IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-3, Issue-7 E-ISSN: 2347-2693

Hybrid Parallel Multithreading Encryption

Deepali[1]* and Namita Kakkar [2]

[1*, 2*] Department of Computer Science & Engg, PTU, India

www.ijcseonline.org

Received: Jun/09/2015 Revised: Jun/28/2015 Accepted: July/18/2015 Published: July/30/ 2015

***Abstract*—** Cloud computing is a new area for the field of research. In the current scenario the server and client architecture is advanced giving rise to speed and reliability and is been shifting from distributed or cluster to cloud architecture since cloud architecture maintains the server in various number of features. The main part of this research relies on a robust architecture which deals with Cloud Storage as a Service (SAAS) and comparative security measures of improvement and modifications. Various security measures have been studied during this research which is briefly described in various sections of this report. The main motive of shifting the platform to cloud is its "popularity" and "portability". Smart phone devices are booming in market and it covers most of the works of people which was earlier used to done by the help of computer. We can read mails with push notifications facility, we can communicate and store large number of data in mobile devices thus the technology is shifting from distributed to cloud platform. Client Server Architecture- this method is a first part of study of this thesis which was needed to be developed before moving onto the next levels of Cloud Computing. The client section was a simple application for user which was made on Socket Programming in Java. Application connection was made with Server which is a LAN based server on which data is to be uploaded and downloaded. Analyzing RSA and NTRU in parallel computing environment is developed, then it needs to be secured with a particular algorithm or technique. The algorithm studied is known as RSA key oriented algorithm which offers dynamic security on client and server level during communication. The other technique for advancing the level of scalability and improvement alone the network layer we used is NTRU encryption.

***Keywords*—**RSA, LOSSY, SAAS

I. INTRODUCTION

Distributed parallel cloud database plays a very vital and paramount role in our day to day life [5]. Before dealing with this, first of all we will have a brief introduction about the distributed computing. So, distributed computing system is the collection of the processing elements that are interconnected by network and these processing elements coordinate to perform a specific task. Moreover these processing elements are heterogeneous in nature. Whereas distributed system is the collection of logically related database that are distributed over a network. 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 [5]. The major problem that we face in normal database is that failure at one point means overall failure, but in Distributed parallel cloud database, failure at a single point problem is removed because in this system database is distributed to many locations and if there is some kind of failure at one point, we can access data from the other location also [5].

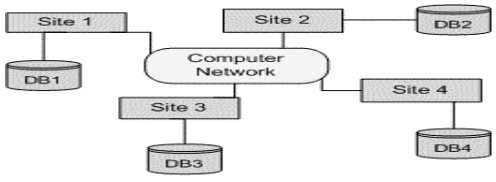

Figure I Distributed parallel cloud database Systems [17]

I.I PARALLEL AND DISTRIBUTED COMPUTING

In parallel computing all the processing elements will access the shared memory for the purpose of exchanging information. Whereas in the distributed computing each and every processing element has its own memory or we can say it has its private memory. In the following diagram distributed and the parallel systems are shown.

Parallel computing is mainly the type of computation in which multiple operations or calculations are performed simultaneously. In this computing problem is divided into small parts and then each part is solved concurrently and hence the work gets completed in less time. Parallel computing is of many types i.e. bit level, instruction level, task parallelism and each type has its own significance and importance. In instruction level parallelism computation is done mainly on the basis that how many operations can be computed at the same time. In parallelism task is distributed across the several parallel computing nodes. Distributed computing is the field in which we focus mainly about the distributed system. The distributed system is the system in which components are dispersed on different geographical locations and these components interact with each other by the means of the message passing. These components communicate with each other so to achieve the common goals. There are present some characteristics that differentiate this distributed environment from the centralized environment. The major advantage of using this is increasing the availability and also enhancing the speed.

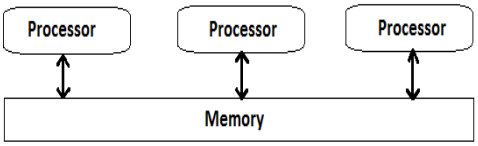

Figure I.I: Parallel Computing [17]

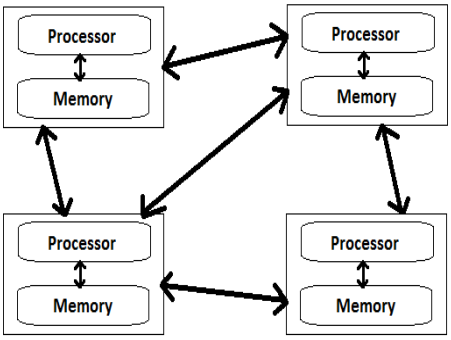

Figure I.II: Distributed Computing [10]

I.I.I CHARACTERISTICS OF DISTRIBUTED PARALLEL CLOUD DATABASE

Distributed parallel cloud database system has following some of the different characteristics and these were discussed below with some brief introduction in this regard [10].

Concurrency of components: It means that all the components perform concurrently within Distributed parallel cloud database and are able to access the results efficiently without any error.

Lack of global clock: It means there is absence of any global clock. Therefore different processor will have different notion of time and hence due to this they are unable to determine the order in which two processors are executing.

Independent failure of components: It means that if any one site fails, then it will not slower or interrupt our overall task but rather than that task will be shifted to another site. Hence single site failure problem will not occur in case of Distributed parallel cloud database.

I.II DISTRIBUTED PARALLEL CLOUD DATABASE MANAGEMENT SYSTEM

Distributed parallel cloud database is the database that is placed not a single location, but at several location or network sites. This feature enable us to access or data easily and also at the fast speed. Since the data is distributed it does not means that all the storage devices of that particular database is attached to or with the help of same or we can say unique processing unit. Distributed parallel cloud database management system is the system that manages the Distributed parallel cloud database and responsible for making this distribution transparent. This transparent means that user is not aware of this distribution.

Suppose the user make a query to p1 "find all the employees working in research department". The user is unaware that employee is not at p1 rather it is present at p3. Therefore Distributed parallel cloud database distribute the query into two parts. First it will fetch the tuples of department table then it will fetch the tuples of employee table after that join the result. This all is done to make the distribution transparent. In the following diagram there is the clear demonstration of the above scenario, that how distribution is made transparent from the user and how the overall work precedes.

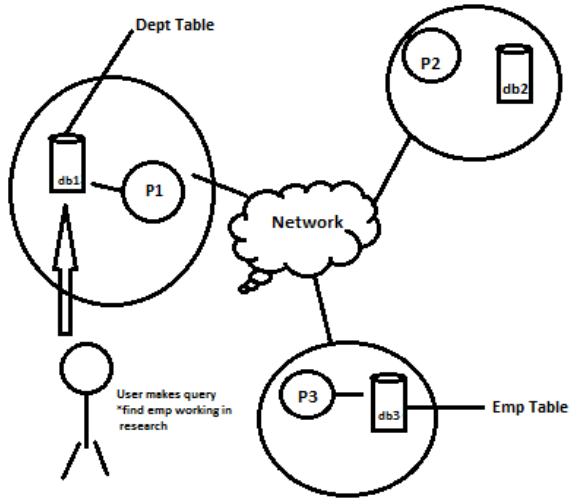

Figure I.III.I: Distribution Database System with Transparency [10]

Distributed parallel cloud 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 [17]. Another factor that is considered in Distributed parallel cloud databases is updations of the contents 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.

I.III Distributed Parallel Cloud Database Design

Distributed parallel cloud database design plays an important role, it is not only because of its performance but also because of its reliability and also is an efficient way of reducing the overall cost and hence symmetric design will

act as best solution to our problem. This design phase will include two approaches [5] i.e. top down and bottom up approach.

a. Top down approach: This approach generally follows hierarchical pattern i.e. information flows in hierarchy that means first of all defines the generally used concepts followed by the framework that we are going to use and then the detail.

b. Bottom down approach: This is generally the reverse of the top down approach, instead of defining the framework, this approach focuses on details first, then later on deal with the framework.

There are present some additional factors that are considered under this concept along with these top down and bottom down approach [5]

I.IV Advantages of Distributed Parallel Cloud Database

Distributed parallel cloud database is the database which is distributed at several locations, therefore due to this there arises many benefits out of this and some of the benefits are discussed below:

I.IV.I Transparency: In Distributed parallel cloud database transparency means when complexity related to the distribution is hidden from the user and the user feels as if it is dealing with the centralized system. Moreover transparency can be related with some simple example. Suppose any user wants to fetch the any particular record from the employee table. This table is located in the database of some other site. The user will able to fetch the records by applying the joins between the two queries, but this entire process is hidden from the site of the user.

Network transparency: In this transparency user doesn't know about the network and it will look like the standalone computers.

Location transparency: Location of the distribution is not known to the user. User can access any data from any location by using the single command without knowing its actual location. It means the user can able to access the record of some other location also even though he is suited somewhere else. This entire process is transparent from the site of the user. Therefore this will help to increase the availability and the speed of fetching any particular data.

Naming transparency: This transparency will allow accessing any object name like amazon.com from any location.

I. **Replication transparency:** In this transparency if some modifications are made at site1 then that modification should be reflected in site '2' also and user is unaware of this replication. Moreover the difference between the replication and the duplication is that, in duplication there we identify the master database and then duplicates that database. Whereas in replication once the changes are identified then replication process makes all databases look same. [4]

II. **Fragmentation transparency:** In this transparency fragments of any particular data or we can say data is divided into different parts and each part is processed separately, this technique will improve the overall performance with appropriate speed and this overall process is hidden from the user.

Horizontal fragmentation: In this fragments are prepared horizontally by selecting any relevant row. Here fragments are constructed on the basis of attribute values. In the given scenario we mainly included the global relation. They include all the attributes that we considered while dealing with the horizontal fragmentation. The difference that we analyzed in this fragmentation is fragment is prepared on the basis of the attribute value i.e. in first fragment there exist all the entries of the male and then in the corresponding fragment their present the entries of the females. This way maintenance is done properly.

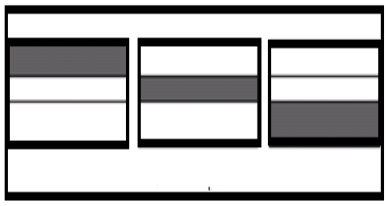

Figure I.IV.I: Horizontal Fragmentation

Following is the relation on which we apply horizontal fragmentation

Table I.IV.I: Relation for Horizontal Fragmentation

Customer Id	Name	Area	Payment type	Sex
1	A1	Chandigarh	Credit card	Male
2	A2	Jalandhar	Cash	Male
3	A3	Patiala	Cash	Female

Fragment I: This fragment includes the entries of the males.

Fragment II: This fragment includes the entries of the females.

Table I.IV.II: Horizontal Fragment I

Customer id	Name	Area	Payment type	Sex
1	A1	Chandigarh	Credit card	Male
2	A2	Jalandhar	Cash	Male

Fragment II: This fragment includes the entries of the females.

Table I.IV.II: Horizontal Fragment II

Customer id	Name	Area	Payment type	Sex
3	A3	Patiala	Cash	Female

Hence this way the vertical and the horizontal fragmentation are performed on the defined relation. Hence basic idea behind the fragmentation is that, we mainly split complex problem into multiple parts. Then each part is executed individually and after its execution we reassemble all the fragments. This way we evaluate results efficiently and speedily.

I.IV.II Increased reliability and availability: Reliability means the probability by which system is working at

Method	RSA	NTRU
Approach	Symmetric	Asymmetric
Encryption	Slow	Fastest
Decryption	Slow	Faster
Key Distribution	Easy	Easy
Complexity	O(N^3)	O(N log N)
Security	Highest	High

specific point in time and whereas availability means probability at which system is working continuously during the particular time interval. Moreover increased availability means that particular site fails due to some problem then at that case query will be shifted to some other site which is working efficiently. Hence availability means that we will be available with our data even if any site corrupts.

I.IV.III Improved performance: In centralized database suppose there are four sites and request for all these sites reaches to the single database and due to this database become the bottleneck. Whereas in Distributed parallel cloud database all the sites have their respective database due to which the performance gets improved.

I.IV.IV Easier to expand: In the centralized database there is a limit behind adding the number of processors and beyond that we can't add more processors. Whereas in distributed there is no limit behind this, if we want to add more processors then they can be added by including more sites to it.

II. CURRENT WORK

II.I SCOPE OF STUDY

Following are the points which make this thesis scope a promising approach.

a) Improving the RSA or Rinjdael without compromising the security of existing technique.
b) To integrate the new technique by introducing the cipher text conversion of NTRU algorithm.
c) Improving the computation time of encryption and decryption by integrating the existing algorithm with NTRU in parallel.
d) To improve the throughput of existing RSA. The benefit of increasing the throughput on decryption and encryption is proposed method will save the energy of server and client devices by using a core CPU threads two at a time.

II.II PROBLEM FORMULATION

Rinjdael or RSA which is second of this good encryption algorithm. What it does, it encrypt the message or can encrypt the data which is been put on network. We can work on the technique by integrating the Rinjdael algorithm NTRU algorithm to speed up the system, moreover there will be a multithreaded server which runs the both algorithm parallel. The hybrid encryption/cryptography technique using this architecture in parallel environment which enhances the performance and speed of Encryption/ Decryption process. That is multiple (two) algorithms will run simultaneously in a single thread. We shall be running two main servers at single system once by using the processor's core thread in short two servers will be running on single system. These two servers will work together to provide a multilevel encryption and generates a secret file from a plain text file.

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 superior security encryption algorithm [21]. 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 [14].
- Throughput in case of the NTRU is improved 60% when it gets combined with SSL [14].
- It helps in reducing server resource utilization significantly in case of large-scale deployments.

II.III OBJECTIVES ACHIEVED

Objectives aimed at to be achieved when two threads of single server are running in parallel gave successful completion of this work:

- Reduced encryption and decryption time compared to the other algorithms.
- Reduced decryption time with respect to increase in the number of bits.
- Better accuracy at detecting authorized and unauthorized users using different packages.

Better throughput compared to the other algorithms.

II.IV METHODOLOGY ADOPTED

In this concurrency and security in Distributed parallel cloud database, the language which we have considered is java.

Backend we are going to use WampServer with MYSQL database

Frontend java followed by the net beans

SO the programming language that we are going to use is java, whole coding of our work or we can say that implementation will be preceded by using java, code that we are going to write is tested and compiled on IDE.

WAMPSERVER is the server that we are going to use at backend is the combination of different components such as MYSQL, PHP server and all these are available in a single package. There are present various ways by which or by the help of which we can construct WAMPSERVER. Moreover it is the open source and their present a graphical tool that help to handle the administration of MYSQL.

II.IV.I System flow design: In this design we mentioned the entire steps we are going to perform in our entire work like upload the content and then afterwards encrypt the data using NTRU algorithm with its cipher text formation and public and private key is enabled by RSA then download the content and after that decryption is performed.

Database: first of all we deal with the database, place where data is stored. So when we need any data we can fetch our valuable data from the database.

Upload the content: Then after fetching our valuable data we will we upload that content.

Encrypt with NTRU: After uploading the contents of the data, we need to encrypt it so that we can maintain security. Therefore we are adopting the algorithm named NTRU. By this algorithm we can encrypt efficiently and able to improve the RSA algorithm by reducing the encryption and the decryption time. It is responsible for increasing accuracy in terms of throughput and processing speed.

Download the content: after encrypting our data with the help of the NTRU algorithm we send it to the server. The server will download the content. Then he will find that data is in encrypted form.

Decryption: when server downloads the content that was sent by the client, then he will find that data in plaintext form if the user is authorized. When the user is not authorized get data in encrypted form. This procedure is used to maintain the security.

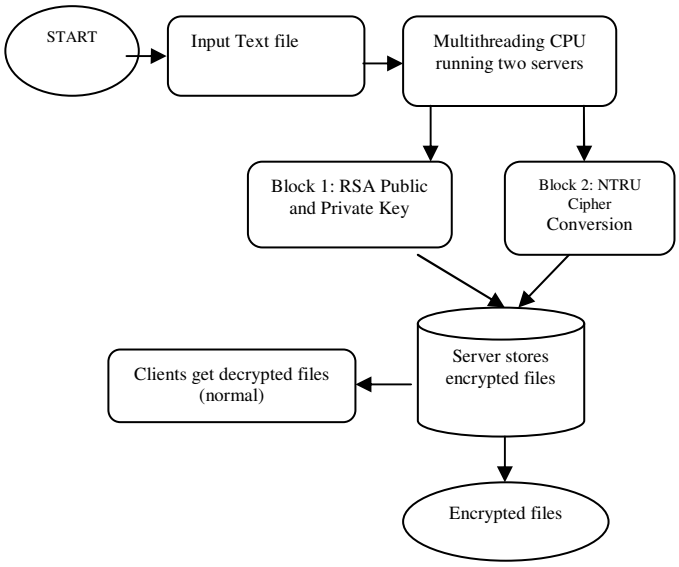

Figure II.IV.I: System flow design

II.IV.II Working of proposed architecture

I. The generic steps used for Encryption [5]:

Step-I: Read the content from a file and store in string builder.
Step-II: Convert the string builder in to character array.
Step-III: Take every character from an array then take its ASCII value after that convert it in binary value example like 10011101111110000001.
Step-IV: 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 [5]:

Step-I: Take the decryption files from computer and read its content.
Step-II: 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-III: Now apply inverse Euclidian algorithm to get decryption number and then apply it on a binary pattern.
Step-IV: apply the following steps

a. After that take five 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.

III. RESULTS AND DISCUSSIONS

In this part we are basically going to discuss about the encryption and decryption timing with regards to RSA and NTRU as to how they behave at different data packets and what their results are accordingly. So in this we will mainly focuses on the encryption and decryption timings and to analyze them as to get the answer of our problem qua NTRU's better position than RSA and also to calculate the throughput vis-à-vis RSA and NTRU together.

III.I Performance analysis of NTRU and RSA with respect to encryption and decryption

Here we are going to evaluate encryption and decryption timings of NTRU and RSA to show that NTRU is better encrypting algorithm with respect to RSA

III.I.I Encryption analysis of NTRU and RSA

The graph mentioned below shows that as the input size increases timings of NTRU and RSA changes. It shows us explicitly that NTRU's timings is far better than RSA

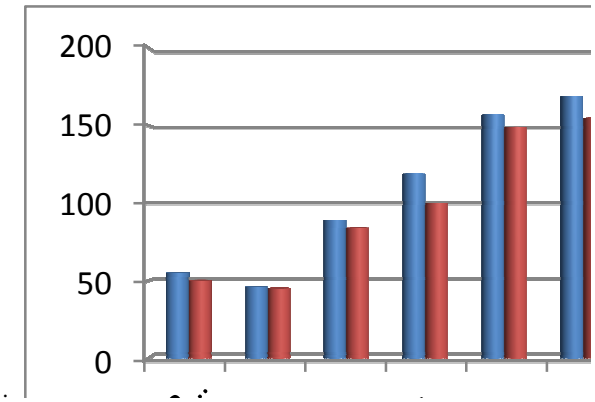

Figure III.I: Comparison Analysis of Encryption

Table III.I: Encryption Timings

Input size(Kb)	RSA Timing(ms)	NTRU Timing(ms)	RSA/NTRU Timings in Parallel Environment
32 bytes	730ms	2ms	562ms
2.44	872ms	15ms	78ms
1.44	563ms	15ms	62ms
63bytes	610ms	31ms	63ms
6.69	297ms	16ms	47ms
892	62ms	17ms	62ms

The table constructed above shows the variations in the timings for the encryption in NTRU and RSA. When includes 892kb input size for RSA, it will take 62ms for encrypting the data, whereas in NTRU only 17ms required for encryption and both in parallel environment 62ms.

III.I.II. Decryption analysis of NTRU and RSA

Here analyzed decryption for NTRU and RSA timings vary on the rival of different data packets.

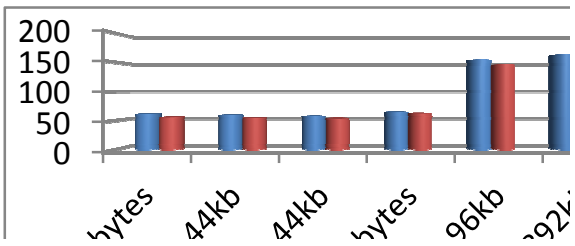

Figure III.I.II: Comparison Analysis of Decryption

Table III.I.II Decryption Timing

Input size (Kb)	RSA Timing (ms)	NTRU Timing (ms)	RSA/NTRU Timings in Parallel Environment
32bytes	15ms	1ms	47ms
2.44	40ms	9ms	31ms
1.44	12ms	32ms	31ms
63bytes	31ms	16ms	30ms
6.96	20ms	31ms	15ms
892	62ms	20ms	16ms

The table constructed above shows the variations in the timings for the decryption in NTRU and RSA. When includes 892kb input size for RSA, it will take 62ms for decrypting the data, whereas in NTRU only 20ms required for encryption. Therefore NTRU is speedier while decryption

III.II Throughput Evaluation of NTRU and RSA

Throughput is inversely proportional to number of recourses used, more the throughput less will be the resource utilization and vice versa RSA

And the formula in this regard to calculate the average throughput is by converting the input size into MB by dividing it by 1024 and time in seconds by multiplying it with 0.001 as (1 sec=0.001 ms) and (1024 KB=1mb). Suppose input size is 45 kb. 45/1024=0.04 and 55ms * 0.001=0.055. Now 0.04/0.05 =0.8.

III.II.I Throughput evaluation of NTRU and RSA with regards to encryption

The throughput of NTRU is better than RSA it means that it uses less resources that is the reason why it is so efficient.

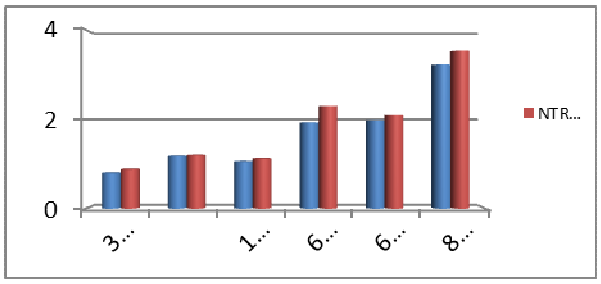

Figure III.II.I: Throughput Evaluation of Encryption

Table III.II.I: Throughput for encryption

Input size (Kb)	RSA throughput (MB/sec)	NTRU throughput (MB/sec)
32 bytes	0.239257	4.4456
2.44	0.242838	3.3597
1.44	0.147135	5.7240
63 bytes	0.061921	4.8027
6.96	0.434265	1.0193
892	0.568924	5.3553

The table constructed above shows the throughput for the encryption in NTRU and RSA. When includes 6.96kb input size for RSA, it will give 0.4342mb/sec throughput during encryption, whereas in NTRU generates 1.0193mb/sec throughput. Therefore more the throughput less will be the consumption of resources, so NTRU is better than RSA.

III.II.II Throughput evaluation of NTRU and RSA with regards to Decryption

Here shown that the throughput of NTRU is better than RSA it means that it uses less resources that is the reason why it is so efficient.

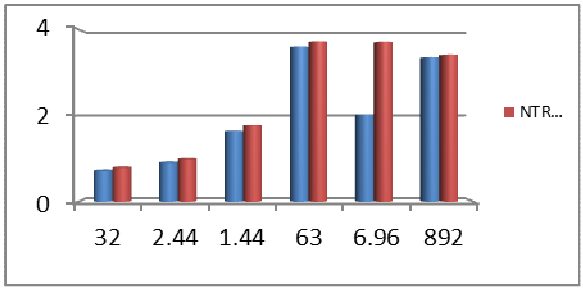

Figure III.II.II Throughput Evaluation for Decryption

Table III.II.II Throughput for decryption

Input size (Kb)	RSA throughput (MB/sec)	NTRU throughput (MB/sec)
32 bytes	0.239257	4.4456
2.44	0.242838	3.3597
1.44	0.147135	5.7240
63 bytes	0.061921	4.8027
6.96	0.434265	1.0193
892	0.568924	5.3553

The table constructed above shows the throughput for the decryption in NTRU and RSA. When includes 892kb input size for RSA, it will give 0.5689kb/sec throughput during decryption, whereas in NTRU generates 5.3553kb/sec throughput. Therefore more the throughput less will be the consumption of resources, so NTRU is better than RSA.

As there is the need of security in every step of life we have discussed each and everything in detail about out work that how our work can be taken as a primary source of consideration. We have discussed each and everything about Distributed parallel cloud database and its components in detail and our main stress always remains on the NTRU's better position than RSA. So NTRU is far finer and finest than RSA algorithm. We have mainly tried to enhance the encryption, decryption timings and throughput and processing speed of NTRU with respect to RSA and our results are explicitly showing NTRU's healthier position with regards to RSA.

Table III.II.II.I: Throughput Comparison

Input size (Kb)	RSA throughput (MB/sec)	NTRU throughput (MB/sec)	Throughput in parallel Environment (Mb/sec)
32 bytes	0.239257	4.4456	6.4293
2.44	0.242838	3.3597	4.2568
1.44	0.147135	5.7240	5.8278
63 bytes	0.061921	4.8027	5.2703
6.96	0.434265	1.0193	7.2722
892	0.5689243	5.3553	5.9853

IV. CONCLUSION AND FUTURE SCOPE

After undergoing each one of the illustrations and delineations mentioned supra which we have considered in our proposed work and on culmination of that to obtain the valid and substantiated particulars, facts and details through Distributed parallel cloud database Management System, we came to conclusion that NTRU is the matchless and we can easily makes NTRU as a chief and foremost choice to use it not only because its speedier and prompt than any other algorithm but also because it possess eye-catching features which force us to use NTRU as a primary choice. The main and chief characteristics which coerce us to use it are like on the market it's the highest performing crypto. In addition to this the other quality it possess that it is more rapid than RSA because of its speed i.e. it is 5x to 200x, which is also one of the most astonishing quality. Moreover the execution of effective algorithms for the motive of polynomial generation in future can also be done. Additionally the comprehensive annotations qua the position of NTRU is being provided in this proposed work vis-à-vis DES and RSA because of some surprised points which we can take into our consideration like its security level is the first and paramount point to be considered because the security level of NTRU is approving and highest, and apart from this point the another point to take into our consideration is the cryptography of NTRU which is the most smallest available. Furthermore the capability of protecting systems because of its trait of being future proof from today's attacks and entirely we have mainly focused in this proposed work on the prodigious position of NTRU with regards to DES or RSA as its more effective and more efficient than any other Algorithm.

REFERENCES

[1] B. Padmavati and S. Ranjitha Kumari "Security and performance analysis of DES, RSA and RSA algorithm with LSB substitution technique" International Journal of Computer Science Vol-2, Issue-4, Page No.**170-174**, April-**2013**

[2] Dr. C. Sunil Kumar, J. Seetha, S.R Vinotha "Security implications of Distributed parallel cloud database management system models" International Journal of Software Computing and Software Engineering, Vol-2, Issue-11,Page no-**20-28**, **2012**.

[3] Dr. Lokanatha C. Reddy "A Review on Data mining from Past to the Future", International Journal of Computer Applications (0975 – 8887), Vol-15, Issue-7, Page No. **19-22**, February - **2011.**

[4] Gupta V.K., Sheetlani Jitendra, Gupta Dhiraj and Shukla Brahma "Data concurrency control and security issues of Distributed parallel cloud database transaction" NIMS University, Jaipur, Rajasthan, INDIA Vol-1, Issue-2, Page No. **70-73**, August-**2012**.

[5] Gurkamal Bhullar and Navneet Kaur "Concurrency and security control with NTRU" International Journal of Innovative Research in Computer Science and Communication Engineering Vol-2, Issue 3, March **2014.**

[6] He.Debiao, Chen Jianhua and Hu Jin "Random Number Generator based on the NTRU Cryptosystem" Maejo Int. J. Science Technology Vol-4, Issue-3, Page No. 428-434, 2010.

[7] Ilker Kose "Data and Network Security" Springer, 2002 GYTE, Computer Science, Page No. 1-9.

[8] Kalyam M Raval, "Data Mining Techniques", Advanced Research in Computer Science and Engineering Vol-I, Issue IV, Page No. 1-7, Sep 2014.

[9] Manpreet "Concurrency control in Distributed parallel cloud database system" International Journal of advanced research Vol 3, July 2013.

[10] MD. Tabrez Quasim "Security issues in Distributed parallel cloud database system model" International Journal of Advanced Computer Science Department Vol-2, Issue 12, Page No. **396-399**, December **2013**.

[11] Navjot Kaur and Jaspreet Kaur Shaiwal "Efficient k mean algorithm, using ranking algorithm", International Conference in Computer Engineering and Technology Vol- 1, Issue 3, May **2012.**

[12] Obaidan A.Rawashdeh, "Optimistic approach in Distributed parallel cloud database concurrency control" Journal Conference on Computer Science in Amman University in year **2013**.

[13] Parsi Kalpana and Sudha Singaraju, "Data security in cloud computing using RSA algorithm, International Journal of Research in Computer and Communication Technology,Vol-1,Issue-4,Pageno-**143-146**,September **2012**.

[14] Ranjit Ranjan, Dr.A.S Baghel, Sushil Kumar "improvement of NTRU cryptosystem" international journal of advanced research in computer science Vol-2, Issue-9, Page No. **79-84** September **2012.**

[15] 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, Vol-3, Issue-11, Page No. **1283-1286**, Nov **2013**.

[16] Shashi Mehrotra Seth and Rajan Mishra "Comparative Analysis of Encryption Algorithm for Data Communication", International Journal of Computer Science and Technology, Vol-4, Issue-8, Page no-**348-354**, August **2014**.

[17] Sheetlani Jitendra and Gupta V.K. "Concurrency Issues of Distributed Advance Transaction Process", Res. J. Recent Sci., Issue-1(ISC-2011), Page No. **426-429** , **2012**

[18] Subedari Mithila, P. Pradeep Kumar, Subedari Mithila et al "Data Security through Confidentiality in Cloud Computing Environment",(IJCSIT) International

Journal of Computer Science and Information Technologies, Vol-2 , Page No.**1836-1840, 2011**

[19] Swadeep Singh and Anupriya Grag "Comparison of cryptographic algorithm ECC and RSA", International Journal of Computer Science and Communication Engineering, Vol-6, June **2013**.

[20] Vishma Gupta and Gajendra Singh "Advanced cryptography algorithm for improving data security", International Journal of Advanced Research in Computer Science and Software Engineering, Vol-2 Issue-1, January **2012.**

[21] YashPal Mote and Shekhar Gaikward, "Superioer Security Data Encryption Algorithm", International Journal of Computer Scienece, Vol- 6, Page no-**171-181** , July **2012.**