ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 3, March 2014

Concurrency and Security Control with NTRU

Gurkamal Bhullar, Navneet Kaur

Student, Department of Computer Science, Lovely Professional University, Phagwara, India
Assistant professor, Department of Computer Science Lovely, Professional University, Phagwara, India

ABSTRACT : Distributed database is the emerging technique that plays an important role, in day to day life, so we focus on concurrency control and security issues under this distributed database. We are going to discuss some techniques like locking but our emphasis is mainly on query redirection. Under which if the particular server gets overloaded with traffic, we put forward the load to another server. In this paper we are going to analyze the NTRU, based Encryption decryption technique for security to Distributed Database System. The NTRU being fast and secure hashing algorithm will provide more security to the system, in terms of throughput and processing speed.

KEYWORDS -: Concurrency control, Distributed database, NTRU, Security, Query redirection.

I. INTRODUCTION

Distributed database plays a very vital and paramount role in our daily life, because in this present era business environment is increasing at very rapid rate, therefore due to this reason our basic desire is that the information we receive which might be from any source should be reliable as per our needs, because it is useless or of no value if it is not befitting.[1] Since our database is distributed, as itself it can be perceived by its name, it means that data is located at different geographical locations and finally this helps us to easily access our valuable and precious data that also so briskly. 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.

Concurrency control through query redirection and security with NTRU is addressed in this paper. [2] To understand the concept of concurrency and to determine how much it is important to control the concurrency we discussed one scenario, in this case we took the example of theater where two persons book the same seat at the same time as there arise conflict as one person can book the seat. In this example there present two persons 1&2 they read from the database at the same time that seat no 9 is available from the database so both persons try to reserve that seat hence arise problem in that case because only one person can reserve that seat, therefore it is necessary to take proper measures to control the concurrency. NTRU is the superior security data encryption algorithm [3]. It is superior then other algorithms in terms of some of the following points.

Encryption

1) Decryption
2) Throughput
3) 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

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 3, March 2014

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.RELATED WORK

In [1] author states some of the issues related to the concurrency control and security issues of the distributed database. in this main concerned is about the concurrency control techniques like locking and timestamp. In [2] author discussed about the advanced cryptography algorithm for improving the data security by using the asymmetric approach i.e., using public and private key differently. In [3] author discussed about the superior security encryption algorithm. Moreover focus entirely on AES, DES, triple DES, and NTRU from where derived that NTRU is the superior algorithm among all used above in terms of throughput and speed. This paper also provides the comparison between five of the most common encryption algorithm and this comparison has been conducted by running the several encryptions setting to process different sizes of data blocks to evaluate the encryption and decryption algorithm. In [5] author focused on focus about the data security issues in the cloud in that discussed about the privacy and the confidentiality which means that once the client hosted data to the cloud there should be some guarantee that access to that data will only be limited to the authorized access. Then next discussed about data integrity in which they ensure that cloud provider should be aware of what particular data is hosted on the cloud, origin and integrity. Then focus about the data location and relocation. Cloud computing must offer high degree of mobility. Customers do not always know the location of their data. There present data availability, storage and many other problems in that which come under the issues then other point of discussion is the data security that was the major factor. Since secure the data was the major factor now days therefore in order to protect our sensitive data from the unauthorized excess we use certain encryption and decryption techniques or with the help of certain approaches that can be with symmetric or that can be asymmetric approach that can be implemented with the help of certain types of algorithm.

III. BACKGROUND

In this we formulate some basic detail about NTRU encryption algorithm and also the related work is discussed over here. [4] NTRU was founded in 1996 by 3 mathematicians: Jeffrey Hoff stein, Joseph H. Silverman, Jill 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).NTRU Superior security data encryption algorithm Focus on asymmetric approach i.e. NTRU algorithm uses two keys one for encrypting the message and another for decrypting de message. It has long key, so outperformed with another algorithm Low memory usage allow it to use in applications like mobile device

A. Highest Performing Algorithm

There are many reasons due to which we conclude that NTRU is the highest performing algorithm some of them are discussed below.

- Highest performance crypto, that we can say present in the now days market.
- 5x to 200x times faster than RSA as it consumes minimal resources including CPU and battery run time memory utilization below 4.5K.therefore it is used widely.
- Significantly reduces server resource utilization for large-scale deployment
- Ideal for the environment which is hard to access or the environment in which high volume transactions are performed.

NTRU Cryptography is the compact, quick and well built accessible. It is mostly be acceptable to each and every type of systems. Furthermore it also able to protect systems from today's attacks, its future proof and besides this it resists attacks when they come available by quantum computers.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 3, March 2014

IV. EXPERIMENTAL WORK

In this we are going to discuss the work on which we focused. So his part formulates the NTRU algorithm steps. They mainly include all the steps that we require during the encryption and decryption phase. So plays the important role in maintaining the security.

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 $\phi(n)$ 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.

V. SYSTEM ARCHITECTURE

This architecture shows the overall process of the system. This will help us to indicate how the entire process works. The following architecture shows us the steps that how the entire work will proceed or in other words we show the step to step representation of the entire work with proper data flow diagram

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 3, March 2014

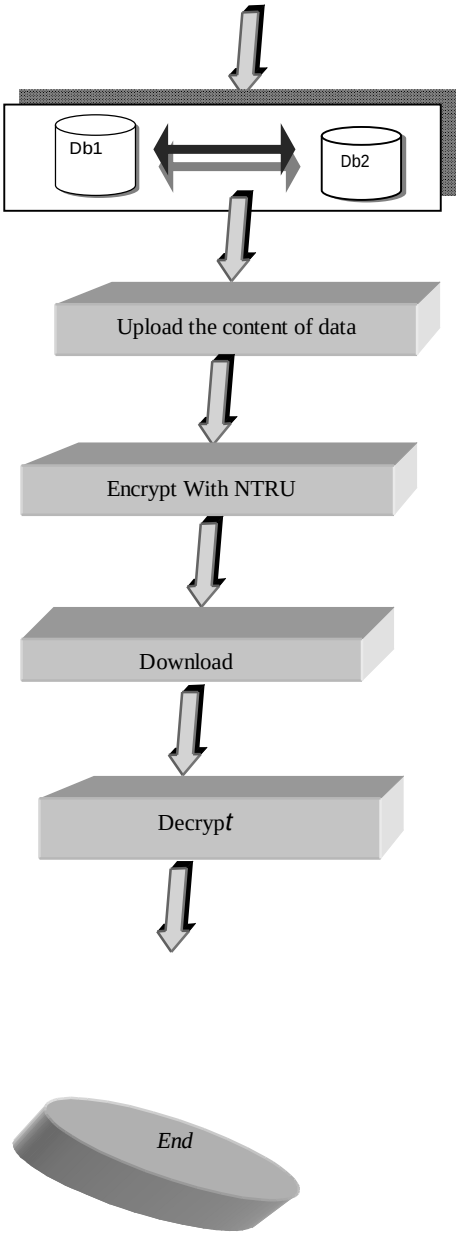

Fig 1: System architecture

In the above architecture we have shown that how our work proceeds. In this, first we will include the database. Then we upload the content of database, after that encrypt with NTRU. The next part includes downloading the content, if the person is authorized then content will appear in plaintext form otherwise it will appear in cipher text form

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 3, March 2014

A. Comparative Analysis:

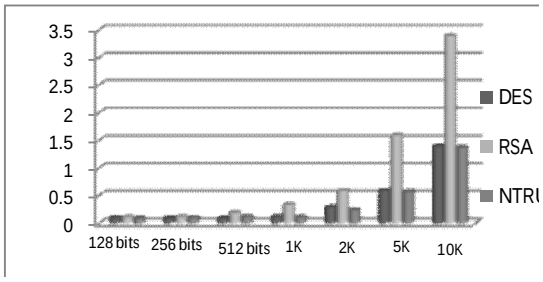

Fig 2: Comparative analysis [6]

In the above graph we have done the comparative analysis among DES, 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. [7] Hence as the no of bits exceed, encryption will take place as faster rate in NTRU

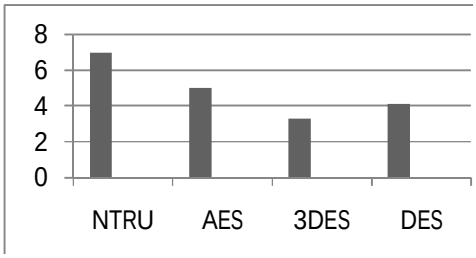

Fig3: Throughput Analysis

VI. CONCLUSION

So, conclude the points mentioned supra, as to access reliable information through distributed database management system .we may easily turn our face towards NTRU algorithm as NTRU is much better because of various reasons like it possess Highest performance crypto on the market and also 5x to 200x times faster than RSA and ECC. However it is Ideal for low power or hard to access environments (battery powered, electric grid, remote sensors) and high-volume transaction environments (payment processors, virtualization/cloud computing, etc.) In this paper we mainly concern about the better position of NTRU than RSA or DES because of some striking reason like the higher level of security, the higher performance gains versus competition and most importantly NTRU Cryptography is the smallest, fastest and strongest available. It is well suited to all types of systems including full scale servers down to the smallest of embedded systems. As well as being able to protect systems from today's attacks, the NTRU algorithm is future-proof and will resist attacks by quantum computers when they come available.

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 Parsi Kalpana ,"*data security in cloud computing using RSA algorithm,* International Journal of Research in Computer and Communication technology ,I, ISSN 2278-5841, Vol 1, Issue 4, September 2012

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 3, March 2014

6 Hoffstein J., Lieman D., Pipher J., Silverman J. "NTRU: A Public Key Cryptosystem", NTRU Cryptosystems, Inc. (www.ntru.com).
7 Parasitism C, Prada J. "Evaluation of Performance Characteristics of Cryptosystem Using Text Files", Journal of Theoretical and Applied Information Technology, Jatit, 2008

BIOGRAPHY

Ms. Gurkamal Bhullar is a student and received her Degree of BCA and M.Sc. IT from D.A.V. College, Abohar affiliated from Punjab University Chandigarh in 2012. She is currently pursuing her M.Tech in Computer Science and Engineering from Lovely Professional University, Phagwara, Punjab, India. Her research area in Database is to provide Security and Concurrency control in Distributed Database.

Ms. Navneet Kaur Bajwa has done her M.Tech from Punjabi University Patiala, Punjab, India. She has done her research in field of Security. At present she is working as an Assistant Professor in Lovely Professional University, Phagwara, Punjab, Patiala.