ISSN:0975-9646

Implementation of NTRU Algorithm for the Security of N-Tier Architecture

Amandeep Kaur Gill[#1], Charanjit Singh[*2]

[#] *M.Tech, Research Scholar,*
Department of Computer Science and Engineering,
RIMT-IET, Mandi Gobindgarh, Fatehgarh Sahib, Punjab, India

[*] *Assistant Professor,*
Department of Computer Science and Engineering,
RIMT-IET, Mandi Gobindgarh, Fatehgarh Sahib, Punjab, India

***Abstract*— In these days, Security is necessary for all the applications on the network. Number of mechanisms is used for the purpose of providing the security to many applications. But for the N-Tier architecture there is no such type of mechanism is implemented for security till now. N-tier architecture has number of levels or tier, and for each tier security is essential. For providing the security to the data transferred on the network, NTRU algorithm is seen as fast and best algorithm. NTRU is patented and an open source public-key cryptosystem in which lattice-based cryptography system is used for encryption and decryption of files. Many applications make use of extensive databases to store the data and are accessible from anywhere by the multiple people simultaneously via World Wide Web. Applications that use this type of database can be implemented using 3-tier architectural model. There are different types of architectures like 1, 2, 3 or more tier architectures. This paper represents the implementation of the NTRU algorithm for security of such application that is N-tier architecture and showed that this algorithm provides the best security at each tier. The keys generated by the server are used for encryption/decryption of files and encrypted files are stored in the database. This paper focuses on the comparison of proposed work with previous on the basis of parameters like encryption and decryption time, throughput.**

***Keywords*— Encryption, Decryption, N-Tier architecture, NTRU, AES, Encryption time, Decryption time**

I. INTRODUCTION

N-tier architecture means splitting up the system into N tiers, where N is a number from 1 and more which means it includes a client tier, a database tier, and n-2 tiers in between them. The client tier is used as an interface between the system and the user, the database tier is to manage the data in the database and middle tier is used to provide the communication between other tiers. N-tier application is that in which more security is required at the different levels. It is also known as layered architecture. It can be used to model both a web-based application and a desktop application. [3, 13] In this, one layer uses the services from the other layer in order to provide its own services.

For n-tier, some of the layers of 3-tier architecture have been broken into number of layers and these layers are required to run on more tiers. For example, Application layer can be divided into business layer, persistence layer or more and Presentation layer can be split into client and client presenter layer. In Fig. 1, in order to get a complete N-Tier architecture, client business layer, presenter layer and data layer should have an ability to run in three separate computers (tiers). Practically, all these layers can also be deployed in one compute (tier) [9].

A. *Client layer:* This layer is usually interacts with users directly. There are many types of clients coexisting, such as Window form, WPF (Windows Presentation Foundation), HTML web page and etc.
B. *Client presenter layer:* This layer includes presentation logic required by clients, such as ASP .NET MVC in IIS web server. It usually adapts different clients to the business layer.
C. *Business layer:* This layer is called as domain layer because it handles and encapsulates all the business logics and domains such as WCF (Windows Communication Foundation) etc.
D. *Persistence layer:* This is called as data access layer (DAL) because it performs the read/write operations of data to data layer.
E. *Data layer:* It basically contains server that can be used for storing the application's data.

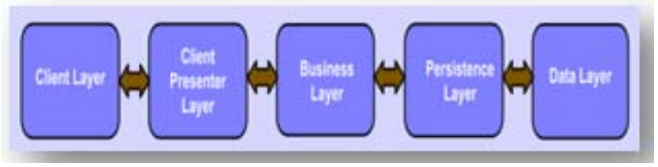

Fig. 1 N-tier architecture

In 1-tier architecture, both application and data layer can run on one computer. We have to use the embedded database system in order to achieve this architecture. Otherwise, because non-embedded databases can run only in an individual computer (tier) there will be at least 2-Tier architecture exists. 1-tier architecture is also known as single-process architecture.

2-tier architecture is the same as client / server architecture. Either application and presentation layer can only run in one computer or application or data layer can run in one computer only but the whole application cannot run in more than 2 computers.[3]

The 3-tier architecture is an easiest case of N-Tier architecture. In this, all the three tiers such as presentation, application and data tiers are required to run in three different computers respectively. In one computer these three layers can also be deployed practically. This diagram illustrates a 3- tier architecture:

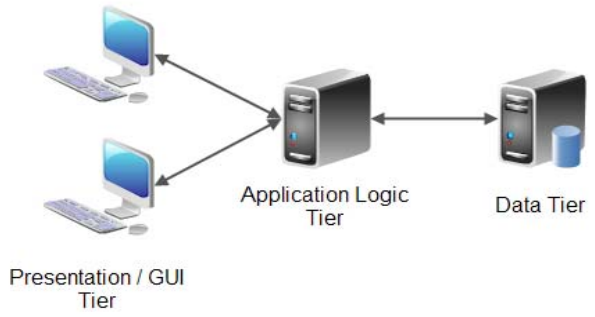

Fig. 2 Three-tier architecture

II. Related Work

In literature reviewed, several researchers have shown their interest in evaluating and presenting performance of different encryption algorithms. There are number of conclusions which have been made with regard to the performance of encryption algorithm in terms of throughput, encryption time, decryption time.

Sukhjinder Singh et al. [1], their work showed the implementation of NTRU algorithm on Cloud network with an android platform and comparison between RSA, DES and NTRU algorithms based on these three parameters: encryption time, decryption time and throughput. They concluded the result that NTRU algorithm is much faster and secure than other algorithms. It improved the speed, security level and provided reliable message to key generation respectively, encryption and decryption at the receiver end.

Parsi Kalpana et al. [4], provides a method to provide the security to the cloud data by implementing the RSA (Rivest, Shamir and Adleman) algorithm. This paper also considered the security issues which arise in cloud computing like integrity, location and relocation, Confidentiality etc.

Subedari Mithila et al. [5], describes the security control process by describing the security controls like technical, operational and management with respect to security control families. Their research provides a list in which required technical controls in order to match security requirements of any information system given the confidentiality impact level of the information system.

Yashpal Mote et al. [6], addressed about the Authentication, Confidentiality and Integrity in SMS (Short Message Services). It is important to secure the SMS with the help of encryption algorithm because transfer of the SMS over the network is insecure. They have used these two parameters which are: its ability to secure the protected data against attacks by hackers and its speed and efficiency, to show the difference between encryption algorithms and to evaluate the algorithm's speed. Their result showed the superiority of the NTRU algorithm in terms of the processing time over the other algorithms.

Ranjeet Ranjan et al. [7], gives the description of NTRU cryptosystem, its analysis and some needed improvement in it for the network security. Their research proved that improved NTRU algorithm works better than existing NTRU because it encrypts and decrypts the large files quickly.

Leena et al. [2], proposed a security framework for centralized database security in cloud by combining TORDES and RSA algorithms. TORDES is symmetric key algorithm used for two factor authentication process. RSA is used to enhance the authentication process by integrating the digital fingerprint mechanism.

III. Overview of NTRU Algorithm

NTRU (N-th degree Truncated polynomial Ring Unit) is an open source and patented public-key cryptosystem which uses lattice-based cryptography for encryption and decryption of files. The two keys used in this algorithm are: public key and private key. The key is used for the encryption is Public Key or to verify the digital signature but private key is used for decryption or to create digital signature, as shown in Fig. 3. [10]

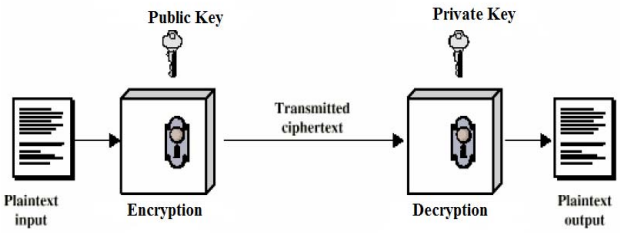

Fig. 3 Working of NTRU algorithm

It is based on polynomial arithmetic; therefore it provides very fast computation for the encryption and decryption of the message. NTRU has less complexity i.e. $O(N^2)$ [7, 8]. The operations are based on objects that are in a polynomial ring:

$$R = Z [X] / (X^N - 1)$$

The polynomials, present in the ring have integer coefficients and degree N – 1:

$$a = \alpha_0 + \alpha_1 X + \alpha_2 X^2 + \ldots\ldots + \alpha_{N-2} X^{N-2} + \alpha_{N-1} X^{N-1}$$

Actually the NTRU is a parameterised family of cryptosystems; in which each system is defined by three parameters (N, p, q), which represents the maximum degree N-1 for all of the polynomials in the ring R, small and large modulus respectively, N is assumed as prime, where p and q are co-prime. Suppose f, g, r, e, and a are all ring polynomials.

A. Key Generation: NTRU involves a public key and a private key. The public key is used for encrypting message and can be known to everyone. Messages encrypted with this key can only be decrypted in a reasonable amount of time using the private key.

B. Encryption: For encryption of a plaintext message m ε R using h as the public key, Alice chooses a random element r ε R and creates the ciphertext:

$$e \equiv r * h + m \pmod q$$

C. Decryption: For decryption of the ciphertext e using the f as a private key, Bob firstly computes the value:

$$a \equiv f * e \pmod{q}$$

Bob then selects a ε R to satisfy this congruence and to lie in a certain pre-specified subset of R. He next does the mod p computation $f_q^{-1} * a \pmod{p}$ and the value he calculates is equal to m modulo p [11].

The main characteristics of NTRU algorithm are low computational and memory requirements for providing a high level security. In this algorithm the difficulty is faced during the factorisation of the polynomials into two different polynomials having very less coefficients [12]. NTRU is a widely usable, well-accomplished and promising cryptosystem.

IV. Proposed Work

In Existing work, NTRU algorithm was implemented on an android platform for security purpose. But NTRU Algorithm has not been implemented on the N-tier architecture where multiple servers exist like job portal application where job seekers, recruiters and admin are present. Challenge is to secure database system of N-Tier architecture using encryption algorithm i.e. NTRU.

The first objective of proposed work is to study the various encryption/decryption algorithms either they are asymmetric or symmetric. Symmetric key algorithms are those in which use the same key for the encryption and decryption of data but in this asymmetric key algorithms, the key which is used for encryption of data is not same with the key used for decryption of data. The next objective is to design the N-Tier architecture, which has multiple servers and then next one is to implement the NTRU algorithm on N-Tier architecture to provide the security. The last objective is to analyse the results of proposed work.

V. Methodology Used

The research methodology is divided into 6 steps as shown in Fig. 6 which achieve our desired goal:

Step 1: In this phase, we have to initiate all the servers that are used to process the user requests.

Step 2: In this, admin can login in order to see user's request and user can login for sending the request.

Step 3: This phase include the uploading of file by the user, which is to be encrypted as shown in Fig. 4. Server receives the file and generates a unique key.

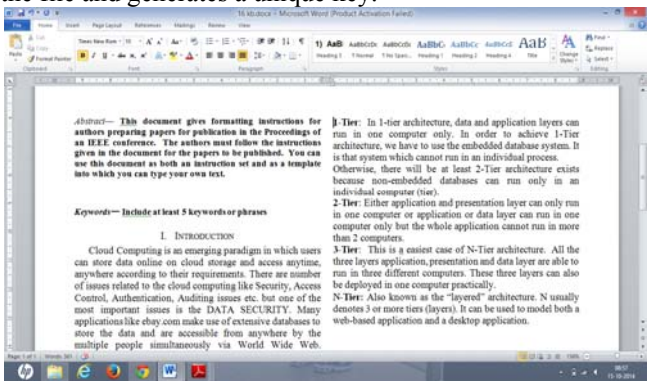

Fig. 4 Before the encryption

Step 4: This phase include the encryption of the file uploaded by the user with help of encryption /decryption algorithm i.e. NTRU algorithm, as shown in Fig. 5. Then, the encrypted file is stored in the database.

Fig. 5 After the encryption

Step 5: This phase include the decryption of the file using NTRU that is stored in the database and should be downloaded by the user.

Step 6: Final results are validated. The given results are analyzed and provide the conclusion on the basis of results obtained.

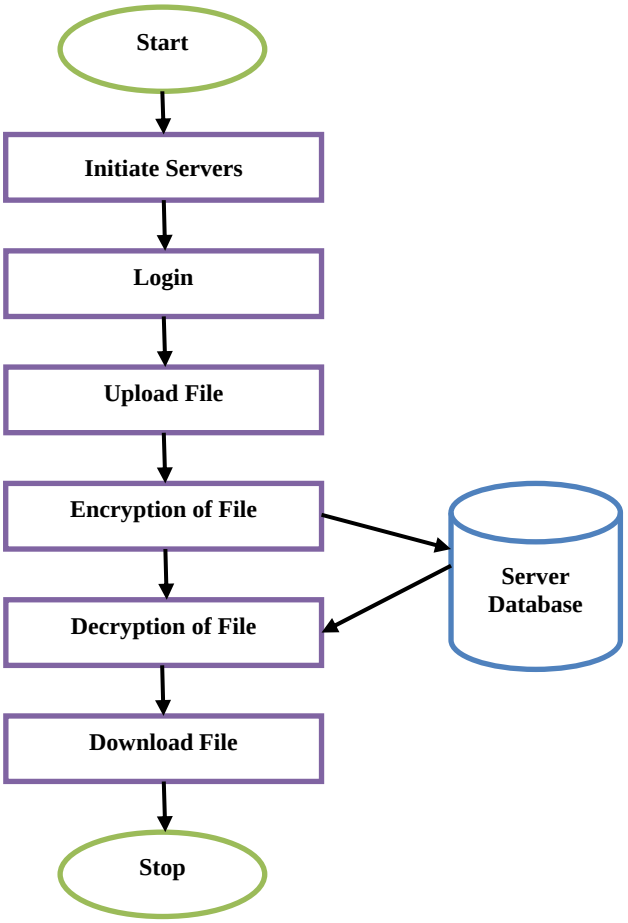

Fig. 6 Research Methodology

This is how the research work carried out; the information gained at each step plays vital inputs for the research and produces the desired output according to the given input.

VI. Experimental Results and Discussion

Our research work is to measure the Encryption and Decryption speed for data inputs of different sizes. It considers the three parameters i.e. Encryption time, Decryption time and Throughput, which are given below:

A. Encryption Time: Encryption is the process of converting the plaintext into the cipher text, which cannot be understood by the unauthorised user. So, the time taken to encrypt the data is known as encryption time.

TABLE I
Encryption Time For Data Inputs of Different Sizes

Data Input(Size)	NTRU
16 kb.docx	1
1.66 mb.docx	2
10 mb.docx	2.4
28 mb.docx	3
74 mb.docx	4

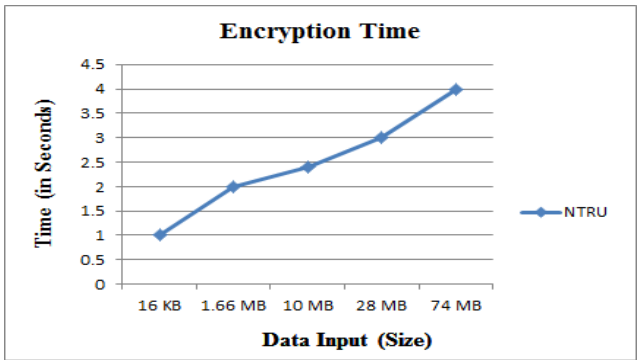

Fig. 7 Encryption Time of NTRU algorithm

B. Decryption Time: Decryption is the process of converting the cipher text (encrypted data) into the plaintext (original data), so that it can be easily understood. The time taken to decrypt the data is known as decryption time.

TABLE II
Decryption Time For Data Inputs of Different Sizes

Data Input(Size)	NTRU
16 kb.docx	1
1.66 mb.docx	1
10 mb.docx	1.4
28 mb.docx	2
74 mb.docx	3

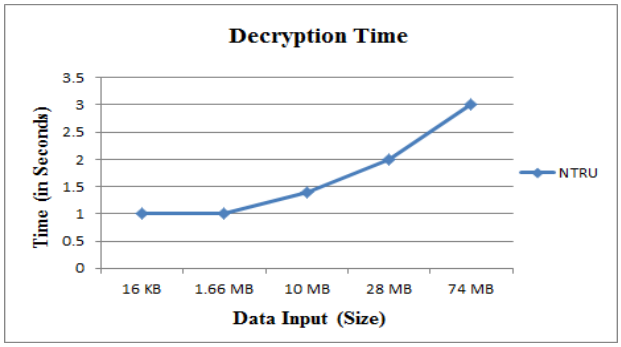

Fig. 8 Decryption Time of NTRU, AES algorithms

C. Throughput: The throughput is calculated by dividing the total plaintext/cipher text (in Megabytes) encrypted/decrypted to the total encryption/decryption time (in seconds). If the throughput value is increased, then the power consumption of encryption technique is decreased.

Throughput = Total text (in MB) / Total Time Taken (in Sec.)

TABLE III
Throughput of NTRU Algorithm

Throughput(MB/Sec)	NTRU
Encryption	9.16
Decryption	13.53

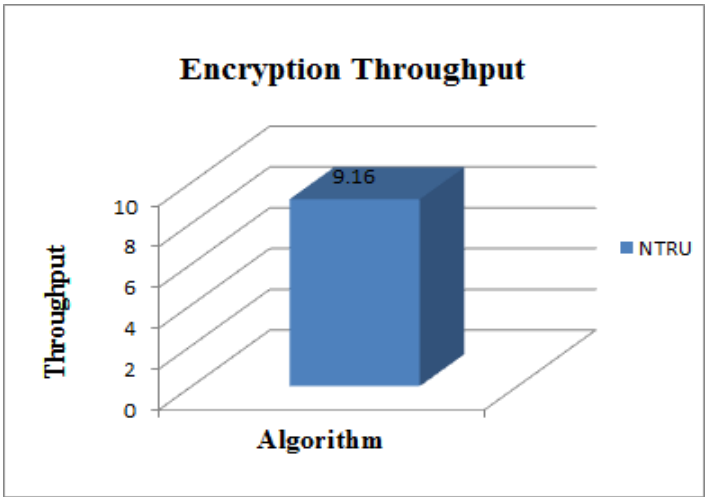

Fig. 9 Encryption Throughput of NTRU algorithm

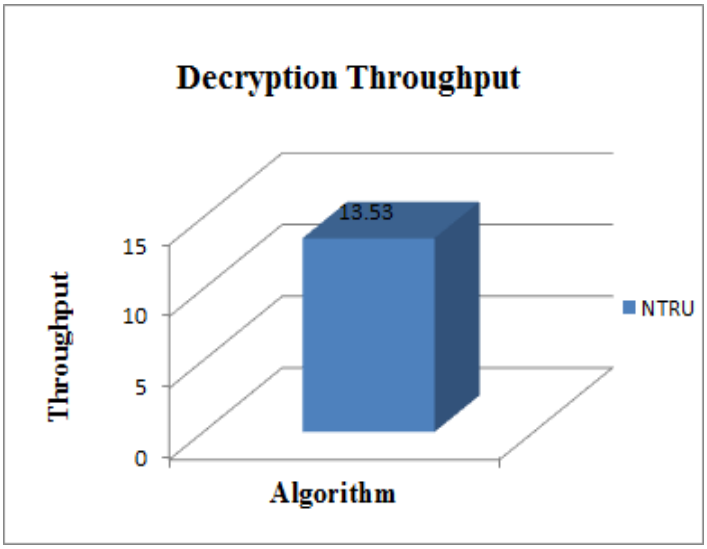

Fig. 10 Decryption Throughput of NTRU algorithm

VII. COMPARISON

By considering different sizes of data blocks two algorithms NTRU, AES are evaluated, which results in terms of the time taken to encrypt and decrypt the data block.

TABLE IV
ENCRYPTION TIME FOR DATA INPUTS OF DIFFERENT SIZES

Data Input(Size)	AES	NTRU
16 kb.docx	8	1
1.66 mb.docx	9	2
10 mb.docx	16	2.4
28 mb.docx	20	3
74 mb.docx	26	4

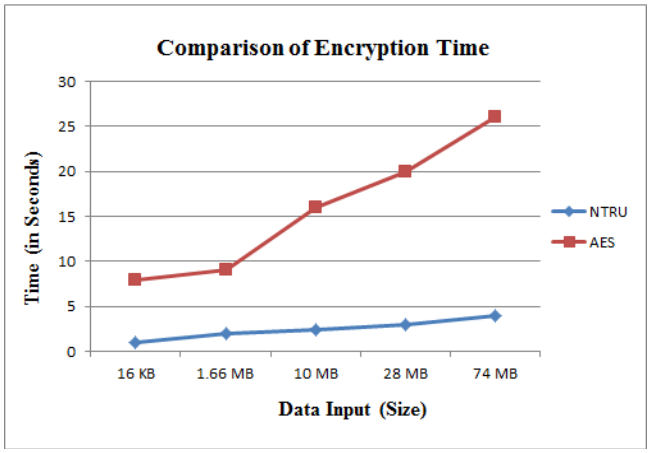

Fig. 11 Encryption Time of NTRU, AES algorithms

TABLE V
DECRYPTION TIME FOR DATA INPUTS OF DIFFERENT SIZES

Data Input(Size)	AES	NTRU
16 kb.docx	8	1
1.66 mb.docx	9	1
10 mb.docx	16	1.4
28 mb.docx	20	2
74 mb.docx	26	3

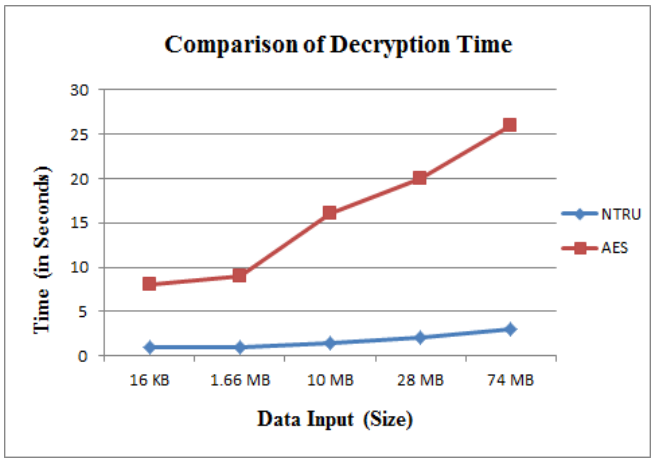

Fig. 12 Decryption Time of NTRU, AES algorithms

TABLE VI
THROUGHPUT OF DIFFERENT ALGORITHMS

Throughput(MB/Sec)	AES	NTRU
Encryption	1.64	9.16
Decryption	1.64	13.53

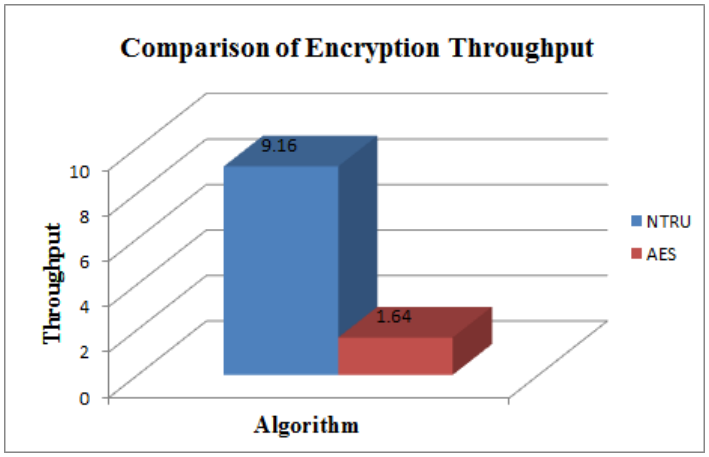

Fig. 13 Encryption Throughput of NTRU, AES algorithms

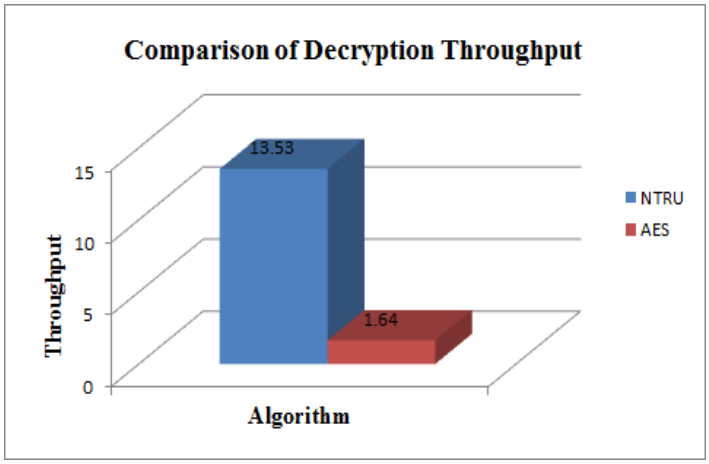

Fig. 14 Decryption Throughput of NTRU, AES algorithms

VIII. CONCLUSION AND FUTURE WORK

In this paper, for security purpose NTRU algorithm is implemented on N-Tier application. The simulation results shows that NTRU algorithm has better performance than other commonly used encryption algorithms. Since NTRU has not any known security weak points till now, it can be considered as an excellent standard encryption algorithm. AES showed performance results poor as compared to NTRU algorithm, since it requires more processing power. The experimental results reveal that the proposed method offers better performance over previous work.

In future, we intend to provide security on N-Tier architecture having cloud database using NTRU algorithm. Also try to provide security on N-Tier architecture using other algorithms.

ACKNOWLEDGMENT

The author would like to thank the RIMT Institutes, Mandi Gobindgarh-147301, Fatehgarh Sahib, Punjab, India. Author also extremely grateful and remain indebted to all the people who have given their intellectual support throughout the course of this work. And a special acknowledgement to the authors of various research papers and books which help me a lot.

REFERENCES

[1] Sukhjinder Singh and Mr.Sachin Majithia, "*Implementation of NTRU on Cloud Network in an Android Platform and Comparison with DES and RSA* ", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 11, November 2013, pp-100-104.

[2] Leena and Miss A.Kakoli rao, "*Centralized Database Security in Cloud*", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 1, Issue 8, October 2012, pp-544-549.

[3] http://tutorials.jenkov.com/software-architecture/n-tier-architecture.html

[4] Parsi Kalpana and Sudha Singaraju, *"Data Security in Cloud Computing using RSA Algorithm",* International Journal of Research in Computer and Communication technology, IJRCCT, ISSN 2278-5841, Vol 1, Issue 4, September 2012, pp-143-146.

[5] Subedari Mithila and P. Pradeep Kumar, "*Data Security through Confidentiality in CloudComputing Environment*" (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 2 (5) , 2011, pp- 1836-1840.

[6] Yashpal Mote, Paritosh Nehete and Shekhar Gaikwad, "*Superior Security Data Encryption Algorithm(NTRU)*" An International Journal of Engineering Sciences ISSN: 2229-6913 Issue July 2012, Vol. 6, pp-171-181.

[7] Ranjeet Ranjan, Dr. A. S. Baghel and Sushil Kumar, "*Improvement of NTRU Cryptosystem*" International Journal of Advanced Research in Computer Science and Software Engineering , Volume 2, Issue 9, September 2012, pp-79-84.

[8] http://en.wikipedia.org/wiki/NTRU.

[9] http://www.codeproject.com/Articles/430014/N-Tier-Architecture-and-Tips#Tier%20And%20Process%20Relationship.

[10] Amandeep Kaur Gill and Charanjit Singh, "*Survey on Encryption Algorithms to Overcome Security Issues in Cloud Computing*", International Journal of Advanced and Innovative Research (2278-7844) / # 475 / Volume 3 Issue 4, 2014, pp- 475-480.

[11] Fei Hu, Kyle Wilhelm, Michael Schab, Marcin Lukowiak, Stanislaw Radziszowski and Yang Xiao, "*NTRU-based sensor network security: a low-power hardware implementation perspective*" Security and Communication Networks Copyright # 2008 John Wiley & Sons, Ltd.

[12] https://www.cdc.informatik.tu-darmstadt.de/reports/reports/Nikolay_ Vizev.bachelor.pdf.

[13] http://matifnadeem.blogspot.in/2013/03/n-tier-architecture.html.