Review Paper on Post-Quantum Cryptography-Driven Security for Cloud Computing

Krati Vishwakarma (0225CS20MT09, krativishwakarma9@gmail.com)*

*[1](Department of CSE, Global Nature Care Sangathan's Group of Institutions, Jabalpur)

Abstract: Data security in the cloud has been a major issue since the inception and adoption of cloud computing. Various frameworks have been proposed, and yet data breaches persist. Since encryption is the dominant method of cloud data security, the advent of quantum computing implies an urgent need to proffer a model that provides adequate data security for both classical and quantum computing. Thus, most cryptosystems will be rendered vulnerable and obsolete, although some cryptosystems will stand the test of quantum computing. The article proposes a model that includes a type of McEliece cryptosystem, which is proposed to replace Rivest-Shamir-Adleman (RSA) in the quantum computing era to secure access control data and implement N-th variables. Degree Truncated Polynomial Ring Units (NTRU) cryptosystem for securing cloud user data. Simulation of the proposed McEliece algorithm shows that the algorithm has better time complexity than the existing McEliece cryptosystem. Furthermore, the novel modification of S and P parameters further improves the security of the proposed algorithms. Moreover, the simulation of the proposed NTRU algorithm revealed that the existing NTRU cryptosystem had better time complexity when combined with the proposed NTRU cryptosystem.

Keywords: Cryptography, Public-key cryptography, private key cryptography, data security, quantum cryptography

Introduction

With the emergence of cloud computing, the provision of data security through encryption has been a major technique to safeguard data against attackers/hackers [1]. Usually, data exchange is carried out in mediums that are not secure enough, which gives room for the interception of data by intruders [2-4]. According to ref. [4], cloud computing pro- mises enhanced data security, reduced cost for services, enhanced flexibility, and higher availability, but the knowl edge domain shows that frameworks for various data security models have been proffered for enhanced cloud data security using advanced encryption standard (AES), data encryption standard, RSA, and Elliptical Curve Cryptography (ECC), yet data security issues still prevail.

Cryptosystems such as RSA and ECC based on fac toring problems and discrete logarithms, respectively, have sufficiently provided cloud data security for years over all forms of classical attacks. However, today's data- driven society is gradually drifting from classical computting, where information is stored in 0s and 1s to quantum computing, where information is stored in qubits. The advent of quantum processors and hence quantum computing, has revealed potential weakness in existing crypto- systems, thus necessitating the urgent need to source for alternatives that will ensure data protection.

Frequently used Cryptosystems, for example RSA and ECC have sufficiently provided cloud data security for years over all forms of classical attacks, yet the theft of data prevails. Hence, the urgent need to deploy quantum safe cryptosystems that are both safe for data processing in the classical and quantum space.

This article proposes a variant of the Code-based cryptosystems and Lattice-based cryptosystems. It seeks to develop a robust hybrid cloud data security framework with a view to understudy the cryptosystems as mentioned earlier and the designing of a variant of McEliece cum NTRU cryptosystems, respectively, in a hybrid architecture.

Post-Quantum Cryptography

The dominance and recognition of the need for the use of public, key cryptography such as RSA and ECC demanded researchers to find a proficient way for unravelling the factorisation problem and discrete logarithm problem. The unravelling of these hard-mathematical problems will thus provide a breakaway for RSA and ECC security. While researchers have tried to solve the problems with the use of classical computers, Peter Shor in 1994 used a quantum computer to develop and demonstrate an algorithm for efficient factorisation [5]. It is pertinent to note that with the advent of quantum computers, the present security infrastructure cum cryptosystems, where users and internet users rely, will be rendered obsolete and irrelevant [6].

Post-quantum cryptography is a branch of study whose sole aim is to update and provide security for the current cryptosystems with the presence of quantum computers [7]. Research in this branch of study entails studying cryptosystems that make use of the factorization problem and discrete logarithm problem, and remain secured against the two problems even though the hacker/attacker is armed with quantum computing. However, the National Academies of Sciences, Engineering, and Medicines describes quantum computing as the usage of the quantum phenomena (entanglement and superposition) to carry out computation for solving computational problems such as the integer factorisation of the RSA.

Classes of quantum cryptography

There are four major classes of quantum cryptographicalgorithms that resist quantum attacks [8]. These are:

a) Code−based cryptosystems: These categories of crypto-
systems adopt the principle of extracting the initial bits of data transmitted over a channel by encoding the data in a specific structure, which may be recovered to a certain number of errors during transmission. Additional bits of data are added during the encoding of the data to be sent and then decrypted on reception if the specific information about the coding structure is known. An example of the code-based cryptosystem is the McEliece cryptosystem.

b) Lattice−based cryptosystems: Lattice-based cryptosystems are the foremost candidates for public-key post-quantum cryptography [9]. They use multidi- mensional lattices on solving the hardness of certain problems. An example of a lattice-based cryptosys- tems is the NTRU cryptosystem.

c) Multivariate public key cryptosystem: Shehata [6] described multivariate cryptosystems as one that uses random sets of quadratic equations, and the proces- sing of the encryption or decryption uses these equa- tions at particular points.

d) Hash−based cryptography: Is a cryptosystem that uses hash functions to guarantee the integrity of mes- sages. An example is the Merkle's hash-tree public-key signature system.

National Institute of Standards and Technology (NIST) carried outa research to find a solution to the imminent threat of rendering the present cryptosystems obsolete on classical symmetric and asymmetric cryptosystems as regards the emerging quantum computation. Table 1 below presents their findings:

Table 1: Cryptosystems under quantum computation

S no.	Cryptosystems	Current status
1	AES	Large key sizes needed
2	SHA-2	Larger output needed
3	SHA-3	Larger output needed
4	RSA	Broken
5	Deffie–Hellman key exchange	Broken
6	Elliptic curve cartography	Broken
7	Buchmann Williamn Key Exchange	Broken
8	Algebraically homomorphic	Broken
9	McEliece	Not broken yet
10	NTRU	Not broken yet

The security of cloud computing

According to the Organisation of NIST, cloud computingis described as a service model that enables immediate, simple, and on-demand available network access to shared computing resources such as servers, networks, data, appli-cations, and services [10].

There are four cloud computing models: hybrid, public,private, and community clouds. Furthermore, the model also depicts service delivery models, which include Infrastructure-as-a-Service (IaaS), the Platform-as-a- Service (PaaS), and the Software-as-a-Service (SaaS) (Figure 1).
Though it is expected that computing will serve as a utility such as telephone, gas, water, and electricity, it comes with a major challenge: data security problems.Cloud user reception of cloud services can be hindered due to security and privacy issues. Information sourced from the knowledge domain also reveals that cloud users feel reluctant to fully adopt cloud services because of security and privacy issues. Ref. [11] describes data security as a means of securing digital data against unauthorised users/actions. Data sharing is carried outin unsecured channels, which is susceptible to intercep- tion. This has led to cloud providers and clients resorting to various means of data protection techniques, one of such techniques is cryptography.
Additionally, data security encompasses three attributes: confidentiality, integrity, and authentication. Confidentialityentails the protection of information and restricting it fromunauthorised access. This is achieved by the application ofcryptography. Integrity ensures that unauthorised persons are not able to change or manipulate data intended for a specific user and could be achieved by the use of crypto- graphy. It is pertinent to note that data has value only if it is safe. Data which has been manipulated does not have anyvalue and may cause financial waste, for example, data manipulation in which information about financial accountsis stored. Similarly, cryptography plays an important role inensuring data integrity. Frequently used methods of data integrity protection contain information about data changesand hash checksums by which data integrity is verified. Availability simply refers that information be made consistently/readily accessible for authorised parties. Availability also involves properly maintaining hardware, technical infra-structure, and systems that hold and display the information.

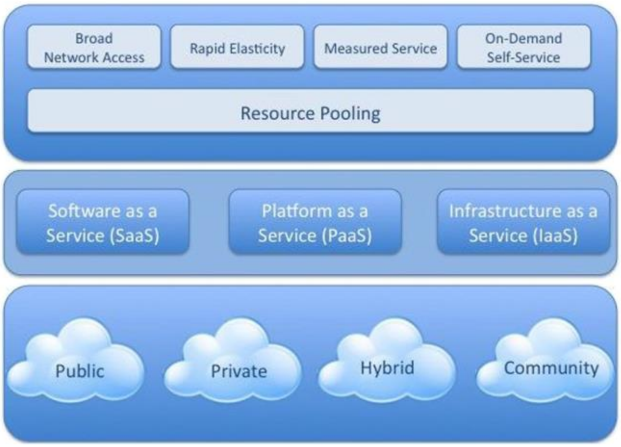


Figure 1: Cloud computing model [31].

Literature review

Ref. [12], proffered a secure framework for a multi-user and multi-owner cloud environment. The authors opined that security, integrity, and privacy of cloud data is the primary threat for cloud deployment in a multi-user/ multi-tenant cloud environment. They further developed an algorithm to address the security issues of the cloud environment and proposed/applied a novel algorithm with the integration of Ciphertext Policy-Identity Attri-bute-based Encryption and the RSA algorithm for securing the cloud. Their research was able to establish a frame- work where both the owners and users are provided with the public and distinct secret keys that are generated by the Automated Certificate Authority. The proposed frame-work was implemented through Java. The performance of the proposed framework was analysed using standard metrices by comparing with the metrics output of Anand and Perumal, 2019 and Xue and Ren, 2019. However, the simulation of various data sizes revealed that the proposed framework is more expedient and effective when com- pared with EECDH and I-CP-ABE algorithms. The study also revealed that the proposed algorithm prevents man- in-the-middle attack. The authors adopted and applied RSA cryptosystem to the model, however, the RSA crypto-sytem is not quantum safe.

Ref. [13] posited that the provision of data confidentiality and integrity of user's cloud data is subject to the provision of an effective security model that provides the mechanism that guarantees prevention of unauthorised access by third parties and a secured communication channel. The authors proposed a security framework that allows cloud users to handle the privacy and integ- rity of their data. The proposed model avails the user the opportunity to security, network usage, privacy, and data storage in the cloud without depending on the cloud pro- vider. The model grants access to authorised and authenticated users to the cloud data, which has been proposed to be encrypted using a variant of AES algorithm. The proposed model was simulated using CloudSim with iFogSim as simulators on Eclipse integrated development environment. Results of the simulation revealed that the proposed model reduces energy consumption, network usage, and delay. Hence, the proposed framework enhances security, minimises resource utilisation, and reduces delay while utilising services of the cloud. The limitation of the study lies in the fact that the AES cryptosystem has key distribution challenges.

Ref. [14] suggested that cryptography is the most well-known technique for data security in a cloud environment. They further posited that cryptographic services in any cloud environment must accommodate authorisa- tion, availability, confidentiality, integrity, and non-repudia- tion. They proposed the implementation of RSA, AES, and SHA256 in data security. The limitation of this mechanism is that it consumes a lot of time during execution. The long keys of RSA means that they incur high computational over-head and RSA cryptosystems are susceptible to quantum attacks. Furthermore, AES suffers from key exchange pro-blem which is a limitation.

Ref. [10] stated that in spite of research works carried out in the area of cloud computing, challenges have per- sisted in the section of load balancing in cloud-based applications directed to the IaaS cloud service model. They postulated that IaaS model is technological driven that manages backend servers and virtual machine. Further-more, they stated that cloud service providers should ensure situations where clients are being overloaded/underloaded to forestall machine failure or higher execution time sug- gesting task scheduling. The scholars proffered an LB algo-rithm directed towards optimising resources and enhancing load balancing considering the quality of service (QoS) task parameters, priority of virtual machines, and resource allocation. Results from their experiment revealed that the proposed LB algorithm had better execution time and make-span when juxtaposed with the Dynamic LBA algorithm.

Table 2: Reviewed literatures

	Methodology	Remark
[15]	The McEliece cryptosystem was subjected to simulation in various extension degrees.	
[16]	Simulated NTRU, RSA, and AES to ascertain the performance of the cryptosystem	
[17]	Used genetic algorithm to determine where data could be stored and adopted the capability list.	
[18]	Used tornado codes and AES cryptosystem for cloud data security	
[19]	Provided an overview of algorithms in lattice-based, super-singular elliptic curves, and code-based, and suggested adopting lattice-based algorithms	

[20]	Proposed adopting an RSA cryptosystem that generates primes in batches.	The private and public keys for the McEliece cryptosystem are very large matrices and consumes time in classical processing NTRU offers better performance when compared to other existing cryptosystems because the mechanism for encryption and decryption is simple
[21]	Applied binary method in Lattice multiplication to ECC cryptosystem	
		Consumes time in identifying the storage location of data
		AES has a simple key management system and encryption Computationally expensive and hence impractical to apply
		RSA cryptosystem will be broken by quantum computing
		ECC increases the size of encrypted data and is not quantum safe
[22]	Proposed hierarchical role for access control encrypted data	The proposed method cannot be applied to
[23]	Applied RNS on NTRU	Any slight modification on the parameters of the framework slows down its computation

Materials and method

The article proposes a framework for an enhanced cloud data security. The proposed framework comprises a variant of the McEliece and NTRU algorithm. Subsequently,

the algorithms are subjected to simulation with standard performance metrics alongside ECC, RSA, AES, and theexisting NTRU and McEliece algorithms using MATLAB. The following subsections present the framework and theresult of the simulation.

The proposed hybrid framework

In the proposed system, as depicted in Figure 3, a block diagram of the proposed framework is shown. McEliece cryptosystem is used to encrypt/decrypt user credentials, while the proposed NTRU is used to encrypt/decrypt user data.

The proposed framework for enhanced data security is presented in Figures 2 and 3 depicts the processes inthe proposed framework. The cloud administrator createsusers such that their user credentials are encrypted/ decrypted using the proposed McEliece cryptosystem. Upon request to access the cloud, users provide their user credentials, which is subjected to authentication. Itshould be noted that the cloud administrator provides users with their credentials. The proposed model also includes the encryption and decryption of cloud data using a variant of the NTRU cryptosystem. The sectionsbelow explain the details of each segment of the model.

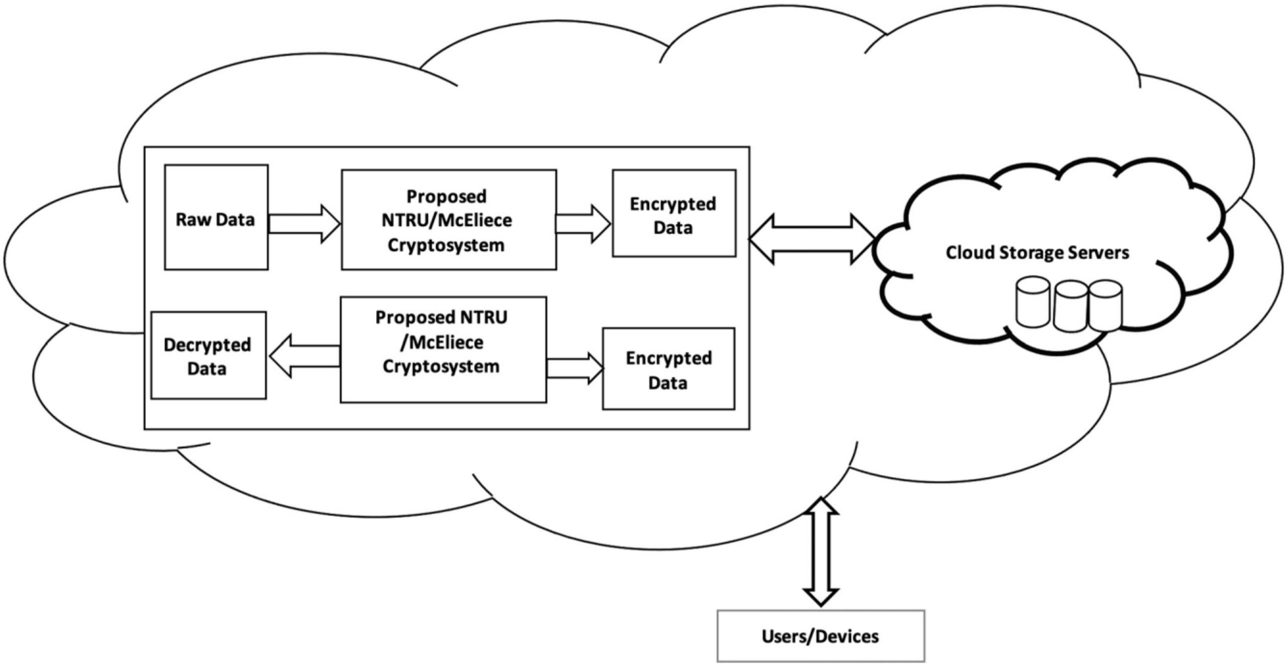
Proposed user verification

The framework proposes the authorisation and authenti- cation of cloud users using onetime password (OTP) authen-tication and user credentials authentication. The figurebelow depicts the processes involved in the authenticationand authorisation of cloud users (Figure 4).

For the proposed data storage/retrieval, an authenticated and authorised user accesses the data that have been stored in the cloud. Data is encrypted using a variant of the McEliece for user credentials and NTRUcryptosystems for user data and then stored/retrieved in the cloud.

Proposed McEliece cryptosystem

In a bid to increase the security of the McEliece crypto- system, the key generation mechanism is strengthened,as shown below.



Conclusion

This article proposes a framework that adopts quantum- safe algorithms to safeguard cloud data. Innovatively, a variant of McEliece cryptosystem was used to safeguard user credentials, while a variant of NTRU cryptosystem was used to safeguard cloud data. The McEliece and NTRU cryptosystems were proposed to provide an efficient data security in the cloud environment amidst the emergence of quantum computing. It is expected that the proposed model will decrease man-in-the-middle attacks and improves data security.

References

[1] M. N. Daodu, A. Gabriel, B. K. Alese, and A. O. Adetunmbi, “Adata encryption standard (DES) based web services security architecture,” *Ann Comput Sci Series, Tibiscus Univ*, vol. 14, no. 2. pp. 53-8, 2016.

[2] B. K. Alese, Deign of public key cryptosystem using ellipticcurve, *Thesis*, Akure, Ondo State, Nigeria, The Federal University of Technology, 2004.

[3] A. F. Thompson, O. E. Oyinloye, M. T. David, and B. K. Alese, “Asecured system of Internet Enabled Host Devices,” *Netw Commun Technol*, vol. 5, no. 1. pp. 26-36, 2020.

[4] A. J. Gabriel, B. K. Alese, A. O. Adetumbi, and O. S. Adewale, “Post-quantum cryptography based security framework for Cloud Computing,” *J Internet Technol Secured Trans*, vol. 4, no. 1. pp. 351–7, 2015.

[5] A. M. Kuo. *Opportunities and Challenges of Cloud Computingto Improve Health Care Services*. 2011. Available at: https:// www.ncbi.nlm.nih.gov/pmc/articles/PMC3222190/. Accessed 02/03/2018.

[6] S. S. S. Shehata, *Post Quantum Cryptography with RandomSplit of St-Gen Codes*, Norwegian University of Science
and Technology, Department of Information Security andCommunication Technology, 2017. Available at: https:// ntnuopen.ntnu.no/ntnu-xmlui/bitstream/handle/11250/ 2450584/16929_FULLTEXT.pdf?sequence=1.

[7] J. Buchmann, and J. Ding, “Post-quantum cryptography”, *Second Int Workshop*, PQCrypto, 2008, pp. 17–9.

[8] L. Chen, S. Jordan, Y. -K. Liu, D. Moody, R. Peralta, R. Perlneret al., Report on post-quantum cryptography, *National Institute of Standards and Technology Internal Report 8105*, 2016. Available at: https://dl.acm.org/doi/proceedings/10. 5555/1473109.

[9] D. Micciancio and O. Regev *Lattice-based cryptography*. 2008. Available at http://cims.nyu.edu. Accessed 28/06/2020.

[10] D. A. Shafiq, N. Z. Jhanjhi, A. Abdullah, and M. A. Alzain, “A load balancing algorithm for the data centres to optimisecloud computing applications,” *IEEE Access*, vol. 9,

pp. 41731–44, 2021, doi: 10.1109/ACCESS.2021.3065308.

[11] G. Summers, Data and databases, *Developing Databases withAccess*, H. Koehne, editor, Nelson Australia Pty Limited, 2004, pp. 4-5. Available at: https://catalogue.nla.gov.au/Record/ 4610312.

[12] S. Chandel, G. Yang, and S. Chakravarty, “RSA-CP-IDABE: asecure framework for multi-user and multi-owner cloud environment,” *Information*, vol. 11, p. 382, 2020.

[13] I. J. Awan, M. Shiraz, M. U. Hashmi, Q. Shaheen, R. Akhtar, and A. Ditta, “Secure framework enhancing AES algorithm in cloudcomputing,” *Hindawi, Security Commun Netw*, vol. 2020,

pp. 1-16, 2020.

[14] M. M. Abdelnapi, F. A. Omara, and N. F. Omra, "A hybrid hashing security algorithm for data storage on cloud com- puting," *Int J Comput Sci Inf Security* (*IJCSIS*), vol. 14, no. 4, pp. 175–181, 2016.

[15] R. Kumar, A. S. Naidu, A. Singh, and A. N. Tentu, "McEliece cryptosystem: simulation and security vulnerabilities," *Int J Comput Sci Mathematics*, vol. 12, no. No 1. pp. 64-81, 2020.

[16] N. Rani, N. Juliet, and S. Arunkumar, "A novel cryptosystem for files stored in cloud using NTRU encryption algorithm," *Int J Recent Technol Eng* (*IJRTE*), vol. 9, no. 1. pp. 2277–3878, 2020.

[17] S. Mall, and K. Saroj, "A new security framework for cloud data", *8th International Conference on Advances in Computing and Communication* (*ICACC*), 2018.

[18] R. Wang, Research on data security technology based on cloud storage, *13th Global Congress on Manufacturing and Management, GCMM 2016*, 2016.

[19] M. Kindberg, "A usability study of post-quantum algorithms", *Master's thesis*, Lund, Sweden, Department of Electrical and Information Technology Lund University, 2017 Retrieved from https://pdfs.semanticscholar.org/8ed3/ 7b0e436e96384bfb14f02ea21c9a9f84ee65.pdf. Accessed 21/09/2020.

[20] D. J. Bernstein, N. Heninger, P. Lou, and L. Valenta, *Post- quantum RSA*, 2017, Available at https://cr.yp.to/papers/ pqrsa-20170419.pdf. Accessed 04/06/2018.

[21] S. Pavithra and S. Baskar, "Lattice based multiplier for WSN applications for ECC," *Int J Trend Res Dev*, vol. 2, no. 6, pp. 21-27, 2015.

[22] P. Zhang, J. Xu, H. Muazu, and W. Mao, "Access control research on data security in cloud computing", *2015 IEEE 16th International Conference on Communication Technology* (*ICCT*), Hangzhou, China, 2015, pp.874–44.

[23] A. Zalekian, M. Esmaeildoust, and A. Kaabi, "Efficient implementation of NTRU cryptography using residue number system," *Int J Comput Appl* (*0975 – 8887*), vol. 124, no. 7. pp. 33–7, 2015.

[24] A. Siam, H. El-khobby, S. Abd Elkader, and M. AbdelNaby, "Enhanced data security model for cloud computing platform,"*Int J Sci Res Science, Eng Technol*, vol. 1, no. 4, pp. 450–460, 2015.

[25] D. V. Kumar, "A hybrid security protocol using python," *Int J Comput Sci Inf Technol Res*, vol. 2, no. 4, pp. 9–16, 2014.

[26] L. Ducas, V. Lyubashevsky, and T. Prest, *Identity-based encryption NTRU lattices*, 2014, https://eprint.iacr.org/2014/ 794. Accessed 28/07/2020.

[27] O. D. Alowolodu, B. K. Alese, A. O. Adetunmbi, O. S. Adewale, and O. S. Ogundele, "Elliptic curve cryptography for securing cloud computing applications," *Int J Comput Appl* (*0975 – 8887*), vol. 66, no. 23, pp. 11–17, 2013.

[28] P. Dhawan, "Data security model for cloud computing," *Int J Res Sci Technol* (*IJRST*) *2013*, vol. No. 2, no. V, pp. 264-271, 2013.

[29] U. P. B. Ivy, P. Mandiwa, and M. Kumar, "A modified RSA cryptosystem based on 'n'

prime numbers," *Int J Eng Comput Sci*, vol. 1, no. 2. pp. 63–6, 2012, ISSN:2319-7242.

[30] S. H. Gill, M. A. Razzaq, M. Ahmad, F. M. Almansour, I. Haq,
N. Z. Jhanjhi, et al., "Security and privacy aspects of cloud com-puting: a smart campus case study," *Intell Autom Soft Comput*, vol. 31, no. 1, pp. 117–128, 2022, doi: 10.32604/ iasc.2022.016597.