Providing a Quantum Attack Resistant Security System for Cloud Computing

Depavath Harinath [1] ,Archana Patil [2], M.V.Ramana Murthy[2a,] Mohd Riyazuddin [3]and Pentyala Sreenivasa Rao[4]

[1]Dept of Computer Science, Ramnath Guljarilal Kedia College of Commerce, Hyderabad, Telangana, India.
mail id ;- harinath.depavath@gmail.com,
[2]Dept of CSE, Rishi MS institute of Engineering and Technology for Women, Hyderabad ,Telangana, India ,
mail id ;- archanbpatil@gmail.com
[2a]Dept. of Mathematics and Computer Science, Osmania University, Hyderabad, Telangana, India.
Mail id :- mv.rm50@gmail.com,
[3]Dept of CSE, KMIT, Narayana guda , Hyderabad, Telangana ,India
mail id ;-riyazuddin17@gmail.com
[4]Dept of Mathematics, ,Indian Institute of Technology, Dhanbad, Jharkhand, India,
mail id :-psrao@iitism.ac.in

***Abstract*— Cloud services have recently gained widespread acceptability in both the private and public sectors around the world. As a result, data storage, distribution, and transmission have expanded dramatically in this technological age. In general, information is exchanged across open channels, which makes it vulnerable to interception. The prospect of a trespasser gaining access to confidential information has been a persistent concern for the Information Technology (IT) industry, resulting in cloud providers and clients adopting and applying various measures to secure cloud data, such as encryption. Therefore, Lattices have emerged as a powerful mathematical tool in the field of cryptography, offering a diverse set of applications ranging from encryption to secure multi-party computation. This paper illustrates lattice cryptography- a NTRU cryptosystem providing a quantum attack resistant security system for cloud computing.**

Keywords—Lattice Cryptography, NTRU Cryptosystem, Cloud Computing, Information Security.

I. INTRODUCTION

Lattice-based cryptography is the generic term for constructions of cryptographic primitives that involve lattices (Lattice can be described as a free abelian group of dimension which spans the vector space.), either in the construction itself or in the security proof. Lattices have many significant applications in pure mathematics, particularly in connection to Lie algebras, number theory and group theory. They also arise in applied mathematics in connection with coding theory, in percolation theory to study connectivity arising from small-scale interactions, cryptography because of conjectured computational hardness of several lattice problems, and are used in various ways in the physical sciences. For instance, in materials science and solid-state physics, a lattice is a synonym for the framework of a crystalline structure, a 3-dimensional array of regularly spaced points coinciding in special cases with the atom or molecule positions in a crystal. More generally, lattice models are studied in physics, often by the techniques of computational physics.

Lattice-based constructions support important standards of post-quantum cryptography. Post-quantum cryptography (PQC), sometimes referred to as quantum-proof, quantum-safe, or quantum-resistant, is the development of cryptographic algorithms (usually public-key algorithms) that are thought to be secure against a cryptanalytic attack by a quantum computer.

Cloud services have recently gained widespread acceptability in both the private and public sectors around the world. This can be linked to the benefits of cloud computing, which cloud providers present to cloud consumers. These benefits include scalability, elasticity, powerful calculations, and lower service costs, despite the fact that data security is one of the roadblocks to mainstream use of cloud services [1]. Reference [3], defines data security as "a method of protecting digital data, such as data stored in a database, from attackers and unauthorised actions of unauthorized users. As a result, data storage, distribution, and transmission have expanded dramatically in this technological age. In general, information is exchanged across open channels, which makes it vulnerable to interception. The prospect of a trespasser gaining access to confidential information has been a persistent concern for the Information Technology (IT) industry, resulting in cloud providers and clients adopting and applying various measures to secure cloud data, such as encryption. Encryption dates back to ancient times, but it was seen as a means of secret communication at the time. However, has evolved in areas such as electronic voting, digital currency, and digital signatures. The most dominant worrisome issue of cloud computing is data security, which specifically involves the safeguarding of sensitive data from uninvited access/users [3]. Reference [4], defines privacy as having prior knowledge of an attack/data breach that is bound to occur and being able to use controls to prevent it/control it from happening. When an intruder intercepts data, the data is safe because it has been encoded, and the intruder is unable to interpret what he or she has intercepted due of cryptography [5]. It's worth noting that, with the introduction of quantum computing, some cryptosystems will no longer be secure, as the science behind quantum computing will render some cryptosystems unsafe or obsolete. Additionally, [30] avers that the advent of quantum computing poses threats to public key cryptosystems currently in use. More importantly, progress has been made in the development of quantum-computing technologies [6].

As a result, the introduction of quantum computers will once again revolutionize the world. Due to the high expenses of creation and maintenance, the first quantum computer is

likely to be held by only a few businesses. Fortunately, customers can apply to use quantum computers for testing their apps or for any other comparable purpose through the usage of cloud services. The fear of quantum computer-assisted cryptanalysis is driving the security community to create new security protocols and methods. These solutions must be resistant to both classical and post-quantum cryptanalysis, as well as adaptable to a wide range of devices.

Post-quantum cryptography research, according to [7], is mostly focused on lattice-based encryption, multivariate cryptography, hash-based cryptography, code-based cryptography, and single elliptic curve isogeny cryptography. The focus of this paper will be on Lattice based cryptography (NTRU). Although, post quantum cryptography has limitations, which include increased key sizes and high cost of deployment [36]. Similarly, as RSA will be rendered obsolete with the development of quantum computing, the NTRU cryptosystem has proven to be an outright successor. Most importantly, NTRU Cryptography has never been known to be broken by a quantum computer, and it has proven to be the most efficient [8]. Cloud data encryption has become an important mechanism to protect data against attackers as cloud computing has grown in popularity (hackers). Typically, information is exchanged across channels that are not sufficiently secure, making it vulnerable to interception [9]. Cloud computing promises increased security, cost savings, flexibility, faster time to market, and availability [10].

Various types of frameworks have been established and applied for modeling the security of cloud data from the beginning stage of data upload, data processing, through the final stage of data storage/download, according to studies carried out and still ongoing in the domain of cloud computing data security. Despite the use of cryptosystems like as symmetry and asymmetric encryption (RSA ECC), data theft continues to be a challenge. This work proposes and implements a variation of the NTRU cryptosystem as a better way of safeguarding and accessing data in the cloud. The NTRU lattice-based cryptosystem is touted to become a viable alternative to RSA and ECC, and is thus based on polynomial multiplication (a property that this study will investigate). This feature allows NTRU to execute quicker than existing cryptosystems. NTRU has a reduced complexity and smaller key size, making it a good modern encryption alternative that can be used in computing (Cloud and Quantum Computing).

II. RELATED WORK

Cryptography is the science of distorting data to make it indecipherable to third parties (hackers), except for the intended person. Cryptography's principal goal is to protect the interests of parties interacting in the presence of adversaries via any type of communication medium. Related works are reviewed so as to identify some of the challenging problems of existing techniques. Also, the limitations of the concluded works of these authors will be identified. The relevant points of these works are documented as follow;

In [33], the authors designed a data security model driven by steganography and cryptography for cloud computing data to address issues which include but not limited to data theft and data manipulation. A four-phase model driven by AES-256 and RSA cryptosystems, LSB steganography technique and identity-based encryption (IBE) was proffered. While the AES is used to encrypt the plain text, RSA is used to encrypt the key generated by AES key and the ciphertext. More so, the asymmetric encryption (RSA and AES-256 cryptosystems) is used for encryption and the encrypted data is concealed in a photo applying the LSB steganography technique. Subsequently, users' strategies are used to back up the outcomes of the decryption procedure. Additionally, with identity-based encryption (IBE), the outcomes of the encryption and decryption are possibly shared and securely transmitted to recipients that are authorized.

In the model proposed in [34], which is multileveled, text files are initially uploaded to the cloud and DES is applied in the first level of encryption and RSA is applied at the second level of encryption. The simulation of the cryptosystems and comparison with the outcome of a similar study [35], revealed that the model enhances data security and has faster processing speed. Although, the limitation of the model is that only text files were used during simulation.

The research in [31] stated that in order to achieve high level security, high security cryptosystems with low processing power must be deployed. The authors proposed BOTRU as a possible alternative to the NTRU cryptosystem. The proposed algorithm uses bi-octonion sub-algebra and structured to be multi-dimensional, that is, there exist the possibility of the encryption of two messages from one source and two independent messages from various sources simultaneously. More importantly, the system's creation of two public keys distinguishes it from other variants of NTRU. The performance of the proposed system was juxtaposed with OTRU of [32], it was revealed based on arithmetic evaluation that BOTRU has a faster processing speed though had a low-security level when likened with the OTRU cryptosystem proposed by [32].

The study in [11], posited that there is need to protect cloud data from invaders in order to preserve its integrity, confidentiality, protection, privacy and procedures required for managing same. The authors proposed to design a New Lightweight Cryptographic Algorithm for Enhancing cloud Data Security. Using a 16 bytes (128-bit) block cipher that uses a 16 bytes (128-bit) key to encrypt data. This is inspired by feistal and substitution permutation architectural methods to improve the complexity of the encryption. The proposed algorithm achieves Shannon's theory of diffusion and confusion by using logical operations, such as (XOR, XNOR shifting, swapping). It also features flexibility in the length of the secret key and the number of turns. The proposed algorithm is faced with a limitation which is, the Feistel architecture has similar encryption and decryption operations, thus making it easier for an intruder to hijack the entire system in times of system compromise.

In [12], a secure framework for a multi-user and multiowner cloud Environment was suggested. The authors opined that security, integrity, and privacy of cloud data is the primary threat for cloud deployment in a multiuser/ 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 Attribute based Encryption (CP-IDABE) and the RSA algorithm for securing the cloud. Their research was able to establish a framework where both the owners and users are provided with the public and distinct secret keys that are generated by the Automated

Certificate Authority (ACA). The proposed framework was implemented through Java. The performance of the proposed framework was analysed using standard metrices though compared with the metrics output of some existing related works. However, the simulation of various data sizes revealed that the proposed framework is more expedient and effective as to when compared with Elliptic Curve Diffie Helman (EECDH) and I-CP-ABE algorithms. The study revealed that the proposed algorithm prevents man in the middle attack. Although the application of the RSA cryptosystem in the proposed framework is a limitation as it will be rendered obsolete with the full deployment of quantum computing.

The research in [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 unauthorised access of third parties and a secured communication channel. The authors proposed a security framework that allows cloud users to handle the privacy and integrity of their data. The proposed model avails a user the opportunity to security, network usage, privacy and data storage in the cloud without depending on the cloud provider. The model grants access to authorized 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, minimizes resource utilization, and reduces delay while utilizing services of the cloud. The limitation of the study lies on the fact that AES cryptosystem has key distribution challenges.

The study in [14], averred that there exist security challenges during key and data distribution among users in an environment where security is not guaranteed. The authors reviewed McEliece cryptosystem with much emphasis on its algorithmic description, implementation and numerous attacks on the cryptosystem. The McEliece cryptosystem was subjected to simulation in various extension degrees and it was revealed that security of the McEliece system increases with increasing extension degrees. They concluded by stating that McEliece will be adopted in the nearest future amidst the advent, adoption and application of quantum computing in various spheres of the computing world. The limitation of their research is that McEliece has large keys and could pose a challenge when storing files.

In [15], a review of existing cloud storage cryptosystems was carried out. It was observed that, RSA and AES were used mostly used by cloud providers to secure data. They proffered the application of NTRU cryptosystem in the storage of cloud data. The authors further subjected their proposal to simulation. The experiment, juxtaposed NTRU against RSA and AES, results revealed that NTRU showed a faster processing time for encryption and decryption against other cloud storage cryptosystems. They posited that the application of NTRU offers better performance when compared to other existing cryptosystems reasons been that the mechanism for encryption and decryption is simple.

Ramkumar and Gunasekaran in [16], researched on preserving security using crisscross AES and FCFS scheduling in a cloud computing environment. The authors established the need to model a data security framework for efficient ordering of work to be implemented in a cloud computing environment. The specific objective of the research was to enhance efficiency and data security by using the crisscross AES and collocate FCFS. They applied the proposed crisscross AES and collocate FCFS to a cloud computing environment. The research established the use of scheduling in a cloud computing environment to enhance system efficiency. The application of AES will result to key distribution problem and the application of scheduling implies more computational cost.

The study in [23], opined that the security issues under cloud computing is a major problem in the era where the security of a user's data is of utmost priority. The authors proposed a security model for cloud computing that ensured the security and integrity of cloud user data by applying cryptography. They further stated that in addition to data security, the other challenges faced in cloud computing include; malicious insiders, data breaches and loss, hypervisor vulnerabilities, account or service hijacking and denial of service. They adopted and applied the combination of a symmetric algorithm (AES), XOR operations and message digest with a central key distribution center (CKDC) that stored keys generated for data security. However, the limitation of the approach is that XOR operations are reversible, which could expose the keys and AES cryptosystem is susceptible to quantum attacks.

An overview of algorithms in lattice-based, super-singular elliptic curves and code-based, as well as a comparison and evaluation of existing implementations of such algorithms was reported in [17]. The metrics used for comparison includes, security performance and implementation of the selected algorithm. The metrics used for each algorithm had its advantage and disadvantage, thus to choose the best algorithm, the requirements of the application were considered. The research discovered that the lattice-based algorithms provided the best trade-off between speed, key size and memory consumption, and is easy to implement. The limitation of this study lies on the fact that lattice-based cryptosystems are computationally expensive and hence impractical compared to conventional cryptosystems.

The study in [8], proposed a variant of RSA, whose parameters are feasible in the present-day computers and quantum computers. They carried out performance analysis by introducing a new algorithm to generate primes in batches and proposed a quantum factorisation algorithm that is faster than Shor's algorithm, which is much faster to execute than pre-quantum algorithms. Initial *pq* RSA implementation results were provided. The limitation of the method is that the approach may not be practicable as RSA cryptosystem will be broken by quantum computing in the nearest future. Furthermore, on classical computers, there is computation cost in the key generation, encryption and decryption processes for the RSA algorithm.

The study in [18], researched on the need to proffer a framework that is in four levels for cloud computing. They posited that the standard cloud storage uses a three-level data security model in cloud processing and could be extended to a fourth level with the sole responsibility of data integrity check. Their objective was to design a four-level data security model that will handle data integrity check and

applied Petri Nets on each level of the proposed data security model for cloud computing. Petri Net possess concurrency of operations consequently increasing complexity, which is a limitation of the proposed model.

The article in [19], suggested t hat cryptography is the most prominent technique for the security of data in a cloud environment. They further posited that cryptographic services in any cloud environment must accommodate authorization, availability, confidentiality, integrity, and non-repudiation. They proposed the implementation of RSA, AES and SHA256. 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 overhead and RSA cryptosystems are susceptible to quantum attacks. Furthermore, AES suffers from key exchange problem which are limitations.

The article in [20], posited that the efficiency of ECC depended on point multiplication and the lattice multiplication operation could be applied to it, suggesting that ECC is efficient but most suitable for environments where keys of small size could be applied. They further stated that wireless sensor networks is the best area where ECC is to be applied, which enhances wireless devices to perform end to end secure communication efficiently. They presented methods that could be used for lattice multiplication operation and proposed the use of binary method in Lattice multiplication suggesting that it promotes the speed and accuracy of the multiplication. They presented simulation results that validated the proposed method and analysis. Despite the fastness in execution of the binary method in lattice multiplication, the limitation of the proposed scheme is that ECC increases the size of encrypted data. Additionally, the ECC algorithm is complex to deploy, increasing the chances of implementation errors thus this affects the security of the algorithm.

The research by [30] revealed that a lot of post quantum solutions are been developed and submitted to National Institute of Standards and Technology (NIST) for onward standardisation and possible deployment. The study also implemented NTRU cryptosystem on an embedded system. Using a python driven development framework for the design. evaluation was carried out based on speed and consumption of resources metrics. The experiment carried out revealed that operations using the python+C programming enhanced performance ranging from 130 to 450 depending on the scenario in the application of the algorithm.

The study by [37] portrayed a technique for data security in the cloud. The authors also presented various techniques and characteristics for big data cloud computing and stated some of the challenges of data security. The authors presented a virtualization technique for safeguarding data in the cloud. However, the study did not simulate the proposed technique and make comparison with similar techniques. Thus, its level of efficiency could be established.

III. PROPOSED SYSTEM DESIGN

The proposed NTRU cryptosystem was applied to the data that will be stored in the cloud. Below is a conceptual architecture for the security of data stored in the cloud.

Quantum attack-resistant crypto schemes such as those that are based on code, hash, multivariate quadratic polynomial or even the lattice (NTRU) cryptosystems are tipped to become alternatives to RSA and ECC [21-24]. Thus, this current study seeks establish if NTRU will be faster in execution when compared to other cryptosystems [25] and [26]. NTRU possess lower complexity and smaller key size which makes it a good alternative for modern cryptography, hence adoptable to computing (Classical and Quantum Computing).

The following variables are used in processing the encryption/decryption of the NTRU cryptosystem;

N - the polynomials in the ring *R* with degree *N-1*.

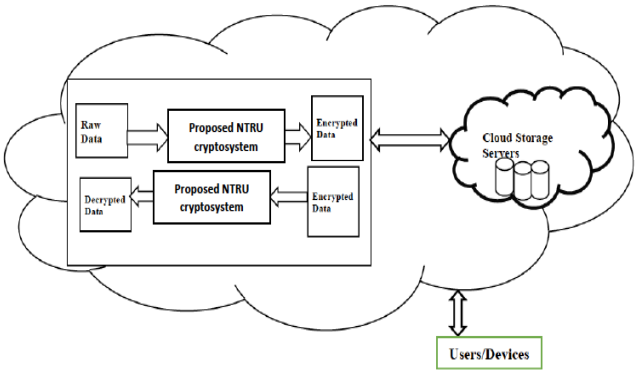


Figure 1. Conceptual Architecture of the proposed cloud data security framework

q - the large modulus, which is used for the reduction of coefficients.

p - the small modulus, which is used for the reduction of coefficients.

f - a component of the private key, which is represented in polynomial form.

g - a polynomial used to process the public key h from f

h - is a polynomial

r - a random blinding polynomial used to distort data

m- is the message to be encrypted represented in polynomial form.

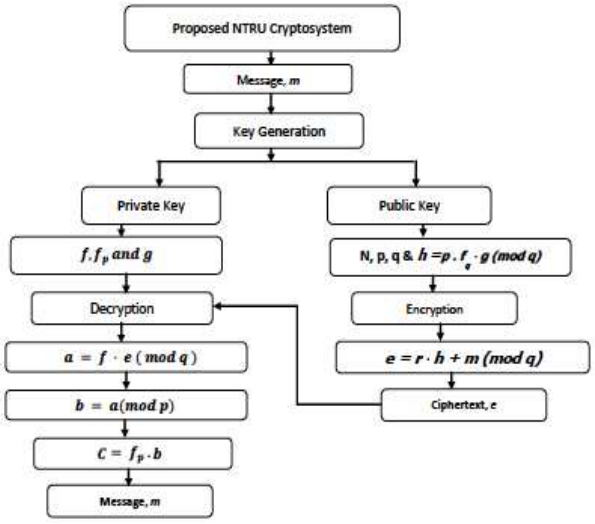


Figure 2. The flow in the proposed Lattice-based NTRU cloud data security system

A. Key Generation in the proposed system

The sender computes $f \cdot f_p=1(mod\ p)$ and $f \cdot f_q=1(mod\ q)$ and then processes the public key h using:

$$h=p.f_q.g\ (mod\ q) \quad (1)$$

The above equation 1 is computed using lattice multiplication

B. Data Encryption in the proposed systemt

To encrypt a message, the sender following is processed:

$$e=r.\ h+m\ (mod\ q) \quad (2)$$

C. DataDecryptionintheproposedsystem

The following is computed to decrypt the message

$$a=f\ .\ e(moq\ q) \quad (3)$$

$$b=a(mop\ p) \quad (4)$$

$$C=f_p\ .b \quad (5)$$

The above equation 1, 2, 3 4 and 5 is computed using lattice multiplication.

D. Implementation of the Proposed System

To verify the efficiency of the suggested algorithm, symmetric and asymmetric cryptosystems were chosen. Various data sizes were simulated against four algorithms (RSA, ECC, AES, and NTRU), as well as the proposed algorithm, with the sole purpose of determining the throughput of the encryption and decryption execution time of the data used and determining whether the proposed algorithm is a better way of safeguarding cloud data.

On a Mac OS computer with an Intel Core i5 processor, 8GB of RAM, and 250GB of hard disk space, the simulation was run with MATLAB.

Table1:Time Taken for The Generation of Private Key

Input File Size (KB)	ECC(s)	AES(s)	RSA(s)	Existing NTRU(s)	Proposed NTRU(s)
20	0.000191	0.000109	0.00000048	6.1037757	7.1810455
77	0.000193	0.000097	0.00000095	6.2219977	6.8497849
153	0.000189	0.000100	0.00000072	6.2695474	6.9003048
283	0.000185	0.000094	0.00000072	6.1897840	6.8672769
305	0.000180	0.000114	0.00000072	6.2266142	6.8146033
Average time(s)	**0.000188**	**0.000103**	**0.00000072**	**6.202344**	**6.9226031**

Table2.TimeTakenforTheGenerationofPublic Key

Input File Size(KB)	ECC(s)	AES(s)	RSA(s)	Existing NTRU(s)	Proposed NTRU (s)
20	0.000220	0.000109	0.000002	6.103776	7.181046
77	0.000222	0.000097	0.000002	6.221998	6.849785
153	0.000219	0.000100	0.000003	6.269547	6.900305
283	0.000214	0.000094	0.000002	6.189784	6.867277
305	0.000209	0.000114	0.000002	6.226614	6.814603
Average time(s)	**0.000217**	**0.000103**	**0.0000023**	**6.202344**	**6.922603**

Table3.TimeTakenforTheEncryptionProcessof Various Cryptosystems

InputFileSize(KB)	ECC (s)	AES (s)	RSA (s)	ExistingNTRU(s)	Proposed NTRU(s)
20	0.0097	0.3122	0.0753	320.8390	564.1053
77	0.0080	0.2490	0.7298	1319.4852	2339.64560
153	0.0119	0.2537	0.5514	2616.9852	7724.5771
283	0.0228	0.2471	0.0228	4898.3393	11570.9521
305	0.0181	0.2490	0.7932	5268.4621	37354.0916
Average time(s)	**0.0141**	**0.2622**	**0.4345**	**2884.8222**	**11910.6744**

Table 4.Time Taken for the Decryption Process of Various Cryptosystems

File Size(KB)	ECC(s)	AES(s)	RSA(s)	Existing NTRU(s)	Proposed NTRU(s)
20	0.0032	0.2415	0.0820	477.9566	1446.2688
77	0.0052	0.2383	0.4338	1911.9348	5822.7922
153	0.0096	0.2506	0.7058	3931.4452	11834.1894
283	0.0161	0.2514	1.4746	7313.5120	32812.9468
305	0.0167	0.2780	1.5585	32157.8710	
Average time(s)	**0.0102**	**0.2520**	**0.8509**	**9158.5439**	

Table 5: Total Average Execution Time of Various Algorithms

	ECC	AES	RSA	Existing NTRU	Proposed NTRU
Private Key Execution Time	0.0002	0.0001	0.0000	6.2023	6.9226
Public Key Execution Time	0.0002	0.0001	0.0000	6.2023	6.9226
Encryption Execution time	0.0141	0.2622	0.4345	2884.822	11910.6744
Decryption Execution Time	0.0102	0.2520	0.8509	9158.5439	22458.0793
Total Execution Time	0.0247	0.5144	1.2854	12055.7708	34382.5989
Throughput (KB/S)	33919.0879	1629.1607	651.9196	0.0695	0.02435

The deductions from the simulation carried out are arranged based on the time taken to generate private key, public key, encryption and decryption.

E. Private Key Generation time

Figure 3.Average Private Key Generation

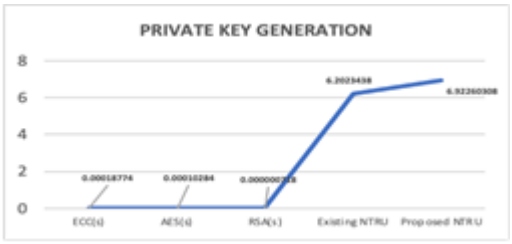


Figure 3 shows the average time it takes to generate the private key for ECC, RSA, AES, existing NTRU and Proposed NTRU.

Equally, regards to NTRU algorithms, it can be deduced from the foregoing that the proposed NTRU cryptosystem takes more time to generate the private key while existing NTRU cryptosystem takes lesser time, this could be as a result of the lattice arithmetic approach, which was introduced in the computation proposed in the NTRU algorithm or the hardware used for the simulation.

F. Public Key Generation time

The Figure below shows the average time it takes to generate the public key for ECC, RSA, AES, exiting NTRU and Proposed NTRU.

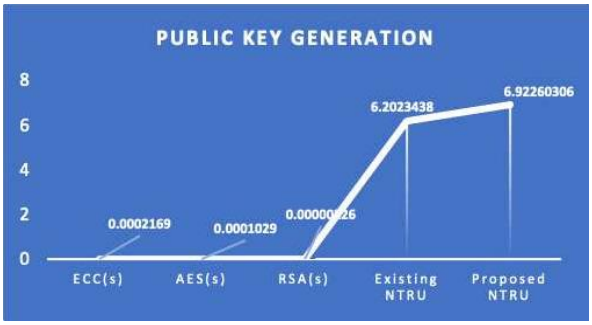


Figure 4.Average Public Key Generation

Similarly, as regards to NTRU algorithms, it can be inferred from the above Figure above that the existing NTRU cryptosystem takes lesser time to generate the key as against the proposed NTRU cryptosystem which takes more time. The lesser time that the proposed NTRU takes could be as a result of introduction of lattice arithmetic that this study introduced to the processing of NTRU as against the polynomial arithmetic, which the existing NTRU algorithm dwells on.

G. Encryption Time

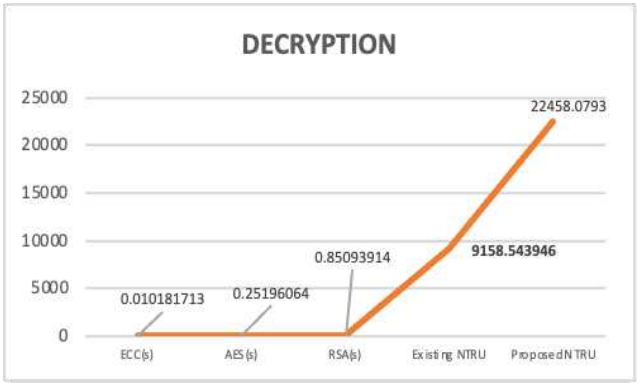
Figure 5 below depicts the average encryption time for ECC, RSA, AES, existing NTRU and Proposed NTRU.

Figure 5: Average Encryption time

With respect to NTRU algorithm, it canbe inferred from Figure 5, that the proposed NTRU cryptosystem takes more time to encrypt while the existing NTRU cryptosystem takes lesser time. The more time that the proposed NTRU takes could be as a result of introduction of lattice arithmetic that drives the encryption process. Thus, the proposed NTRU takes more time to encrypt data.

H.. DecryptionTime

The Figure below depicts the average decryption



time for ECC, RSA, AES, existing NTRU and Proposed NTRU.

Figure 6: Average Decryption time Generation

In respect to NTRU algorithms, it can be deduced from the above Figure that the proposed NTRU cryptosystem takes more time to decrypt while the existing NTRU cryptosystem takes lesser time. The more time that the proposed NTRU takes could be as a result of introduction of lattice arithmetic that drives the decryption process.

I. ThroughputoftheAlgorithms

The throughput is computed based on the private and public key computation; and also, encryption and decryption execution times of the algorithms.

Figure 7: Execution throughput

Figure 7 above shows that ECC has the best throughput, however, the existing NTRU algorithm has a better throughput when compared with the proposed NTRU algorithm.

J. Power consumption of various cryptosystems

If the throughput is calculated correctly, the higher the throughput of a cryptosystem's time complexity, the lower the power consumption [27-29]. As a result, execution throughput is proportional to power consumption. From the Figure 7 above, it can be inferred that ECC has the lowest power consumption. The existing NTRU, on the other hand, consumes less power than the proposed NTRU.

IV. COMPLEXITY OF THE ALGORITHM

Algorithmic complexity is a measure of how long it would take an algorithm to complete a given n-dimensional input. Even with huge values of *n*, a scaling method should compute the result within a finite and reasonable time bound. As a result, as *n* approaches infinity, complexity is estimated asymptotically. While complexity is normally measured in terms of time, it can also be measured in terms of space, which corresponds to the memory requirements of an algorithm. When comparing algorithms or looking for improvements, it's useful to look at their complexity. Computational complexity theory is an area of theoretical computer science that deals with algorithmic complexity. It's vital to note that the paper is only interested in the time complexity order of an algorithm.

A. Time complexity for the Proposed NTRU algorithm

For the computation of the time complexity for the key generation of the proposed NTRU, the computations in the algorithm is considered which is shown below.

i. Complexity of the proposed NTRU Key Generation process

Complexity for modulus arithmetic is $O(n^{1/2})$

Process1---Time Complexity for modulus lattice multiplication = $O(n^3)$

Process2--- Time Complexity for modulus lattice multiplication = $O(n^3)$

Process3---Time Complexity for modulus lattice multiplication = $O(n^3)$

Process 4 --Time Complexity of retuning the output = $O(n)$

Hence, the time complexity for the key generation considering the highest complexity is $O(n^3)$.

Proposed NTRU-Encryption

Input: Parameters for encryption (m,r,h,q)
Output: Cipher Text (e)
Begin
i. Compute $e = r \cdot h + m \pmod q$
ii. Return (e)
End

ii. Complexity of the proposed NTRU Encryption process

Complexity for modulus arithmetic is $O(n^{1/2})$

Process1—Time Complexity for computing the modulus lattice multiplication = $O(n^3)$

Process 2 --Time Complexity of retuning the output = $O(n)$
Hence, the time complexity for the encryption considering the highest complexity is $O(n^3)$.

iii. Complexity of the proposed NTRU Decryption process

Proposed NTRU-Decryption

Input: Parameters for encryption (e,f,p,q)
Output: Plain Text (c)
Begin
i. Compute $a = f.\ e \pmod q$
ii. Compute $b = a \pmod p$
iii. $C = f_p.\ b$
iv. Return (c)
End

Complexity for modulus arithmetic is $O(n^{1/2})$

Process 1: Time Complexity for modulus lattice multiplication = $O(n^3)$

Process 2: Time Complexity for modulus lattice multiplication = $O(n^3)$

Process 3: Time Complexity for lattice arithmetic = $O(n^2)$

Process 4: Time Complexity of retuning the output = O(n). Hence, the time complexity for the Decryption considering the highest complexity is $O(n^3)$.

Finally, time Complexity of the Proposed NTRU Algorithm = Time complexity for (Key generation + encryption + decryption) = $O(n^3) + O(n^3) + O(n^3) = 3O(n^3)$. Upon eliminating constants, the time complexity of the proposed NTRU algorithm is $O(n^3)$.

Proposed NTRU-Key Generation

Input: Parameters for encryption (p,f,g,q)
Output: Keys (h)
Begin
i. Compute $f \cdot f_p = 1 \pmod p$ and
ii $f \cdot f_q = 1 \pmod q$
iii. $h = p.\ f_q \cdot g \pmod q$
Return (h)
End

Zalekian et al. in [26], opines that the NTRU algorithm requires approximately $O(N^2)$ operations. However, the proffered algorithm suggested by this study requires approximately $O(N^3)$ operations. Hence, it can be stated that the existing NTRU has a better time complexity when compared with the proposed NTRU algorithm which is mainly as a result of the lattice multiplication operations.

VII. CONCLUSION

Cloud services have recently gained widespread acceptability in both the private and public sectors around the world. As a result, data storage, distribution, and transmission have expanded dramatically in this technological age. In general, information is exchanged across open channels, which makes it vulnerable to interception. The prospect of a trespasser gaining access to confidential information has been a persistent concern for the Information Technology (IT) industry, resulting in cloud providers and clients adopting and applying various measures to secure cloud data, such as encryption. Therefore, Lattices have emerged as a powerful mathematical tool in the field of cryptography, offering a diverse set of applications ranging from encryption to secure multi-party computation.

This paper proposes a variant of NTRU cryptosystem with the focus to establish its fastness and security in a cloud environment. The proposed variant was simulated together with NTRU, RSA, AES and ECC cryptosystems to establish the time complexity of the algorithms in regard to key generation, encryption and decryption. The simulation showed that as in terms of the private and public key generation, the RSA cryptosystem showed to consume the least time (average). The simulation revealed that the existing NTRU cryptosystem has a better time complexity compared to the proposed NTRU cryptosystem. The existing NTRU cryptosystem has a time complexity of $O(n^2)$ while the proposed variant has $O(n^3)$. Though had a better capacity of handling large data because of the introduction of lattice multiplication. In terms of key generation, comparing the existing and proposed NTRU cryptosystem, the existing NTRU cryptosystem proved to be more efficient for private and public key generation. More so, as regards encryption and decryption, the existing NTRU cryptosystem proved to be more efficient. The proposed NTRU cryptosystem has a lower throughput when compared with the existing NTRU algorithm which proposes that the existing NTRU has lower power consumption.

Therefore the introduction of lattice arithmetic to drive the processing of the existing NTRU cryptosystem via simulation has proved not to be effective.

REFERENCES

[1] M. Marwan, A. Kartit, and H. Ouahmane, (2017), "A Secured Data Processing Technique for Effective Utilization of Cloud Computing", Journal of Data Mining and Digital Humanities. Special Issue on Scientific and Technological StrategicIntelligence.

[2] G. Summers, (2004). Data and databases. In: Koehne, H Developing Databases with Access: Nelson Australia Pty Limited. p4-5.

[3] A. J. Gabriel, B. K. Alese, A. O. Adetunmbi, O. S. Adewale (2015), "Post-quantum crystography based security framework for Cloud Computing", Journal of Internet Technology and Secured Transactions Vol 4 Issue 1 351-357.

[4] T. Sanamrad, (2014), "Encrypting Databases in the Cloud, Threats and SolutionsETH Zurich, Switzerland".http://e-collection.library.ethz (Access DateL 15 November, 2021).

[5] S. Xue, and C. Ren, (2019),"Security Protection of System Sharing DatawithImproved CP-ABEEncryption Algorithmunder CloudComputingEnvironment",Autom.ControlComput.Sci.53, 342–350.

[6] H. Huang, Y. Zhao, T. Li, F.Li, Y.Du, F. Xiang-Qun S. Zhang, X. Wang, and B. Wan-Su,(2016), "Performing Homomorphic Encryption Experiments on IBM's Cloud Quantum Computing Platform", Available at: https://arxiv.org › cs. (Access Date: 2 April 2021).

[7] D. J. Bernstein, J., Buchmann, and E. Dahmen, (2009). Introduction to post-quantum cryptography. (Introductory chapter to book "Post-quantum cryptography"). Springer, Germany.

[8] D. J. Bernstein, N. Heninger, P. Lou, and L. Valenta, (2017), "Post-quantum RSA", Available at: https://cr.yp.to/papers/pqrsa- 20170419.pdf. (Access Date: 4 June2018).

[9] A. Thompson, O.E. Oyinloye, M.T. David, and B.K. Alese, (2020), "A Secured System for Internet Enabled Host Systems. Network and Commination Technologies", Vol. 5, No 1. DOI: 10.5539/nct.v5n1p26.

[10] A. M. Kuo, (2011), "Opportunities and Challenges of cloud computing to improve health care services", https://www.ncbi.nlm.nih.gov/pmc/articles/pmc3222190/. (Access Date: 2 March2018).

[11] F. Thabit, S. Alhomdy, S., Abdulrazzaq, H. A. Ahdal, and S. Jagtap, (2021), "A new lightweight cryptographic algorithm for enhancing data security in cloud computing",Global Transitions Proceedings.

[12] S. Chandel, G. Yang, and S. Chakravarty, (2020), "RSA-CP- IDABE: A Secure Framework for Multi-User and Multi-Owner Cloud Environment", Information. 11, pp 382.

[13] I. J. Awan, M. Shiraz, M. U. Hashmi, Q. Shaheen, R. Akhtar, and A. Ditta, (2020), "Secure Framework Enhancing AES Algorithm in Cloud Computing", Hindawi, Security and Communication Networks. Volume 2020, https://doi.org/10.1155/2020/8863345.

[14] R. Kumar, A. S. Naidu, A. Singh, and A. N. Tentu (2020), "McEliece cryptosystem: simulation and security vulnerabilities", Int. J. Computing Science and Mathematics, Vol. 12, No. 1 pp 64– 81.

[15] N. Rani, N. Juliet and S. Arunkumar (2020), "A Novel Cryptosystem for Files Stored in Cloud using NTRU Encryption Algorithm"International Journal of Recent Technology and Engineering (IJRTE). 2277-3878 Volume-9 Issue.

[16] K. Ramkumar, and G. Gunasekaran, (2019), "Preserving security using crisscross AES and FCFS scheduling in cloud computing", Int. J. Advanced Intelligence Paradigms, Vol. 12,Nos. 1/2.

[17] M. Kindberg, (2017), "A usability study of post-quantum algorithms", A Masters thesis submitted to the Department of Electrical and Information Technology, Lund University.

[18] Z.Balogh,andM.Turcani,(2016),"ModelingofData Security in Cloud Computing", Available at: https://www.researchgate.net/publication/319509441

[19] M. Abdelnapi, F. A. Omara, and N. F. Omran (2016), "A Hybrid Hashing Security Algorithm for Data Storage on Cloud Computing", International Journal of Computer Science and Information Security (IJCSIS), Vol. 14, No. 4.

[20] S. Pavithra, and S. Baskar, (2015), "Lattice based Multiplier for WSN Applications for ECC", International Journal of Trend in Research and Development, Vol. 2(6).

[21] A. J. Gabriel, B. K. Alese, A. O. Adetunmbi, O. S. Adewale, (2013),"Post-Quantum Crystography: A Combination of Post- QuantumCryptography and Steganography".The8th International Conference for Internet Technology and Secured Transactions (ICITST-2013), Technically Co-sponsored by IEEE UK/RI Computer Chapter, 9th-12th December 2013, London, UK, pp454-457.

[22] A.J.Gabriel,A.Darwish,A.E.Hassanien(2021),"Cyber SecurityintheAgeofCOVID-19",In:HassanienA.E.,Darwish A. (eds) Digital Transformation and Emerging Technologies for Fighting COVID-19 Pandemic: Innovative Approaches. Studies in Systems, Decision and Control, vol 322. Springer, Cham.

[23] H. C. Ukwuoma, A. J. Gabriel, A. F. Thompson and B. K. Alese, (2021),"Optimised Privacy Model for Cloud Data," 2021 16th International ConferenceonComputerScienceand Education (ICCSE), 2021, pp. 267-269, DOI: 10.1109/ICCSE51940.2021.9569395.

[24] A.J.Gabriel,B.K.Alese,A.O.Adetunmbi,O.S.Adewale, O. A. Sarumi (2019). "PostQuantum Crystography System for Secure Electronic Voting". Open Computer Science, DeGruyter; 9:292-298. DOI: 10.1515/comp-2019-0018.

[25] N. Gama, N. Howgrave-Graham, and P. Q. Nguyen (2006), "Symplectic Lattice Reduction and NTRU. In: Vaudenay S. (eds) Advances in Cryptology" - EUROCRYPT 2006. Lecture Notes in Computer Science, vol 4004. Springer, Berlin, Heidelberg. https://doi.org/10.1007/11761679_1.

[26] A. Zalekian, M. Esmaeildoust, and A. Kaabi, (2015), "Efficient Implementation of NTRU Cryptography using Residue Number System". International Journal of Computer Applications (0975 – 8887) Volume 124 – No.7.

[27] N. Mishra, T. K. Sharma, V. Sharma and V. Vimal,(2018), "Secure Framework for Data Security in Cloud Computing",Soft Computing: Theories and Applications, Advances in Intelligent Systems and Computing 583, https://doi.org/10.1007/978-981-10- 5687-1_6.

[28] R.Lizy,andV.Raj(2021),"ImprovementofRSAAlgorithm Using Euclidean Technique", Turkish Journal of Computer and Mathematics Education.Vol.12 No.3.

[29] D. Elminaam, H. Kader, and M. Hadhoud, (2009), "Performance Evaluation of Symmetric Encryption Algorithms", IJCSNS International Journal of Computer Science and Network Security. Vol.8 No.12.

[30] E. Camacho-Ruiz, M. C. Martínez-Rodríguez, S. Sánchez Solano and P. Brox, "Accelerating the Development of NTRU Algorithm on Embedded Systems," 2020 XXXV Conference on Design of Circuits and Integrated Systems (DCIS), 2020, pp. 1-6, doi: 10.1109/DCIS51330.2020.9268647.

[31] E. Malekian, A. Zakerolhsooeini, (2010), "OTRU: A non-associative and high-speed public key cryptosystem", IEEE Computer Society, 83–90. https://doi.org/10.3390/s22031109.

[33] S. Kumar, G. Kamani, M.S. Guar, A. Mishra, (2021), "Cloud Security using Hybrid Cryptography Algorithms", 2021 2nd International Conference on Intelligent Engineering and Management (ICIEM).

[34] R.SugumarandK.Raja(2018),"EDSMCCE:Enhanced Data Security Methodology for Cloud ComputingEnvironment", International Journal of Scientific Research in Computer Science, Engineering and Information Technology, Vol. 3, Iss 3. International Journal of Mathematics and Computer Science, No 4 1469-1477.

[32] H.H. Abo-Alsood and H.R. Yassein, (2021), "Designof an a

[35]R. Adee, R. and H.A. Mouratidis, (2022), "Dynamic Four-Step Data Security Model for Data in Cloud Computing Based on Cryptography and Steganography", Sensors 2022, 22, 1109.

[36]K.S. Suresh (2021), "What are Quantum Cryptography's disadvantages", Available at https://www.what-are-quantum-cryptography's-disadvnatages. Access Date: 16th February, 2022.

[37]F.Wang,HWang,L.Xue(2021),"ResearchonDataSecurity in Big Data Cloud Computing Environment", 2021 IEEE 5th Advanced Information Technology, Electronic and Automation Control Conference(IAEAC)|978-1-7281-8028-1/20/$31.00 ©2021IEEE|DOI:10.1109/IAEAC50856.2021.9391025.

[38] Depavath Harinath,et.al,"A Review on Security Issues and Attacks in Distributed Systems," Journal of Advances in Information Technology(JAIT), California, USA, Vol. 8, No. 1, pp. 1-9, February, 2017. doi: 10.12720/jait.8.1.1-9

[39] Depavath Harinath, "Enhancing Data Security Using Elliptic Curve Cryptography in Cloud Computing", *International Journal of Science and Research (IJSR)*, https://www.ijsr.net/archive/v5i7/v5i7.php, Volume 5 Issue 7, July 2016, 1884 - 1890, DOI: 10.21275/v5i7.ART2016624

[40] Depavath Harinath,et.al, "An Interplanetary File System Framework For Invocation and Machine Learning Model Training", Bulletin For Technology And History Journal , Volume 24, Issue 2, 2024, Page No:151-157, DOI:10.37326/bthnlv22.8/1513

Author Profile

Depavath Harinath, Assistant Professor, received Master of Computer Applications degree from Sreenidhi Institute of Science and Technology, an autonomous institution approved by UGC, Accredited by NAAC with 'A+' grade and accredited by NBA, AICTE, New Delhi – permanently affiliated to JNTU, Hyderabad, Telangana, India. Having twelve years of experience in teaching and already published 20 manuscripts in different international journals.Now working as Assistant Professor, Dept. of Computer Science, Ramnath Guljarilal Kedia College of Commerce, Hyderabad, Telangana, India. Research field includes Computer Networks, Network Security, Artificial Intelligence and Machine Learning.

Prof. M. V. Ramana Murthy, Professor in department of mathematics and computer science, Osmania University, since 1985. Obtained PhD degree from Osmania University in 1985 and visited many a countries across the globe in various capacities and participated in many academic programs. Research fields includes computational plasma, Artificial Neural Networks, and Network securities.

Dr. Archana Patil, B.E, MTech(CSE) & Ph.D.(CSE)working as assistant professor in Rishi MS Institute of Engineering & Technology for Women, Hyderabad**.** She has 12+ years of teaching experience. She has completed Ph.D. from VTU Belagavi, Karnataka. Area of research is Green Cloud Computing. She has published many papers in reputed International and National Journals and Conferences with good citation. She already published many books and more than 10 Patents on different area of Computer Science and engineering. Her area of interest includes Cloud Computing, Data structure, Computer Graphics, IOT, Mobile Adhoc Network, Cyber Security,andmachinelearning.