii) Multivariate-based Cryptography

Although, the security of current public key algorithms relies on the difficulty of solving systems of multivariate polynomials over finite fields but the development of multivariate equations for encryption algorithm is extremely [13]. Multivariate cryptosystems are considered for encryption and digital signatures. In a work by Tao et al. [73], several asymmetric key encryption schemes were based on multivariate polynomials which makes them insecure due to the fact that certain quadratic linked forms with their central maps exhibit low rank. The authors in [73] also proposed a new efficient multivariate called Simple Matrix which utilizes matrix multiplication to overcome the aforementioned weaknesses. Similarly, multivariate cryptosystems are also necessary for digitals signatures. However, the unbalanced Oil and Vinegar (UOV) types of multivariate quadratic equations and Rainbow are the most effective. UOV also display a large ratio (3:1) between the number of variables and equations, which makes the signatures three times longer than the initial hash values. Consequently, the public key sizes are large while the Rainbow is more efficient because it uses smaller ratios, smaller digital signatures and key sizes [12].

iii) Hash-based Signatures

The Hash-based signature is the Lamport scheme which was invented in 1979 by Leslie Lamport. Buchmann et al. [18]. In a parameter b, the security level of the desired system is defined such that 128-bit b security level will utilize a secure hash function with an arbitrary input length input and produces a 256-bit output length. Thus, yielding SHA-256 as the optimal solution that can be fitted into a message.

D. Applications Of Quantum Cryptography In Cyber Security.

As a result of the advantages present in the quantum computers, public keys encryption like RSA, ECC, Diffie Hellman etc, becomes vulnerable to cyber-attacks. Besides, quantum computers are capable of solving problems such as discrete logarithm problem or integer factorization. Securing the present systems from quantum attacks, it is necessary to integrate different cryptosystems with quantum cryptography [4]. Network security and Cryptography are keys in facilitating the safety of information systems and data upload/download. One major essentials of Cyber security is to explore the quantum cryptographic protocols.

In [4], Quantum information poses the under-listed properties which classical information do not have. Thus;

1. Uncertainty principle: This principle envisage that the position of a particle in the micro-world is difficult to determine and also that the particles position is different in different places.

2. Quantum No-cloning: Cloning describes the ability of an identical quantum particle in a complete different state. It has been proved by the scientists that the Quantum machines can reflect this property. Quantum states also have a feature called as the undeleting property. This means deleting or damaging of a particle in quantum states will leave a trace in Communication systems. Deleting a copy of a quantum state is not allowed by linearity of quantum mechanics [4].

III. PROPOSED SYSTEM

Cloud storage works by utilizing a data server connected to the Internet. With the data server, a user sends file over the Internet and the cloud storage saves a copy. The user can access the data server through a web-based interface to retrieve information. The proposed system is the client-server architecture which is made up of two parts; Client-side which consists of a web application and a 2F-authenticator app; and the Quantum-computer Server-side which involves the encryption and decryption using post-quantum cryptography. The client-side have the web App and an Authenticator App. The user has to enter his registered email address and password after a code is requested in the authenticator app through the 2F authenticator App to access the web application. After registration by the user in the web App, the user is allowed access to the dashboard through which the files can be uploaded. Once the file is uploaded on the server side of the classical computer, the classical public key encryption algorithms are enhanced by a higher cryptographic scheme as against possible attacks by the quantum computers. The quantum-based computer server applies post-quantum cryptographic techniques of dilithium (lattices) digital signature for security against the advent quantum attacks and save it in the database. Upon request by the user for download, the quantum server takes the encrypted file and decrypts it and then sends same back to the user who made the request. Dilithium digital signature is a cryptography based on the hardness of lattice problems, and considered a promising potential replacement of classical cryptography after the eventual emergence of quantum computing. The enhanced encrypted file will be uploaded to the client side as requested.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 7, July 2022

DOI: 10.17148/IJARCCE.2022.11704

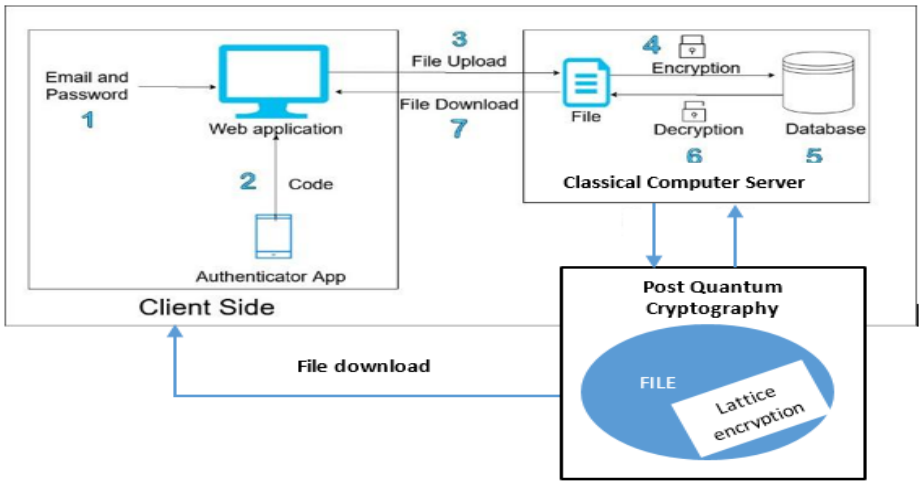

Figure 3: The Proposed Architecture

Lattice-based cryptography belongs to a class of promising post-quantum cryptography family in terms of foundational properties and its application to both traditional and emerging security problems such as encryption, digital signature, key exchange, and homomorphic encryption. The security of the cloud data will be enhanced through the two-factor authentication, public key encryption keys and finally post-quantum encryption using lattice based dilithium digital signature against any occurrences of quantum attacks.

IV. CONCLUSION

With a recent development in IoT, Cloud computing and internet technology, computer systems and its sensitive information are being exposed to cyber-attacks and unauthorized users, compromising the cyber security CIA-TRIAD. This is vehemently creating much attention on new innovations in the aspect of implementing cryptographic paradigms and security measures. Although, previous cryptographic techniques like ECC, RSA, Diffie-Hellman, were difficult to decrypt using classical computation, but with the development of quantum computation, this kind of cryptographic algorithm becomes easy to decrypt for hackers to gain access to sensitive information. Moreover, Cloud computing has become a feasible solution for virtualization of cloud resources, providing many prospective for individuals and organizational benefits. However, security loopholes to outsource data still persist. To ensure the 'security' of data in cloud computing, post-quantum key cryptography was introduced. Post Quantum Cryptography makes use of quantum mechanics and qubits. Post-quantum cryptography, also known as quantum-proof cryptography aim to create new encryption methods that cannot be broken by algorithms, or calculations, that run on future quantum computers. The proposed system is capable of handling any attacks on data integrity and security in cloud data storage.

REFERENCES

[1] Mavroeidis, V., Vishi, K., Zych, M.D and Jøsang, A. The Impact of Quantum Computing on Present Cryptography. (IJACSA) International Journal of Advanced Computer Science and Applications, 9(3). 2018. Department of Informatics, University of Oslo, Norway. Email(s): {vasileim,kamerv,mateusdz,josang}@ifi.uio.no
[2] Gruska, J. (1999). Quantum computing, Citeseer.
[3] Häffner, H., et al. (2008). "Quantum computing with trapped ions. Physics reports. 469(4).155-203.
[4] Zhou, T., et al. (2018). "Quantum cryptography for the future internet and the security analysis." Security and Communication Networks 2018.
[5] Shahin, F. and Ahmad, S.Quantum Key Distribution Approach for Secure Authentication of Cloud Servers. International Journal of Cloud Applications and Computing (IJCAC).11(3). DOI: 10.4018/IJCAC.2021070102
[6] Nejatollahi, H.,Nikil,D.,Sandip, R.,Francesco R, Indranil,B. and Rosario, C.Post-Quantum Lattice- Based CryptographyImplementations:ASurvey.ACMComputingSurveys.5(6).1–41. https://doi.org/10.1145/3292548
[7] Cangea, O., Oprina, C.S and Dima, M.O. Implementing Quantum Cryptography Algorithms for Data Security. International Conference. 8th Edition Electronics, Computers and Artificial Intelligence. Poliesti, Romania.
[8] Hian, J., Liu, Y. and Song, L. Enhancing data and privacy security in mobile cloud computing through quantum cryptography. 7th IEEE International Conference on Software Engineering & Service Science (ICSESS). 2016.

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 7, July 2022

DOI: 10.17148/IJARCCE.2022.11704

[9] Ajtai, M. (1996, July). Generating hard instances of lattice problems. In Proceedings of the twenty-eighth annual ACM symposium on Theory of computing (pp. 99-108). ACM.

[10] Nejatollahi, H., Dutt, N., & Cammarota, R. (2017, October). Special session: trends, challenges and needs for lattice-based cryptography implementations. In 2017 International Conference on Hardware/Software Code sign and System Synthesis (CODES+ ISSS). 1-3. IEEE.

[11] Dadheech, A. (2018, September). Preventing Information Leakage from Encoded Data in Lattice Based Cryptography. In 2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI) (pp. 1952-1955). IEEE

[12] Chun, H., et al. (2017). "Handheld free space quantum key distribution with dynamic motion compensation." optics express 25(6): 6784-6795.

[13] CBInsights. Post-Quantum Cryptography: A Look At How To Withstand Quantum Computer Cyber Attacks. https://www.cbinsights.com/research/post-quantum-cryptography/

[14] Rivest, R.L., Shamir, A. and Adleman, L. A method for obtaining digital signatures and public-key cryptosystems. 1983. Commun. ACM. 26(1). 96–99.

[15] https://quantumxc.com/blog/quantum-cryptography-explained/

[16] Strickland, J. How Cloud Storage Works. 2021. https://computer.howstuffworks.com/cloud-computing/cloud-storage.htm

[17] Ekert, A. Quantum cryptography based on Bell's theorem. 1991. Phys.67. 661.

[18] Gisin, N., Ribordy, G., Tittel, W. and Zbinden, H. Quantum cryptography. 2002. Rev. Mod. Phys. 74.145.

