ISSN:0975-9646

A Highly Secured Four Layer Architecture Using NTRU Algorithem (TITEL)

[1.]Vipanjit Kaur, [2.]Vinay Bhardwaj

[1.]*Research Scholar(Department of Computer Science),Sri Guru Granth Sahib World University, Fatehgarh Sahib.Punjab,India*

[2.] *Asst. Professor(Department of Computer Science) Shri guru granth sahib world university, Fatehgarh Sahib,Punjab,India*

Abstract— Distributed database plays an important role in business environment. The major problem that we face in normal database is that failure at one point means overall failure, but in distributed database single point of failure problem is removed as database is distributable to many locations if there is failure at one point we can access data from the other location. An important area of research in this field provide security to database system. In this work of research, the 4 layered architecture is been developed with introduction of a strong encryption algorithm called NTRU. The four layered architecture is been developed for the purpose of high security which is needed to secure the highly confidential database systems. Each level have its own significance. All the parameters of security is fulfilled by the approach on four levels. No malicious users can interfere with the system, attacks such as brute force are successfully overcomes. The NTRU will save all the data in form of private and public key along the network saving the data from man in middle attacks.

Keywords: Encryption time, decryption time, through put, NTRU.

I. INTRODUCTION

Distributed database play very important role in our day to day life, because now days business environment is increasing at very fast rate, therefore due to this our basic desire is that the information that we get that may be from any source should be reliable as per our need, because if the information is not appropriate than that information is of no use. Since our database is distributed as the name suggests, it means that data is located at different geographical locations and also this help us to easily access our valuable data at also at the fast rate. The major problem that we face in normal database is that failure at one point means overall failure, but in distributed database single point of failure problem is removed as database is distributable to many locations if there is failure at one point we can access data from the other location. We will create the WLAN of system and existing authorized users will make the connection to server of the organization where they work. In case the worker is unauthorized this will need the database verification that present on server all the data of existing user will be present on server's database which will be cross verified dynamically. The database will dynamically remove the churn users from the entry of authorized users. means users who have fully resigned or inactive from long time will not be able to make the connection with server and will be removed automatically from server database . Main focus of our work is providing security to our data from hackers so we use NTRU algorithm for encrypt our data.

II. LITERATURE SURVEY

2.1. Concurrency control and security issues of distributed databases transaction by Gupta V. K. et al[2] in their paper states issues mainly about the concurrency control and some security issues of the distributed database what actually distributed database is, than after that we studied about the design of the distributed database that has three main additional fragments that are data fragmentation, data replication, data allocation and also discussed some of the concurrency control techniques .

2.2 Efficient K-mean clustering algorithm using ranking method by Jaspreet Kaur Sahiwal et al [7] in their paper says about the clustering and that done by the k-mean algorithm. k-mean clustering algorithm, density based clustering, self organization maps, EM clustering algorithm. Then we studied about the steps of the k mean clustering, k-mean clustering algorithm is an idea, in which there is need to classify the given data set into k clusters, the value of k is defined by the user which is fixed.

2.3 Optimistic approach in distributed database concurrency control by Obadiah A.Rawashdeh et al[10] in their paper says about the optimistic concurrency control solutions with this approach we can improve the performance and also increase the productivity and moreover this method include information about the timestamp of transaction and this will make successful updations in the data in main memory and not only this, this approach is useful for long running transactions and this will be done by adding a stamp to each record and then are sent to the user each time a user access the record and stamp will be counted and will hold the value of how many times a certain record is being accessed and this may also be possible through the read write operation.

2.4 Data **mining techniques** by Kalyani M Ravel et al [8] in their paper says about the data mining techniques in which first of all we studied about the knowledge discovery process, it is process that extracts implicit, potential useful or previously unknown information from the data. So the ultimate goal of the knowledge discovery and data mining process is to find the patterns that are hidden among the huge sets of data and interpret them to useful knowledge and information.

2.5 Advance cryptography algorithm for improving data security by Vishwa Gupta et al[9] in their paper says about the encryption in which there we discussed about the two approaches that are symmetric and asymmetric, in symmetric there are present same encryption and

decryption key or we can say that they use same public and private key.

2.6 Superior security data encryption Algorithm by Yashpal Mote et al [11] in their paper says about data encryption algorithm, this algorithm play important role in encrypting and decrypting the data there are present various types of the algorithm that are AES, DES, Triple DES, NTRU, and each of these algorithm have their specific role in day to day life .This paper provides a performance comparison between five of the most common encryption algorithm. This paper also presents a highly efficient implementation of NTRU.

2.7 Data security in cloud computing using RSA by Parsi Kalpana et al[3] mainly 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.

2.8 Dynamic clustering of data with the modified k-mean algorithm by Ahamed Shafeeq B M et al [12] in their paper says that K-mean is the widely used partitioned clustering method. While there are considerable research efforts to characterize the key features of k-mean clustering. This paper presents a modified k-mean algorithm with the improving cluster quality and to fix the optimal number of clusters.

III SYSTEM FRAME WORK AND METHODOLOGY

1) The proposed system exhibits the solid frameworks which were designed during the planning phase of this thesis. Firstly the framework of client-server architecture was been studied which has a Linux based kernel.

The encryption process uses a set of specially derived keys called **round keys**. These are applied, along with other operations, on an array of data that holds exactly one block of data? The data to be encrypted. This array we call the state array.

We can take the following steps to encrypt a 128-bit block:

1.Derive the set of round keys from the cipher key.

2.Initialize the state array with the block data (plaintext).

3.Add the initial round key to the starting state array.

4.Perform nine rounds of state manipulation.

5.Perform the tenth and final round of state manipulation.

6.Copy the final state array out as the encrypted data (cipher text).

The reason that the rounds have been listed as "nine followed by a final tenth round" is because the tenth round involves a slightly different manipulation from the others. The block to be encrypted is just a sequence of 128 bits. NTRU works with byte quantities so we first convert the 128 bits into 16 bytes. We say "convert," but, in reality, it is almost certainly stored this way already.

Each round of the encryption process requires a series of steps to alter the state array. These steps involve four types of operations called:

- SubBytes
- ShiftRows

NTRU algorithm is the algorithm with the help of which we can encrypt our data, and also protects our data from the unauthorized excess. NTRU works on 12 bit of data therefore it is faster as compared to the other algorithms. Encryption requires more time but the data remain safe because decryption become difficult.

Encryption:

It is the process of converting the original text into the cipher text data.

Following are some of the steps [30]:

1.Provider should transmit the public key (n, e) to the user who wants to store the data with him or her. Public key is the key that can be shared easily.

2. User data is now mapped to an integer by using an agreed upon reversible protocol, known as padding scheme.

3. Data is encrypted and the resultant cipher text (data) c is:

$C = me \pmod n$.

4. This cipher text or encrypted data is now stored so that later on can be used when required.

Decryption:

Decryption is the process of converting the cipher text (data) to the original plain text (data)

Following are some of the steps [30]:

1.User request the service provider for the data.

2.The service provider verifies the authenticity of the user and then gives the encrypted data i.e. C

3.The user decrypts the data by computing

$m = Cd \pmod n$.

4.Once the m is obtained the user can get back the original data by reversing the padding scheme.

SIMULATION PLATFORM AND RESULTS

During development phase its quiet difficult to generate the .exe file for testing the application. However to test the application on local environment we need a simulation platform to see its working. This simulation is know as JDK-Netbeans or eclipse is a complete set of tools that provides a virtual environment for Testing of Java Applications. It can be very useful for developers, testers, salesman or even gamers. It is available for most operating systems: Windows, Linux and Mac OS X. It is as simple to install as powerful to use. Encryption timing and decryption time shown in following graphs:

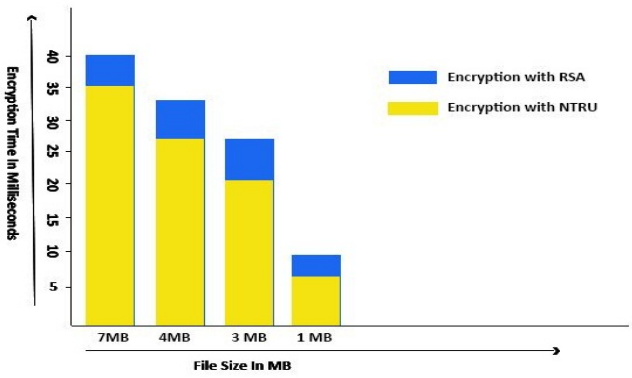

Figure 1. Represent encryption time

In above graph the (figure) the encryption time is shown. In X-axis represent the file size that are in MB. In Y-axis represent the decryption time that in milliseconds. Here two algorithm shows there time for encryption. RSA and NTRU algorithm used for encrypt the data. The graphical representation clearly identifies that the NTRU algorithm needs less time in encryption.

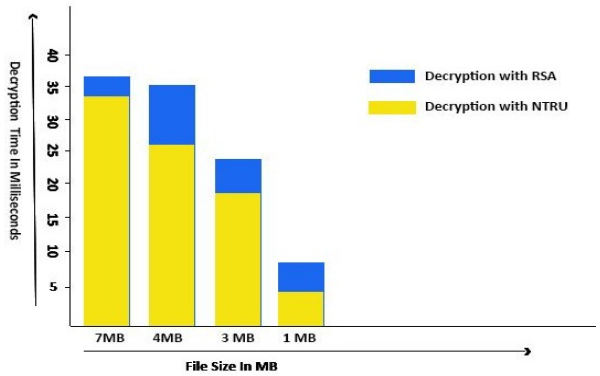

Figure 2. Represent decryption time

In above graph the (figure) the decryption time is shown. In X-axis represent the file size that in MB. In Y-axis represent the decryption time that in milliseconds. We notice that the decryption time of NTRU is faster than the DES.

Throughput:

File Size	Throughput analysis in kb\ms
7MB	210kb/ms
4MB	157kb/ms
3MB	161kb/ms
1MB	204kb/ms

File Size	Throughput analysis in kb\ms
7MB	204kb/ms
4MB	157kb/ms
3MB	139kb/ms
1MB	170kb/ms

CONCLUSION

In this work NTRU algorithm is using to more secured client-server architecture. It has been concluded that NTRU was successful and provides a strong point of security to existing distributed architecture. The Purpose of adding four layered system in client and server side was successful and gave marginal better outcomes than previous research. Some parameters are taken to improve performance and those parameters are encryption time, decryption time, throughput. These parameters are shown by graphs and comparison is done with which conclude that NTRU gives better results than DES. In architecture while adding secured layers we kept in mind the different scenarios of authentication and authorization. The NTRU at last level gave this research and brilliant security that this architecture is fully secured for any kind of confidential data preservation.

FUTURE WORK

Since NTRU provides a strong security measure to existing system. It will be always a area of research as NTRU takes less of power during generation of public and private key and yields higher throughput. On mobile OS NTRU performance can be analyzed in terms of battery consumption and throughput. Preserving the power of smart phones can be new area of research in mobile cloud computing since every application back-end phase is shifting from clusters/grid to cloud based system. These applications usually takes lot of battery power and can effect the battery life of particular phones. Since smart phones processor and RAM runs 24 hours if its not on switched off mode the application running in background can eat up RAM and Processor which leads to decrease in battery life of a smart phone.

REFERENCES

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

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

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

[4] Subedari Mithila, P. Pradeep Kumar, "*Data Security through Confidentiality inCloud ComputingEnvironment*", Subedari Mithila et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 2 , 1836-1840, 2011

[5] Ran Vijay Singh and M.P.S Bhatia , "*Data Clustering with Modified K-means* Algorithm", IEEE International Conference on Recent Trends in Information Technology, ICRTIT 2011, pp 717-721.

[6] Dr. Lokanatha C. Reddy, "*A Review on Data mining from Past to the Future*", International Journal of Computer Applications (0975 – 8887) Volume 15– No.7, February 2011

[7] Navjot kaur and jaspreet kaur shaiwal "*efficient k mean algorithm, using rankingalgorithm*", international conference in computer engineering and technology volume 1, issue 3, May 2012

[8] Kalyam M Raval, "*data mining techniques*", advanced research in computer science and engineering vol-2, issue 2, Oct 2010

[9] Vishma Gupta and Gajendra Singh, "*advancedcryptography algorithm for improvingdata security*",International Journal of Advanced Research in Computer Science and Software Engineering vol 2 issue1,January 2012

[10] Obaidan A.Rawashdeh, "*optimistic approach in distributed database concurrencycontrol*"gernal conference on computer science in Amman University in year (2013)

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

[12] Ahamed Shafeeg B.M "*dynamic clustering of data and modified k mean algorithm*" international conference of information and technology, vol 27(2012), Singapore

[17] D. S. Johnson and L. A. McGeoch. The travelling salesman problem: A case study inlocal Optimization. In E. H. L. Aarts and J. K. Lenstra, editors, Local Search in Combinatorial Optimization, pages 215–310. John Wiley & Sons, Chichester, UK,1997.

[18] Sharad N. Kumbharana1, Prof. Gopal M. Pandey2International Journal of Societal Applications of Computer Science Vol 2 Issue 2 February 2013ISSN 2319 – 8443.

[19] K. F. Man, Member, IEEE, K. S. Tang, and S. Kwong, Member, IEEE, IEEE, VOL. 43,NO. 5, OCTOBER 1996.

[20] Shubhra Sankar Ray, Sanghamitra Bandyopadhyay, and Sankar K. Pal, "First InternationalConference, PReMI 2005, Lecture Notes in Computer Science, vol. 3776, pp. 617-622,2005, Springer-Verlag, Berlin, 2005.