ISSN:0975-9646

Enhancing Security and Concurrency in Distributed Database with 6 Bit Encryption Algorithm

Gurkamal Bhullar[1], Navneet Kaur[2]

Computer Science Department[1], Computer Science Department[2]

Lovely Professional University Phagwara[1](India), Lovely Professional University Phagwara[2] (India)

***Abstract*— Distributed database is the collection of data which are distributed on different network on different computer due to which we eliminate single site failure. Since in previous work RSA is used widely to provide security but in this paper discussion is based on the NTRU. NTRU is superior security algorithm and deal with 6 bits due to which encryption is done in less time and with more accuracy as compared to the RSA. Hence due to this feature we name it as six bit encryption algorithm. This six bit encryption algorithm is used to enhance the security and controlling the concurrency in distributed database. Moreover in this we are going to redirect our query on other server in case of traffic. Hence this query redirection factor will control the concurrency.**

Keywords: **Distributed database, Concurrency control, Security, NTRU, Query redirection.**

I. INTRODUCTION

The development in the technology of the computer and along with that development in the technology of the database system resulted in the development of the distributed database over the centralized database in the mid 1970's [1][2]. This distribution is mainly done because it is predicted that there may be the situation in which application should be distributed for that database. The major problem that we face in normal database is that failure at one point means overall failure, but in distributed database, single point failure problem is removed as in this system database is distributable to many locations and if there is some kind of failure at one point, we can access data from the other location also. The goal for this problem is to obtain maximum throughput with efficient encryption and decryption technique. The distributed database includes the distributed Database management system (DDBMs) that is responsible for managing the distributed database. DDBMS include some of the components and that are discussed below [10]

- Distributed query processing (DQP): This is responsible for handling the queries in the distributed environment.
- Distributed transaction manager (DTM): Manager plays important role in managing the various transactions that have been performed.
- Distributed metadata manager (DMM): Manages distributed metadata.
- Distributed security manager (DSM): Its responsibility is to manage the security related factors.

Security also plays the paramount role in the distributed database. Therefore issues that should be kept in mind while dealing with the security, is authentication, access controls, identification. All issues should be handled with great care. In this case we are using the six bit encryption algorithm for maintaining the security and to achieve the objectives. Hence six bit encryption algorithm is also named as NTRU as it is dealing with six bits due to which, its speed also the accuracy get improved.

Concurrency control techniques ensured us that our database should be consistent at the times when multiple transactions were executed concurrently. Although there are present many concurrency control techniques like locking in which we lock the data item when we are working upon it. Then we have the timestamp in which we give time after each transaction, but we are dealing with the query redirection in distributed environment. According to this query will be directed to other server at the time of network failure. Security with NTRU is addressed in this paper [2]. NTRU is the superior security data encryption algorithm. It is superior then other algorithms in terms of some of the following points.

1) Encryption
2) Decryption
3) Throughput
4) Accuracy with which we attain the goal.

We can also redirect our query at time when server feels overloaded with work or by heavy traffic.

Distributed database has many benefits due to which it is widely used in much business organization but major factor on which it focuses more is performance, it can be increased as database is located at different location therefore access of data become easy hence by this, performance will be increased. Another factor that is considered in distributed databases is updations of the content of the database or to keep in mind that is up to date that work can be done mainly with the help of two processes i.e. replication and duplication although they seems to be the same but done differently. Replication can be done with the help of certain sort of software, when some changes are reflected that changes will be replicated at different places, but in case of duplication database is made or identified as master and then that will be duplicated.

II. BACKGROUND

NTRU is the native time research unit. It is the low memory usage algorithm and hence responsible for providing the extreme or the top most security. Improvement of the public key cryptosystem is the best factor that we consider in the field of the cryptography and they use encryption and decryption method which plays the paramount role in maintaining authentication and confidentiality.

NTRU is the acronym for the nth degree truncated polynomial ring which is called simply the NTRU. NTRU was founded in 1996 by 3 mathematicians: Jeffrey Hoff stein, Joseph H. Silverman, J.Pipher the mathematicians were considered on speeding up the process. In 2009 NTRU cryptosystem has been approved for standardization by the institute of electrical and electronics engineers (IEEE). These mathematicians contact with each other with the D.lieman founded by the NTRU cryptosystem and they also have patent on cryptosystem and therefore is algorithm is considered a relatively new cryptosystem [8] [4]. These mathematicians that are used based on the lattice based cryptosystem and have different cryptographic property than that of RSA [7]. It performs the certain private key operations much faster than RSA. This algorithm is considered as one of the superior security encryption algorithm where we deal large bits of data as compared to the RSA, due to this feature the encryption get completed in less time and also the accuracy level increases.

A. *Asymmetric Approach*

NTRU is using asymmetric approach i.e. using two different keys one for encryption purpose and another is for the decryption. This means when sender wants to send its valuable data to the receiver he will encrypt that data with the help of the public key and after that we that message or data reached at receiver end he will decrypt it with the public key. Hence this approach is used for efficient level of security.

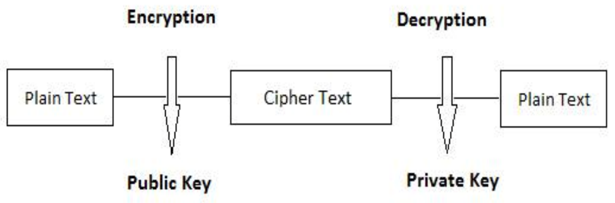


Fig. 1 Asymmetric approach in NTRU

B. *Why NTRU?*

NTRU is the superior security encryption algorithm [3]. It is better and efficient as compared to the RSA. Following were some of the points that are reason why we prefer the NTRU over the RSA.

- It is the cryptosystem that has the highest performance as compared to other cryptosystem or we can say present in the now days market.
- It is five to six times faster than RSA. Along with that NTRU consumes minimum resources that will include CPU, battery, and also how much memory it utilizes at run time [5].
- Throughput in case of the NTRU is improved 60% when it gets combined with SSL [6].
- It helps in reducing server resource utilization significantly in case of large-scale deployments.

III. Implementation Work

A. *NTRU Algorithm Steps*

1) The generic steps used for Encryption

Step-1 Read the content from a file and store in string builder.

Step-2 Convert the string builder in to character array.

Step-3 Take every character from an array then take its ASCII value after that convert it in binary value example like 10011101111110000001.

Step-4 Apply the following steps.

a. Choose two distinct prime numbers p and q.

Find n such that n = p q. n will be used as the modulus for both the public and private keys.

b. Find the totient of n, $\phi(n)$ $\phi(n)=(p-1)(q-1)$.

c. Choose an e such that $1 < e < \phi$ (n), and such that e and ϕ (n) share no divisors other than 1 (e and $\phi(n)$ are relatively prime).e is kept as the public key exponent.

d. Determine d (using modular arithmetic) which satisfies the congruence relation $e \equiv 1 \pmod{\phi(n)}$.

2) The generic steps for decryption

Step-1 Take the decryption files from computer and read its content.

Step-2 follow the same procedure like get the strings from file then store in string builder then convert that string in to char array then take every character and store that character as ASCII value in array list then get binary value from array list.

Step-3 Now apply inverse Euclidian algorithm to get decryption number and then apply it on a binary pattern.

Step-4 apply the following steps

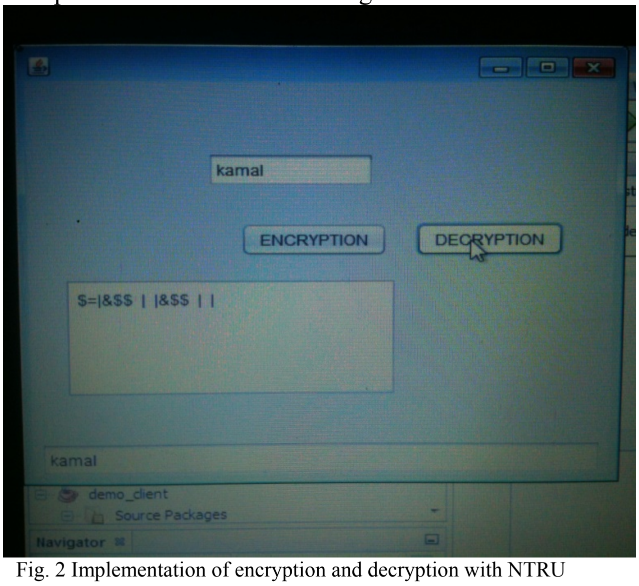
a. After that take 5 combination of binary from resultant binary.

b. Convert that binary into decimal value then convert that decimal value into character value by applying this process.

c. Take all letters and store them in character array.

d. Convert array to string and store in plaintext.

e. Repeat until we achieve our original text.



kamal

$=|&$$ | |&$$ | |

kamal

Fig. 2 Implementation of encryption and decryption with NTRU

IV. System Flow Design

This flowchart conveys us the entire process of the system that how it processes or functions. This will intimate us as to how the complete operation runs. The subsequent architecture shows us the operation works bit by bit and step by step. In other words we shows the slowly but surely representation qua the flowchart.

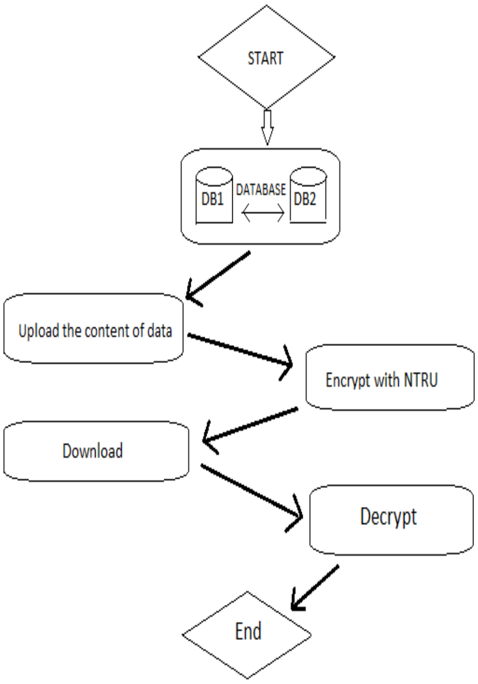


Fig. 3 System Flow Design

Steps with how data flows in above design:

- Data is stored in the database
- Upload the content of the data
- Encrypt it with using the NTRU content
- Then download the content
- Decrypt the content
- Then get the final result

V. Result Of NTRU

In the below Graphical and Tabular representation of RSA and NTRU we have shown comparative analysis of two algorithms and with the help of this process we have come to a conclusion that the encryption and decryption timings of both are different and there is a vast difference between both which makes us understand that the encryption and decryption timings of NTRU is much better than that of RSA.

A. Comparison with respect to encryption and decryption.

In this comparison we analysed that as the no of bits increases encryption and decryption become easier. This simulation will clear our concept that NTRU is superior algorithm as it evaluates the result fastly.

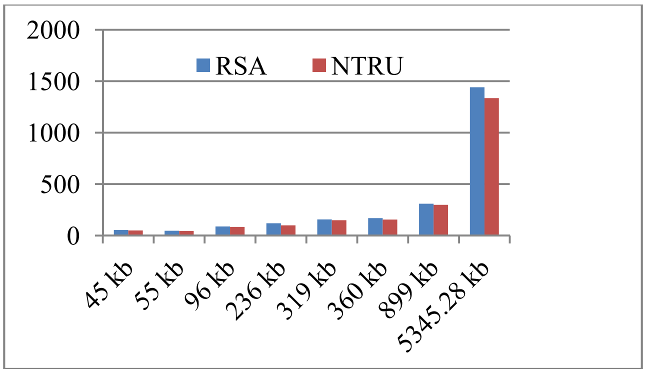


Fig. 4 Comparative Analysis of NTRU & RSA with respect to Encryption.

TABLE I
Performance Evaluation of NTRU & RSA with Respect to Encryption

Input size (Kb)	RSA Timing (ms)	NTRU Timing (ms)
45	55	50
55	46	45
96	89	84
236	119	100
319	157	149
360	169	155
899	309	298
5345.28	1441	1335

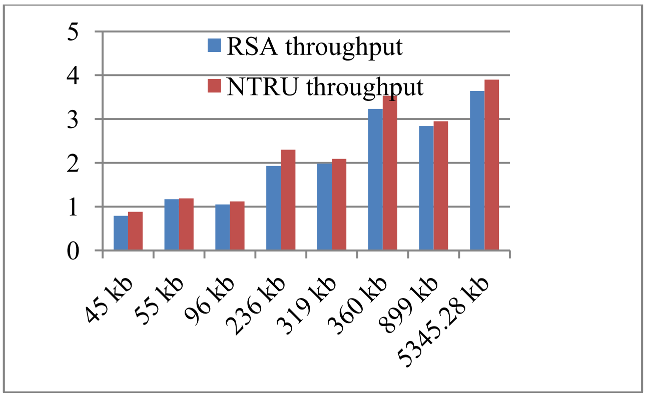


Fig. 5 Comparative Analysis of NTRU & RSA with respect to Decryption

Table II
Performance Evaluation of NTRU & RSA with respect to Decryption.

Input size (Kb)	RSA Timing (ms)	NTRU Timing (ms)
45	61	55
55	59	54
96	57	53
236	64	62
319	154	146
360	163	160
899	183	174
5345.28	827	801

B. Throughput evaluation of NTRU and RSA with respect to encryption

In this we come to know as the throughput increases it means that particular algorithm will consume less resource. Hence with these result we come to know that NTRU is better than RSA in terms of throughput.

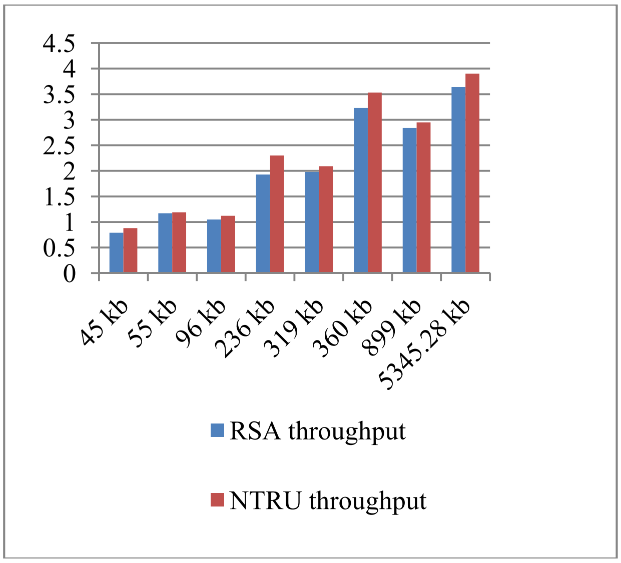


Fig 6: Comparative analysis of NTRU and RSA with respect to throughput in encryption

Table III
Throughput Evaluation of NTRU & RSA with respect to encryption

Input size (Kb)	RSA throughput (MB/sec)	NTRU throughput (MB/sec)
45	0.79	0.88
55	1.17	1.19
96	1.05	1.12
236	1.93	2.30
319	1.98	2.09
360	3.23	3.53
899	2.84	2.95
5345.28	3.64	3.90

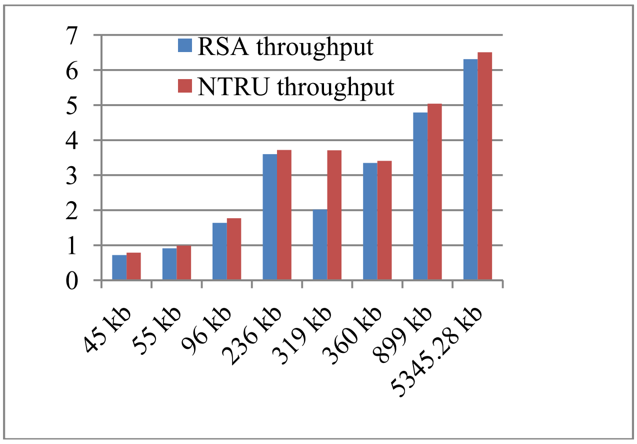


Fig 7: Comparative analysis of NTRU and RSA with respect to throughput in decryption

Table IV
Throughput Evaluation of NTRU & RSA with respect to decryption

Input size (Kb)	RSA throughput (MB/sec)	NTRU throughput (MB/sec)
45	0.72	0.79
55	0.91	0.99
96	1.64	1.77
236	3.60	3.72
319	2.02	3.71
360	3.35	3.41
899	4.79	5.04
5345.28	6.31	6.51

In the above graph we have done the comparative analysis among RSA, and NTRU. Therefore we have arrived at this conclusion that as the no of bits increases NTRU will be able to deal with it more efficiently. [3] Hence as the no of bits exceed, encryption will take place as faster rate in NTRU.

VI. Conclusion

So, after going through all the facts and figures as above mentioned, to get well grounded information through distributed database management system, we bring to an end that we can reliably makes our choice of NTRU as a primary concern, because of its prodigious features which it owns or possesses namely it is being endowed with Highest performance crypto on the market and its characteristic of being 5x to 200x times speedier than RSA is also one of the most stupendous feature. Moreover for the purpose of polynomial generation in future or for future purpose, more effective algorithms can be executed. Furthermore the paper provides detailed elucidation regarding the superior NTRU's position vis-à-vis RSA and DES due to some flabbergasting points such as the security level of NTRU is the highest and approving, besides this the most paramount point which is to be considered is that the NTRU cryptography is the expeditious, strongest, compact or smallest one available. Additionally it is being capable of protecting systems from today's attacks as its future-proof and our concern in this proposed work is mainly on the tremendous position of NTRU with regards to RSA or DES.

References

[1] Sheetlani Jitendra and Gupta V.K., " *Concurrency Issues of Distributed Advance Transaction Process", Res. J. Recent Sci.,* 1(ISC-2011), 426-429 (2012**)**

[2] Gupta V.K., Sheetlani Jitendra, Gupta Dhirajand Shukla Brahma, "*Data concurrency control and security issues of distributed database transaction"* NIMS University, Jaipur, Rajasthan, INDIA Vol. 1(2), 70-73, August (2012)

[3] Yashpal mote and Shekhar Gaikwad," *superior security data encryption algorithm*" international journal of engineering science, issue July 2012, vol-6

[4] Wikipedia - the free encyclopedia "NTRU Cryptosystems Inc."

[5] Hoffstein J., Lieman D., Pipher J., Silverman J. "NTRU: A Public Key Cryptosystem", NTRU Cryptosystems, Inc. (www.ntru.com).

[6] Parasitism C, Prada J. "Evaluation of Performance Characteristics of Cryptosystem Using Text Files", Journal of Theoretical and Applied Information Technology, Jatit, 2008

[7] Coppersmith and A. Shamir, "Lattice attacks on NTRU," in Proc. of EUROCRYPT 97, Lecture Notes in Computer Science, Springer-Verlag, 1997[CS97]

[9] J. Hoffstein, J. Pipper, and J. H. Silverman, "NTRU: A Ring Based Public Key Cryptosystem", in Proc. of Algorithmic Number Theory: Third International Symposium (ANTS 3) (J. P. Buhler, ed.), vol. LNCS 1423, Springer-Verlag, June 21-25 1998, pp. 267-288

[10] Rashmi Jha, Anil Kumar Saini, "A Comparative Analysis & Enhancement of NTRU Algorithm for Network Security and Performance Improvement,", in *IEEE*, 2011.

[11] ILKER KOSE data and network security -spring 2000 GYTE, computer science